### Web Servis Nedir?

### İçindekiler

a. Web Servis Tanımı b. Web Servis Rolleri c. Web Servis Calısma Sekli d. Web Servis Türleri e. Web Servislerin Arayüzleri Olmaması Hk f. Web Servis Arayüz / Kapsam Dosyalarının Güvenliğe Dokunan Yanı g. API ve Web API (Web Servis) Arasındaki Fark h. Web Servisleri Test Etme i. Web Servis Ek Notlar Uygulama [SoapUI Yazılımı ile SOAP Web Servis Test Etme] Uygulama [SoapUI Yazılımı ile SOAP Web Servis Test Etme 2] Uygulama [SoapUI ile Rest Web Servis Test Etme] Uvgulama [Burpsuite WSDLER Eklentisi ile Soap Web Servis Test Etme] Uygulama [Burpsuite ile Rest Web Servis Test Etme] Uvgulama [Netsparker Yazılımı ile Soap Web Servis Test Etme] Uvgulama [Netsparker Yazılımı ile Rest Web Servis Test Etme] Uygulama [Chrome Web Tarayıcı Eklentisi İle Soap Web Servis Test Etme] >>> Web Servisleri Saha Görevlerinde Test Etme Hakkında (Genel Değerlendirme)

#### a. Web Servis Tanımı

Web servisi web sunucularda yer alan, herhangi bir programlama dili (örn; php, java, c#,...) ile yazılabilen, herhangi bir web sunucu platformunda (örn; apache, iis, nginx, ... de) yer alabilen, farklı platformlardaki ve programlama dillerindeki (örn; windows-based, unix-based, web-based, mobile-based,... platformlardaki ve php, java, c#,... dillerindeki) uygulamaların XML mesajlaşma sistemiyle haberleşerek kullandıkları bir yazılım parçasıdır.



Response from server to client

( Örnek Bir Web Servis Haberleşmesi )

(Web Servisler Web Sunucuda Host Edilir)



(Çeşitli İstemcilerin Web Servisle Haberleşmesi)

Web servisi bir programlama dilinin bir başka programlama diliyle haberleştiği bir teknolojidir. Yani web servisi teknolojilerin birbirleriyle bir arada olabildikleri bir yol sunar. Bunu XML ve JSON kullanımı ile yaparlar. Teknolojiler bu ortak platform bağımsız veri formatlarını kullanarak birbirleriyle haberleşebilirler. Sıralanan resimlerde sol tarafta web servis kullanan / tüketen tarafla web servis sunucusu tarafının haberleşme şekli, sağ tarafta web servislerin web sunucularda host edildiği bilgisi, aşağı tarafta ise çeşitli teknolojilerdeki web servisi kullanan / tüketen uygulamaların xml haberleşme şekliyle web servisle haberleşmesi gösterilmiştir.

Web servisi 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 ile konuşması veya iOS bir mobil uygulamanın php ile yazılmış bir web servis ile konuşması örnek olarak verilebilir, veya aynı türden teknolojilerin haberleşmesine dvws (damn vulnerable web services) web servisi kullanan / tüketen uygulamanın web-based bir web tarayıcıdaki php uygulaması olması ve web servisinin de php olması örnek olarak verilebilir.

# b. Web Servis Rolleri

Web serviste

- service requestor ve
- service provider

adlı roller vardır. Bu rollerden service requestor web servisi tüketendir / kullanandır. Herhangi bir platformda / ortamda yer alabilir. Service provider ise web servisi sağlayan ve internetten erişilir kılandır. Web sunucuda yer alır. Service requestor örneğin web-based olabilir, windows-based olabilir, unix based olabilir,..., farklı türden platformlara özgü uygulamalar olabilir. Service provider ise örneğin web sunucudaki java bir uygulama olabilir, asp.net bir uygulama olabilir, php bir uygulama olabilir. Service requestor'lar service provider'a ağda bağlantı açarlar ve XML talepleri yollarlar. Yanıt olarak da XML yanıtları alırlar.

#### c. Web Servis Çalışma Şekli

Service requestor'lar service provider'la xml talepleri ve yanıtlarıyla konuşurlar. Örneğin aşağıda php ile yazılmış bir web servisinin, 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 {
        $row = array("siteStatus" => "General Error");
    }
    print json_encode($row);
    mysqli_close($dbLink);
} // End else condition (for database connection)
?>
```

Kodlamaya 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 yanıt olarak gönderiliyor.

	- • •
🧲 🕘 <i>ể</i> http://tt/fd/b6c: 🔎 - 🗟 🖒 🗙 <i></i> 🧉 tt	2
{"siteStatus":"Up"}	^
	+

Burada service requestor web based bir uygulama olduğundan tarayıcıda yanıt görüntülenmektedir. Web uygulamalarda yanıt paketleri html dökümanı döner iken web servislerde xml / json dönülür. Bu örnekte web servisindeki bu türden dönüş için print\_json\_encode() metodu kullanılmıştır.

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 ikinci örnek için service requestor'ın gönderdiği geçerli hesap bilgilerindeki login olma paketi ve aldığı yanıt örneği,

Örnek Http Request 1:

#### Örnek Http Yanıtı 1:

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

#### Örnek Http Request 2:

Örnek Http Yanıtı 2:

// Headers ... // Headers ... // Headers ... // Headers ... <soapenv:Body> <soapenv:Fault> <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 wuygulamalarda yapılan her işlem yapılabilir. Web servisler bu işlevleri xml (veya json) etiketleri üzerinden gerçekleşen alışverişle yaparlar. Dolayısıyla web uygulamalardaki brute force, sql enjeksiyonu, komut çalıştırma,... gibi saldırılar web servislerde de yapılabilmektedir ve web uygulamalarda çıkan açıklıklar web servislerde de çıkabilir.

## d. Web Servis Türleri

Web servisleri ağırlıklı bir şekilde kullanıma göre iki türdür. Bunlar,

- SOAP Web Servisi
- REST Web Servisi

şeklindedir. Bu iki web servisi piyasadaki en baskın iki türdür. SOAP web servisi zaman zaman 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.

#### e. Web Servislerin Arayüzleri Olmaması Hk

Web servisler kendi başlarına bir arayüze sahip değildirler. Örneğin web uygulamalarda gelen yanıt paketlerinde spidering / crawling yapılarak arayüz / kapsam belirlenir. 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 tarayıcılarının 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 optional (seçime bağlı) olarak WSDL dosyası kullanılır. 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 yanıt olarak bekleniyor, ... gibi bilgileri öğrenilir. Bu şekilde kapsam elde edilir ve saldırı testleri veya fonksiyonel çalışırlık testleri uygulanabilir. SOAP web servisler WSDL'e bağımlıdırlar ve SOAP web servislerini keşfetmek adına başka bir mekanizmaya sahip değildirler. Yani SOAP'ta WSDL tek çözümdür. Fakat soap web servislerin WSDL kullanımı zorunlu değildir.

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 bir 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.

### f. Web Servis Arayüz / Kapsam Dosyalarının Güvenliğe Dokunan Yanı

Web servislerde soap için wsdl veya rest için wadl, openapi (swagger),... gibi arayüz / kapsam dosyalarının public olarak web servis adresinden erişilebilir olması güvenlik riski oluşturmaktadır. Bu durum örneğin soap web servisleri WSDL Enumeration adı verilen açıklığa karşı savunmasız bırakacaktır. Çünkü public olarak arayüz / kapsam dosyalarının erişilebilir olması saldırganların gizli fonksiyonları bulabilmesine yol açacaktır ve muhtemel hassas verilere erişebilmesine yol açabilir. Bu nedenle arayüz / kapsam dosyaları public olarak erişilebilir olmamalıdır. Arayüz / kapsam dosyasına erişim kısıtlanmalıdır ve arayüz / kapsam dosyalarında gereksiz tanımlamalardan sakınılmalıdır.

# g. API ve Web Servis API Arasındaki Fark

API (yani Application Programming Interface) birbiriyle benzerliği olmayan iki uygulamanın haberleşebilmesini sağlayan yazılım bileşenine denir. Eğer API veri göndermek için network'ten yararlanıyor ise bu API'lere de web API denir. API ile Web API arasındaki fark Web API'nin bir API alt türü olmasıdır. Yani API tanımsal olarak daha geniş bir kategoriye tekabül eder. Kök kategoridir. Web API ise bir API türüdür.

API ve web API farklı uygulamalar arasında veri transferi için kullanılan iki teknolojidir. API bir uygulamanın verilerini dış uygulamalara sunan bir arabirimken web API bir uygulamanın verilerini dış uygulamalara sunan daha katı gereksinimlere sahip bir arabirimdir. Web API'nin sahip olduğu bu gereksinimler network üzerinden iletişiminin olması, "birincil" iletişim protokolü olarak SOAP kullanılıyor olması ve genelde public olarak daha az erişime izin veriyor olmasıdır.

Aşağıda API türü olan web API'nin sahip olduğu türler listelenmiştir.

Web API Türleri:

- Open APIs
- Partner APIs
- Internal APIs
- Composite APIs
- Web service APIs (\*)

Web Servis API bir web API'dir. Web Servis API'ye örnek olarak şu popüler türler verilebilir.

Web Servis API Türleri:

- SOAP
- XML-RPC - JSON-RPC
- REST

Tüm web API'ler birer API'dirler, fakat her API web API değildir. Çünkü web api dışındaki api'ler network ile haberleşmezler. Lokalden haberleşirler.

Aşağıda web api ve api arasındaki network farkını göstermek adına temsili resimler verilmiştir:



Sonuç olarak api ve web api (daha spesifik ifadeyle web servis api) arasındaki fark network'ün varlığıdır.

# h. Web Servisleri Test Etme

Web servisler çeşitli web zafiyet tarayıcı araçlarla test edilebilir. Örneğin soap ve rest web servisler için geliştirilmiş SoapUI (Soap User Interface) yazılımı, Burpsuite WSDLER plugin'i, Netsparker veya web tarayıcı eklentileri gibi araçlar test uygulayabilirler.

## \* SoapUI

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 dosyası verilir.

Activiti	es 🧕	com-ins	all4j-run	ime-lau	Incher-Unix	Launcher	*						Cts	15:40									6	6 1	40 🕫	•
	ila Dar	in the Fact		Chan	Taala Daal	ter Itale							Soapl	UI 5.6.0											•	00
9	Empty	SOAP	REST	import	Save All	Forum	, () Trial	Preferences	<b>е</b> Ргоку	Endpoint Expl	orer									Search Fo	rum			ŵ	0 Online He	elp
<b>6</b>		te				SoapU	I Start F	age																	* t* 🗵	I III
		ts Sample S	DAP Projec	Core		Hi th You're'n Web 1 Usual and o Make San Thanh The S	ere! e gettin tet. With Service sure to Bear. cs! martBe	g this mess; nout an Inte testing. is where you evant inform connect to ar SoapUI Tr	age since met conn a would s nation. the Intern cam	your computer eection, you mig ee the SoapUI s net to get access Project N Create R Create R Create R Create R Relative F	is offline pht experi- itart page. is to all th AP Project a WSDL/SO/ ame: cluster equests:	and SoapU lience some b, which inc he services AP based Pro	UI can't acc e issues wi cludes the s and inforr New SO/ roject in this nple request TestSuite for lie paths in p	cess the hen perform latest new mation from AP Project workspace s for all oper t the importe- project relativ	ning 5 n ations? 4 WSDL ely to proje	Browse t file (require K	es save)	1								spector

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.

Activ	ities 🐵	com-inst	all4j-runtime	launcher-Ur	lixLaunche	ar 🕶			Cts 15:48	¢ (	? 📢 🖌 🔻					
	Eile Proj	ect Suite	e Case Ste	o <u>⊺</u> ools <u>D</u> e	sktop <u>H</u> el	lp										
9	Empty	SOAP	REST Impo	rt Save All	Forum	🛞 Trial	Preferences	Proxy	Endpoint Explorer Search Forum	đà	Online Help					
- 🖒	ъ <b>Ш</b>				Soapt	UI Start I	Page				- c 🛛 🗉					
9	Tegwen	s Sample SO	AP Project Con	1	Hi ti	nere!					spector					
0	You're getting this message since your computer is offline and SoapUI can't access the Internet. Without an Internet connection, you might experience some issues when performing Web Service testing.															
					Usua and	Usually, this is where you would see the SoapUI start page, which includes the latest news and other relevant information.										
					Make Sma	ce sure to connect to the Internet to get access to all the services and information from artBear.										
<b>F</b> z ≪					Than The S	smartBe	ear SoapUI Te	am								
<b>V</b>									New REST Project							
									New REST Project Creates a new REST Project in this workspace							
									URE http://example.com/resource/pat/vlearch/parameter=value							
9									OK Cancel Import WAD							
8																

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 seçime bağlı olarak WADL dosyası istenmektedir.

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

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

#### \* Burpsuite

Burpsuite'te wsdler eklentisi 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.

Not: 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 proxy ayarıyla burp'te açarak bu sorunu aşabiliriz ve test uygulayabiliriz. Burpsuite wsdler eklentisi SoapUI ihtiyacını kaldırmak için, ve SoapUI olmadan burspuite'te soap web servisleri test etmek için geliştirilmiş bir eklentidir.

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.

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

#### \* Netsparker

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	□ ×
Target Website or Web Servio	ce URL	
https://php.testsparker.com/		- 💭 Default -
Options		
Scan Settings	Imported Links	
🔊 General	🕂 Add 🥒 Edit 💥 Delete 📑 Clear 🔍 Searc	ch Import From File • Enter Links
Scope	Method URL	ASP.NET Project File
Additional Websites		Burp
A Imported Links		G Comma Separated Values (CSV)
1 URL Rewrite		Fiddler
Authentication		HTTP Archive
Form		I/O Docs
Basic, NTLM/Kerberos		Netsparker Session File
e Header		<b>OWASP ZAP</b>
Client Certificate		O Postman
Smart Card		RAML
G OAutn2	(i) Scan scope rules will be applied to imported	d lin of OpenAPI (formerly Swagger)
		(  Web Application Description Langu
		Web Service Definition Language (V
		WordPress REST API

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

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

- 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 Servi	ice Scan				• ×
Target Website or Web Service	URL				
https://php.testsparker.com/				÷	🗩 Default 👻
Options					
Scan Settings	Imported				
🖋 General	🕂 Add 🖉	🛚 Edit 🗙 Delete 📑 Cle	ar 🔍 Search	Impo	ort From File - Enter Links
O Scope	Method	URL		ASP	ASP.NET Project File
Additional Websites					Burp
C Imported Links				6	Comma Separated Values (CSV)
W OKL Kewhite				•	Fiddler
Authentication				HUR	HTTP Archive
Form					I/O Docs
Basic, NTLM/Kerberos					Netsparker Session File
🔚 Header				0	OWASP ZAP
Client Certificate				<u>©</u>	Postman
			>	2	RAML
GAULTZ GAULTZ	(i) Scan	scope rules will be applied	to imported lin	3	OpenAPI (formerly Swagger)
			-5	<b>{@}</b> }	Web Application Description Language (WADL)
					Web Service Definition Language (WSDL)
				1	WordPress REST API

# (REST Web Servis Arayüzünü / Kapsamını Dahil Etme)



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

URL listesi belirlenmiş rest web servisi bu şekilde taranabilecektir.

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

- 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 Se	ervice Scan 🗆
Target Website or Web Servi	ce URL
http://rest.testsparker.com/	- 🗾 🧿 🕞 Previous Settings
Options	
Scan Settings	Imported Links
🖋 General	Add / Edit V Delete 🕞 Clear O Search Import From File - Enter Links
Scope	
🚷 Additional Websites	Method URL
🔗 Imported Links	
🧭 URL Rewrite	
<u> Pre-Request Script</u>	
Shark (IAST)	
Authentication	
Form	
🔑 Basic, NTLM/Kerberos	
🔚 Header	
Client Certificate	
Smart Card	
2 OAuth2	
Ҟ Manual	<ol> <li>Scan scope rules will be applied to imported links during the scan.</li> </ol>
	Crawl and Wait 👻 Cancel

(Ham Http Talebi Yükleme 1)

(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. Ayrıyetten 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 testleri pratik uygulaması bu dökümanda uygulama başlığı altında gösterilmiştir.

# \* 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 talepleri kullanılarak testler yürütülebilir.

#### \* Wireshark

Web servisi tüketen / kullanan uygulamanın trafiği dinlenerek ve hedef web servis adres filtrelemesine gidilerek web servis talep paketleri "follow tcp stream" ile elde edilebilir ve bu şekilde ham paket burpsuite'e örneğin atılarak güvenlik testleri yürütülebilir veya Netsparker'a örneğin atılarak sadece belirtilen ham paket üzerinden otomatize saldırı testleri uygulanabilir. Bu yöntemde kapsam elde edildiği kadardır ve testler elde edilebilen kapsam kadar uygulanır.

## Bir Tecrübe:

Bir saha görevinde \*SK'da bilgisayarda wireshark açılmıştır ve akan paketler içerisinde post metotlu bir paket görülmüştür. Bakıldığında xml gövdeli bir paket olduğu anlaşılmıştır ve soap xml node'ları yer almaktadır. O paketteki soap xml node'larından bilgisayarın arkaplanda uzaktaki bir web servisle konuştuğu paket olduğu anlaşılmıştır. Pakete sağ tık yapıp Follow->TCP Stream yaparak talep paketi kopyalanmıştır ve Burpsuite'te repeater'a yapıştırılmıştır. Paket burp'te repeater'da gönderildiğinde yanıt olarak başarılı bir soap yanıt mesajı dönmüştür. Dolayısıya pakete burpsuite'te sağ tık yapıp Intruder yapılarak testler genişletilebilir veya Scan ile otomatize tarama yapılabilir. Bu şekilde wireshark'tan elde edilen paketler kapsamınca Burpsuite'te testler yürütülebilir. Veya paket Netsparker'a atılarak otomatize testler yürütülebilir.

## \* Proxy

Web servisi tüketen / kullanan uygulamanın haberleştiği web servis adresi için işletim sistemi /etc/hosts dosyasından karşılık olarak localhost girilerek ve uygulama trafiği lokalde burpsuite'e bu şekilde yönlendirilerek uygulamadan gelen xml talep paketlerini kurcala ve gönder ile güvenlik testleri yürütülebilir. Bu yöntemde kapsam elde edildiği kadardır ve testler elde edilebilen kapsam kadar uygulanır.

#### i. Web Servis Ek Notlar

- Burpsuite WSDL Wizard eklentisi hedef soap web servisinde wsdl keşfi çalışması yapmaktadır.

- ASP.NET web servisler web sunucuda .asmx uzantısı kullanmaktadırlar.
- Endpoint URL web servisin nerede erişilebilir olduğunu ifade eder.

## Uygulama [SoapUI Yazılımı ile SOAP Web Servis Test Etme]

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Bu uygulamada SoapUI kullanılarak SoapUI tutorials'lardaki demo soap web servisi projesi açılacaktır ve soap web servisi testi yapılacaktır.

Gereksinimler

Ubuntu 18.04 LTS	// Ana Makine
SoapUI	// Web Servis Test Yazılımı
Burpsuite	// Proxy Yazılımı

SoapUI yazılımının kurulumu şu şekildedir:

// Download

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

(Kurulum dosyası Downloads klasöründe yer almaktadır: SoapUI-x64-5.6.0.sh)

// Install

Ubuntu 18.04 LTS Terminal:

> sudo su
> chmod +x SoapUI-x64-5.6.0.sh
> ./SoapUI-x64-5.6.0.sh

(Kurulumda home dizinine kurulum yapılır, ve Tutorials da yüklemeye dahil edilir. Tutorials'da soap ve rest için örnek soapui projeleri mevcut )

Kurulum sonrası yazılımı başlatma şu şekildedir:

// Run

Ubuntu 18.04 LTS:

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

(Email kaydı skip'lenebilir)

Çıktı:

Ella Breiast Suite Case Step Teels Desister			oapUI 5.6.0	
The Holect Sole case Step Tools Desktor	p <u>H</u> elp			
Empty SOAP REST Import Save All Fe	🔽 🞯 🔅	ces Proxy Endpoint Explorer		Search Forum
SoapUl	l Start Page			రి లో 🗵
Browth month         Book         Hithe You're Internet Wees S         Hithe You're Internet Wees S           Usual and ot Make + Smither The Sr         Smither You're Smither The Sr           Worksake Projection         Weeks You're Projekty         Value Projekty	Istart Page are! extended to the message e et. Without an internet with the relevant informable are to connect to the bear. si martibear SoapUI Tean	since your computer is offline and SoapUI can't acce connection, you might experience some issues when add see the SoapUI start page, which includes the lat control of the soapUI start page, which includes the lat control of the soapUI start page of the soapul term of the soapUI start page of the soapul result. Request Authentication & Header + Add header Don't show this winder on taurch	s the performing est news where the set of	2 0 ° °

(SoapUI Açılır)

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

SOAP Örnek Web Servisi SoapUI Proje Dosyası Konumu: /home/hefese/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.

Activitie	s 🐵 com-	install4j-r	untime-la	uncher-Uni	xLaunche	r <b>*</b>							Cts 16:43		6	6	ç 40 F	-
.=												5	SoapUI 5.6.0				•	D 😣
E	e Project	Suite Ca	se Step	<u>T</u> ools <u>D</u> es	ktop <u>H</u> elp	p												
• 🧿	Empty SO/	P REST	Import	Save All	Forum	Srial	Prefer	<b>¢</b> rences	о Ргоху	Endpoint Explorer				Search Forum		iii)	0 Online He	lp
• 🍅 🛓	III Desile sta					So	apUI SI	tart Pag	9 ((()))								rt ⊠	Sul 1
		a SOAP Provide SoapBi login 32º login q logout 32º logout seearch 32º search buy 32º buy q ple TestSu tSuite fails anded Tes viceSoapBi logout search buy	iject Core inding rq rq ifte if we don't ifSuite inding Mock	get faults Service	k	כ)	1	Servic Operatio	Pro	inding MockService	equ AfterReq							spector
	а	)				Sat Sat Sat Sat	Aug 07 Aug 07 Aug 07 Aug 07 Aug 07 Aug 07	Message 16:34:15 16:34:15 16:34:15 16:34:15 16:34:49	TRT 2021 TRT 2021 TRT 2021 TRT 2021 TRT 2021 TRT 2021	ITIDEBUG:Senaing reqt ItIDEBUG:Receiving res ItIDEBUG:Connection C ItIDEBUG:Connection C	uest: PUST /accoun sponse: HTTP/1.12 can be kept alive in or [Account creatio 0.0.0.0:48514<->12	creati 00 OK definite n.acco 7.0.0.	ationTusemama=jonn&password=wujsvavudus HTTP/1.1 K itely counterationSubmit RegistrationForm] in 9ms (254 bytes) 0.18690 closed	 				

Activities 🧕 com-install4j-runtime-launcher-UnixLaunch	er * CCS 1645 SoapUI 5.6.0	ت ال ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال ع ال ال ال ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ال عن ا
Elle Project Suite Case Step Iools Desktop H Empty SOAP REST Import Save All Forum	elp Trail Preferences Proy Trail	Search Forum 🗎 🛞 Online Help
Project Super Project Core     Project Super Project Core     Project Super Project Core     Project Super Super Project Core     Project Super Super Project Core     Project Super	SoapUI Start Page	er d" 🗹
	Des Pro Star OnRequ AfterReq Des Pro Star Star OnRequ AfterReq Des AfterReq Message Log 	

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 )

Activ	ities	8 com-ins	tall4j-runi	time-laur	cher-Unix	Launcher	-					Cts 16:49				<b>\$</b>	. 후 🕪 🖌	•
. 🚍												SoapUI 5.6.0					• •	b 😣
	<u>F</u> ile P	roject Sui	te Case	Step <u>I</u>	ools <u>D</u> esk	ctop <u>H</u> elp												
9	Empt	ty SOAP	REST	1mport	Save All	Forum	🛞 Trial	Preferences	<b>B</b> Proxy	Endpoint Explor	er				Search Forum	6	a 🕜	lp
		ets Sample S ⇒ Service ⇒ C log ⇒ Service ⇒ Ser	OAP Project aSoapBindi in loggin rq out loggut rq search rq buy rq TestSuite soapBindi out arch y soapBindi out	t Core ng we don't g ite ng MockSe	et faults ervice			ogin rq soaperv: En soaperv:	L S relope xm ader/> dy>         	(http://127.0.0.1.96 (http://127.0.0.1.96 (http://topsevords/ equilational states/ equilational BUmockServiceSoapl Prechesses unitsoap or	Binding rg/soap/envelape/*	xalnı:came*http://ww	Haw AML	sessenvi Enveloge value i cogeni-http://schesa.valuea <pre> <pre> <pre> <pre> <pre> <pre> </pre> </pre> </pre> </pre> </pre> </pre>	org/somp/envelope/*	v <sup>6</sup> t <sup>4</sup> t <sup>4</sup> ▼ ± + ⊕ xalns:sss= •	P Inspector	
8							AL	th Headers	0) Attac	hments (0) WS-A	WS-RM JMS Headers	JMS Property (0)		Hea	aders (5) Attachments (0) SSL info WSS (0) JMS (0)			
							resp	onse time: 66i	ns (274 b)	ytes)							1:1	11

(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 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.



( 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"e çift 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.



Dönen pakette geçersiz hesap bilgisi hatası yer almaktadır. Buradaki hata ifadesini brute force / dictionary saldırısında flag olarak alabiliriz ve denenen olası hesaplardan başarısız olanlar bu flag'i tick'lesin, başarılı olan ise bu flag'i 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.

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		
1 × 2 ×		
Target Positions Payloads Options		
<pre> Payload Positions Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to p positions - see help for full details. Attack type: Cluster bomb POST /mockServiceSoapBinding HTTP/1.1 Accept-Encoding: gip, deflate Content-Type: text/wml;charset=UTF-B SOAPAction: "http://www.soapul.org/sample/login" Content-Length: 283 Host: 127.0.0.1:8088 User-Agent: Apache-HttpClient/4.5.5 (Java/11.0.11) Connection: close <soapenv:ebuder></soapenv:ebuder> <soapenv:ebuder></soapenv:ebuder> <soapenv:hedder></soapenv:hedder> <soapenv:hedder></soapenv:hedder> <soapenv:hedder></soapenv:hedder>  <soapenv:hedder></soapenv:hedder>  <td>ayload</td><td>Start attack</td></pre>	ayload	Start attack
? < + > Type a search term	0 matches	Clear
2 payload positions	Length: 562	

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:      Payload set:      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.         Paste       abc         abc       yz         Load       yz         Clear       Login         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
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	
$1 \times 2 \times \dots$	
Target Positions Payloads Options	
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 set, and each payload type can be customized in different ways.       Start attack         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.	-
past23 Load 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	
Remove Vp Down	
Payload Encoding	- L

( Olası Parolalar Listesi İkinci Payload Olarak Belirlenir )

Jurp Intruder Repeater Winder Repeater Sequence Decoder Compare Extender Project options User options Alerts   I a unitaria   Target Poations Payloads Options   Itarget Poations Payloads Options Itarget Poations Payloads Options Itarget Poations Payloads Options Itarget Poations Payloads Options Itarget Poations Payloads Options Itarget Poations Payloads Options Itarget Poations Payloads Options Itarget Poations Itarget Poations Payloads Options Itarget Poations Payloads Itarget Poations Itarget Poations Payloads Itarget Poations Itarget	Burp Suite Community Edition v1.7.36 - Temporary Project 🛛 🖱 🛛
Target Provy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options Mers     1 2     Target Postons Payloads Options   Intruder Store requests Store requests Store requests Store store model to service mode (no results) Store full payloads These settings can be used to flag result items containing specified expressions. If Plag result items used to flag result items containing specified expressions. If Plag result items three porses matching these expressions: Invalid Login Match type: Simple string Remove Remove Cleare settings can be used to extract useful information from responses into the attack results table. Extract the following items from responses: These settings can be used to extract useful information from responses into the attack results table. Extract the following items from responses:	Burp Intruder Repeater Window Help
Image: Positions     Target Positions     Pattack Results     Image: Positions     Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts</td>	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Terget Positions Payloads Options     Image: Attack Results   Image: These settings control what information is captured in attack results.   Image: Store requests   Image: Store requests   Image: Store full payloads   Image: These settings can be used to flag result items containing specified expressions. Image: These settings can be used to flag result items containing specified expressions. Image: These settings can be used to flag result items containing specified expressions. Image: These settings can be used to flag result items containing specified expressions. Image: These settings can be used to flag result items containing specified expressions. Image: These settings can be used to flag result items containing specified expressions. Image: These settings can be used to flag result items containing specified expressions. Image: These settings can be used to flag result items containing specified expressions. Image: These settings can be used to expression: Image: These settings can be used to expression: Image: These settings can be used to express the set to expression: Image: Case sensitive match Image: Case sensitive match Image: Case sensitive match Image: Case sensitive match Image: Case sensitive match Image: Case sensitive can be used to extract useful information from responses into the attack results table. Image: The sensitive can be used to extract useful information from responses into the attack results table. Image: The sensitive can be used to extract useful information from responses into the attack results table. Image: The sensitive can be used to extract useful information from responses into the attack results table. Image: The sensitive can be used to extract useful information from respon	
Attack Results These settings control what information is captured in attack results. Store requests Store requests Wake unmodified baseline request Use denial-of-service mode (no results) Store full payloads Cerep - Match These settings can be used to flag result items containing specified expressions. If lag result items with responses matching these expressions. If lag result atems with responses matching these expressions. If lag result items with responses matching these expressions. Invalid Login Match type: Remove Clear Add invalid Login Match type: Simple string Regex Case sensitive match Cises sensitive match Exclude HTTP headers Strict the following items from responses into the attack results table. Extract the following items from responses:	Target Positions Payloads Options
<ul> <li>Chees estings control what information is captured in attack results.</li> <li>These estings control what information is captured in attack results.</li> <li>Store requests</li> <li>Store requests</li> <li>Make unmodified baseline request</li> <li>Use denial-of-service mode (no results)</li> <li>Store full payloads</li> </ul> ? Grep - Match ? Grep - Match ? Hag result items containing specified expressions. <ul> <li>I have settings can be used to flag result items containing specified expressions.</li> <li>Paste</li> <li>Invalid Login</li> <li>Match type: © Simple string</li> <li>Regex</li> <li>Case sensitive match</li> <li>Schucke HTTP headers</li> </ul> ? Grep - Extract ? Grep - Extract ? These settings can be used to extract useful information from responses into the attack results table. Extract the following items from responses:	Attack Desuits
<ul> <li>Store requests</li> <li>Store responses</li> <li>Make unmodified baseline request</li> <li>Use denial-of-service mode (no results)</li> <li>Store full payloads</li> </ul> ? Grep - Match ? Grep - Match ? These settings can be used to flag result items containing specified expressions. ? If lag result items with responses matching these expressions. ? If lag result items with responses matching these expressions. ? If lag result items with responses matching these expressions. ? Grep - Match ? Clear ? Load ? Match type: Imvail Login Match type: Imvailed Login ? Grep - Extract ? Grep - Extract ? Grep - Extract ? These settings can be used to extract useful information from responses into the attack results table Extract the following items from responses:	These settings control what information is captured in attack results.
<ul> <li>Observations</li> <li>Store responses</li> <li>Make unmodified baseline request</li> <li>Use denial-of-service mode (no results)</li> <li>Store full payloads</li> </ul> <b>Grep - Match W</b> These settings can be used to flag result items containing specified expressions. <ul> <li><b>V</b> Flag result items with responses matching these expressions.</li> <li><b>V</b> Flag result items with responses matching these expressions.</li> <li><b>V</b> Flag result items with responses matching these expressions.</li> <li><b>V</b> Flag result items with responses matching these expressions. <ul> <li><b>Paste</b></li> <li><b>Invalid Login</b></li> <li>Match type:</li> <li><b>Simple string</b></li> <li><b>Regox</b></li> <li><b>Cases ensitive match</b></li> <li><b>Exclude HTTP</b> headers</li> </ul> <b>Grep - Extract These settings can be used to extract useful information from responses into the attack results table. <b>Extract the following items from responses:</b></b></li></ul>	C Store requests
<ul> <li>Wake unmodified baseline request</li> <li>Use denial-of-service mode (no results)</li> <li>Store full payloads</li> <li>Cerp - Match</li> <li>These settings can be used to flag result items containing specified expressions.</li> <li>Flag result items with responses matching these expressions:</li> <li>Paste</li> <li>Invalid Login</li> <li>Remove</li> <li>Clear</li> <li>Add</li> <li>Invalid Login</li> <li>Match type:  Simple string <ul> <li>Regex</li> <li>Exclude HTTP headers</li> </ul> </li> <li>Circip - Extract</li> <li>These settings can be used to extract useful information from responses into the attack results table.</li> <li>Extract the following items from responses:</li> </ul>	Store responses
<ul> <li>Use denial-of-service mode (no results)</li> <li>Store full payloads</li> <li>? Grep - Match</li> <li>? These settings can be used to flag result items containing specified expressions.</li> <li>? Paste Invalid Login</li> <li>Load</li> <li>Paste Invalid Login</li> <li>Match type: ● Simple string</li> <li>@ Regex</li> <li>Case sensitive match</li> <li>? Exclude HTTP headers</li> <li>? Grep - Extract</li> <li>? These settings can be used to extract useful information from responses into the attack results table.</li> <li>? Extract the following items from responses:</li> </ul>	☑ Make unmodified baseline request
<ul> <li>Grep - Malch</li> <li>These settings can be used to flag result items containing specified expressions.</li> <li>✓ Flag result items with responses matching these expressions:</li> <li>✓ Paste</li> <li>Invalid Login</li> <li>Load</li> <li>Clear</li> <li>Add</li> <li>Invalid Login</li> <li>Match type: ② Simple string</li> <li>○ Regex</li> <li>Clease sensitive match</li> <li>✓ Exclude HTTP headers</li> <li>✓ Grep - Extract</li> <li>✓ These settings can be used to extract useful information from responses into the attack results table.</li> <li>Extract the following items from responses:</li> </ul>	Use denial-of-service mode (no results)
Grep - Match These settings can be used to flag result items containing specified expressions. I Flag result items with responses matching these expressions: Paste Invelid Login Remove Lead I valid Login Match type: @ Simple string @ Regex Case sensitive match I 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:	Store full payloads
?       Grep - Match         Image: These settings can be used to flag result items containing specified expressions.         Image: Plag result items with responses matching these expressions:         Image: Plag result items with responses matching these expressions:         Image: Plag result items with responses matching these expressions:         Image: Plag result items with responses matching these expressions:         Image: Plag result items with responses matching these expressions:         Image: Plag result items with responses matching these expressions:         Image: Plag result items with responses matching these expressions:         Image: Plag result items with responses         Image: Plag result items items responses         Image: Plag result items items responses         Image: Plag result items responses         Image: Plag result items responses         Image: Plag result items responses         Image: Plag result items responses         Image: Plag result items responses         Image: Plag result items responses	
These settings can be used to flag result items containing specified expressions.	P Grep - Match
Flag result items with responses matching these expressions:   Paste Invalid Login   Load Remove   Clear Add   Match type: Simple string   Regex Case sensitive match   Exclude HITP headers <b>Grep - Extract</b> These settings can be used to extract useful information from responses into the attack results table. Extract the following items from responses:	These settings can be used to flag result items containing specified expressions.
Paste       Invalid Login         Load       Remove         Clear          Add       invalid Login         Match type: ● Simple string          ● Regex          □ Case sensitive match          ● Exclude HTTP headers          ②       Grep - Extract         ③       These settings can be used to extract useful information from responses into the attack results table.         ● Extract       Extract the following items from responses:	☑ Flag result items with responses matching these expressions:
Paste       Invalid Login         Remove       Clear         Add       Invalid Login         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:       Total	
Load         Remove         Clear         Add         Match type: ② Simple string         ③ Regex         ○ Case sensitive match         ✓ Exclude HTTP headers         ② Grep - Extract         ③ These settings can be used to extract useful information from responses into the attack results table.         ③ These settings can be used to extract useful information from responses into the attack results table.         ③ These settings can be used to extract useful information from responses into the attack results table.	Paste Invalid Login
Remove   Clear   Add   Invalid Login   Match type:     Simple string   Regex   Case sensitive match   Exclude HTTP headers     Care - Extract   These settings can be used to extract useful information from responses into the attack results table.   Extract the following items from responses:	Load
Clear         Add         Imvalid Login         Match type: ② Simple string         ③ Regex         Case sensitive match         ✓ Exclude HITP headers         Ø         Grep - Extract         ③         These settings can be used to extract useful information from responses into the attack results table.         Extract the following items from responses:	Remove
Clear         Add         Invalid Login         Match type: @ Simple string         @ Regex         Case sensitive match         @ Exclude HITP 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       Invalid Login         Match type: <ul> <li>Simple string</li> <li>Regex</li> <li>Case sensitive match</li> <li>Exclude HTTP headers</li> </ul> Image: Case sensitive match           Image: Case sensitive match           Image: Case sensitive match           Image: Case sensitive match           Image: Case sensitive match           Image: Case sensitive match           Image: Case sensitive match           Image: Case sensitive match           Image: Case sensitive match         Image: Case sensitive match           Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match           Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match           Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitive match         Image: Case sensitetee         Image: Case sensitive match	Clear
Add       Invalid Login         Match type: <ul> <li>Simple string</li> <li>Regex</li> <li>Case sensitive match</li> <li>If Exclude HTTP headers</li> </ul> Grep - Extract            These settings can be used to extract useful information from responses into the attack results table.            Extract the following items from responses:	
Match type:	Add Invalid Login
Case sensitive match  Exclude HTTP headers  Case Sensitive match  Exclude HTTP headers  Case Sensitive attack  Extract  Extract  Extract  Extract the following items from responses:  Extract the follo	Match type:   Simple string
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:	Regex
Case sensitive match  Exclude HTTP headers  Case sensitive HTTP headers	Case constitue motel
	Case sensitive match
Grep - Extract     These settings can be used to extract useful information from responses into the attack results table.     Extract the following items from responses:	
These settings can be used to extract useful information from responses into the attack results table. Extract the following items from responses:	Cron - Extract
These securitys can be used to extract useful mormation from responses into the attack results table.     Extract the following items from responses:	and presented and a start of the formation for the start back while the start of th
Extract the following items from responses:	Inese settings can be used to extract userul information non responses into the attack results table.
	Extract the following items from responses:
Add	bbA

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

Burp Sulte 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	
Request Headers       Start attact         Image: These settings control whether intruder updates the configured request headers during attacks.       Image: These settings control whether intruder updates the configured request headers during attacks.         Image: These settings control whether intruder updates the configured request headers during attacks.       Image: These settings control whether intruder updates the configured request headers during attacks.         Image: These settings control whether intruder updates the configured request headers during attacks.       Image: These settings control whether intruder updates the configured request headers during attacks.         Image: These settings control whether intruder updates the configured request headers during attacks.       Image: These settings control whether intruder updates the configured request headers during attacks.         Image: These settings control whether intruder updates the configured request headers during attacks.       Image: These settings control whether intruder updates the configured request headers during attacks.         Image: These settings control whether intruder updates the configured request headers during attacks.       Image: These settings control whether intruder updates the configured request headers during attacks.         Image: The control whether intruder updates the configured request headers during attacks.       Image: These setting control whether intruder updates the configured request headers during attacks.         Image: The control whether intruder updates the configured request headers during attacks.       Image: The control whetheres the control whetheres the control whetheres	< ^
Request Engine     These settings 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	
Number of retries on network failure: 3	
Pause before retry (milliseconds): 2000	
Throttle (milliseconds):	- 1
Variable: start 0 step 30000	
Start time:      Immediately	- 1
In 10 minutes	- 1
O Paused	- 1
<ul> <li>Attack Results</li> <li>These settings control what information is captured in attack results.</li> <li>Store requests</li> <li>Store responses</li> <li>Make unmodified baseline request</li> <li>Use denial-of-service mode (no results)</li> <li>Store full payloads</li> </ul>	
P Grep - Match	
These settings can be used to flag result items containing specified expressions.	

( Saldırı Başlatılır )

Burp Suite Community Edition v1.7.36 - Temporary Project															
Burp	Intruder Rep	peater Window Help						_							
Targ	et Proxy !	Spider Scanner Intrud	er Repeater Sequencer	Decoder Comparer	Extender Proj	ect options U	Iser options Alerts								
1 ×	2 ×					_									
Targ	et Positions	Attack Sava Calumna		Intruder at	саск 1			908							
2	Request H	Results Target Posi	tions Rayloads Ontions						Start attack						
	These settin	The state of the s							Start attack						
G	✓ Update C	Filter: Showing all items						(2							
	Opdate     Request     Payload1     Payload2     Status     Error     Timeout     Length     Invalid Login     Comment       Image: Status     Status     Status     Error     Timeout     Length     Invalid Login     Comment														
	21         deneme         deneme123         200         489         V           20         qwerty         Login123         200         489         V         •														
2	Request E	19 Login	Login123	2	00		503 🗌								
	These settin	18 xyz	Login123	2	:00		489 🗹								
G	Natas Cama	16 deneme	Login123	2	:00		489 🗹								
	Note: Some	15 qwerty	parola12*	2	.00		489 🗹	$\mathcal{I}$							
	Number of t	14 Login 13 XV7	parola12* parola12*	2	00		489 🗹 489 🗸								
	Number of n	12 abc	parola12*	2	:00		489 🗹								
	o	11 deneme	parola12*	2	:00	- 4	489 🗹	The second second second second second second second second second second second second second second second se							
	Pause befor 10 nwerty nass123 200 489														
	Throttle (mill	Request Response													
		Raw Headers Hex	XML												
		HTTP/1.1 200 OK						A							
	Start time:	Content-Type: text/x	nl; charset=utf-8												
		Connection: close													
		Server: Jetty(6.1.26	)												
	_	<soapenv:envelope td="" xm<=""><td>lns:soapenv="http://sch</td><td>emas.xmlsoap.org/so</td><td>pap/envelope/"</td><td></td><td></td><td></td><td></td></soapenv:envelope>	lns:soapenv="http://sch	emas.xmlsoap.org/so	pap/envelope/"										
?	Attack Re	<soapenv:body></soapenv:body>	<pre>«.soapu1.org/sample/ &gt;</pre>												
(4)	These settin	<pre><soapenv:fault> <faultcode>Client</faultcode></soapenv:fault></pre>	faultcodes												
	Store rec	<pre><faultstring>Alread;</faultstring></pre>	/ Login												
	Store res	<pre><details +="" 2="" <="" \s="" pre=""></details></pre>	Type a search term					0 matches							
	🗹 Make unr		Type a search term					omatches							
	🗌 Use deni	Finished	•												
	Store full	l payloads													
?	Grep - Ma	itch							-						
L	These settin	as can be used to flag res	ult items containing specified	expressions.											

(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.

#### Uygulama [SoapUI Yazılımı ile SOAP Web Servis Test Etme 2]

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Bu uygulamada SoapUI yazılımı kullanılarak kasıtlı zafiyetler içeren DVWS web servisine ait bir ders sayfasında sunulan WSDL dosyası alınacaktır ve DVWS'nin ilgili sayfasında işlevsel soap web servisini test etme gösterilecektir.

Gereksinimler

Ubuntu 18.04 LTS	// Ana Makine
SoapUI	// Web Servis Test Yazılımı
Burpsuite	// Proxy Yazılımı
DVWS - Windows 7 Home Premium VM	// Hedef Web Servisi - Sanal Makine

Not: SoapUI kurulumu ve başlatma Uygulama [SoapUI Yazılımı ile SOAP Web Servis Test Etme] başlığında bahsedilmiştir.

Not: Kasıtlı zafiyetler içeren DVWS web servisi outdated olduğundan sadece eski php versiyon 5.5.38'de her sayfası düzgün çalışırdır. Bu nedenle XAMPP php 5.5.38 kurulumu ile DVWS web servisi DVWS - Windows 7 Home Premium sanal makinesinde yayındadır.

Örneğin DVWS web servisinin bir ders sayfasında wsdl enumeration saldırısı senaryolaştırılmıştır ve sayfanın dediği üzere dvws'nin arka ucundaki soap web servisin WSDL dosyasının elde edildiği varsayılmaktadır. Bu wsdl dosyasının url'si ders sayfasında verilmiştir:





SoapUI yazılımına bu soap web servisin wsdl dosyasını verelim ve soap web servisin arayüzünü / kapsamını görelim.







Activiti	es 🔞 com-ins	all4j-run:	time-lau	ncher-Un	ixLaunche	r •			Pzt 09:36 👘		<b>? 4</b> 0	÷ •						
. ==					SoapUI 5.6.0													
• E	ile Project Suit	e Case	Step I	ools <u>D</u> e	sktop <u>H</u> elp	p												
0	Empty SOAP	REST	1mport	Save All	Forum	🛞 Trial	Preferences	<b>В</b> Ргоху	Endpoint Explorer Search Forum	âb	0nline	Help						
· 🏠 👌				#	DVWA Web	o Servic	e Binding				ಕರ್	<b>X</b> 5						
	Projects			OV	erview Se	ervice En	idpoints WSDL	Content	WS-I Compliance			pec						
		Web Servin ck_user_in Request 1 Julation Request 1 urn_price	e Binding	V	WSDL Defi WSDL URL Namespace Binding	nition	file:/h dvwa DVW/	file/home/hefese/Desktop/ren/ce.xml Owarwebsen/ce DVWA Webser/ce/Binding										
-	E Sample Si	AP Projec	t Core		Style		BPC	1.1										
A					WS-A version	n	NONE											
-					Definition	Parts												
Z					service.xml		file:/h	iome/hefe	sejDesktop/service.xml									
				V	Operation	s												
					Name		Use	One	Action									
					heck_user_	id	SOAP	false	http://192.168.71.1.2/dvws/vulnerabilities/ws/dienum/service.php/check_user_id									
					Return_price	9	SOAP	false	http://bit.com/s/loanara.aumer									
	Interface Proper	ies																
. 🔞	Property		Value															
	Name Description Definition URL Binding SOAP Version Cached Style WS-A version WS-A anonymol	file:/hu {dvwa SOAP true RPC NONE us optior	Web Servi ome/hefes webservio 1.1															
	Properties			So	apUI log ht	ttp log	jetty log error	log wsrn	i log memory log									

Bu adımlar neticesinde dvws'deki soap web servisin arayüzü / kapsamı yüklemesi ile örnek xml talepleri sol sütunda sıralanır: check\_user\_id, Population, Return\_price. Sol sütundaki request 'lere tıklanıldığında gönderilmeye hazır xml talepleri açılacaktır.



Burada SoapUI ayarlardan proxy ayarı girerek gönderilen paketi yakalayabilir ve Burpsuite'te Intruder'a göndererek çeşitli güvenlik testleri uygulanabilir. SoapUI'de proxy ayarı girmek için;



Activiti	es 🐵 com-inst	all4j-rur	ntime-lau	ncher-U	nixLaunch	er 🔻		_		_	Pzt 09:53				<u>)</u> 🧳	. 🤋 📢 🕖 ∙
-											SoapUI 5.6.0					
E	ile Project Suit	e Case	Step ]	ools [	esktop <u>H</u>	elp										
9	Empty SOAP	REST	1mport	ليًا Save A	ارتی Forum	🛞 Trial	Preferences	e Proxy	Endpoint	Explorer				Search Forum		Online Help
📩 🛯	] ==			S	Request	1										66 X
in the	Projects				🐓 🎲 🖸	0 🛓 🗄	🖇 🔳 🛛 http://192	.168.71.1	2/dvws/vulner	abilities/wsdlen	um/service.php					- = + 🕖
0	🗄 🤁 DVWA V	Veb Servi	ce Binding	5	🗄 «soapen	v:Envelo	pe xmlns:xsi="ht	tp://ww	.w3.org/2001	/XMLSchema-ins	stance" xmlns:xsd="http://www.w3.org/2001/XM		-ENV:Envelope SOAP-ENV:enc	odingStyle="http://schemas.xmlsoa	p.org/soap/encoding/"	xmlns:SOAF
		ck_user_i	d	2.00	E <soa< td=""><td>penv:nea penv:Bod</td><td></td><td></td><td></td><td></td><td>SoapUI Preferences</td><td></td><td></td><td>😣 ="http://schemas.xmlsom</td><td>p.org/soap/envelope/"</td><td>&gt;</td></soa<>	penv:nea penv:Bod					SoapUI Preferences			😣 ="http://schemas.xmlsom	p.org/soap/envelope/"	>
	⊜-¢ Pop	ulation		8		<name< td=""><td>SoapUI Prefe</td><td>rences</td><td></td><td></td><td></td><td></td><td></td><td>2.</td><td></td><td></td></name<>	SoapUI Prefe	rences						2.		
	- 20 Pat	lequest 3			50</td <td>apenv:Bo</td> <td>Set global Soa</td> <td>pUI settin</td> <td>gs</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	apenv:Bo	Set global Soa	pUI settin	gs							
	SO F	Request 3			<td>nv:Envel</td> <td>HTTP Settings</td> <td></td> <td></td> <td>Proxy Setting</td> <td>a: O Automatic</td> <td></td> <td></td> <td>▲</td> <td></td> <td></td>	nv:Envel	HTTP Settings			Proxy Setting	a: O Automatic			▲		
<b>.</b>	Sample SC	AP Proje	ct Core				Proxy Settings				O None					
24							WSDL Settings			Host:	localhost	-				
E							Editor Settings			Port:	8080	-2				
$\sim$							Tools WS-I Settings			Excludes:						
T I							Global Propertie	s		Username						
-01							WS-A Settings	Settings		Password:		_				
							Global Sensitive Version Update	Informati Settings	on Tokens							
							AlertSite Conne	ctor Plugi	n							
The second																
1																
3																
8																
•																
3																
2																
2																
	Request Propertie	15												-		
0	Property	1	/alue							•			V			
_	Name Description	Reque	st 1				•						OK	Cancel		
	Message Size Encoding	414 UTE-8														
	Endpoint	http://	92.168													
	Bind Address				1							1				• e
	Follow Redirects Username	true			Auth Head	lers (0)	Attachments (0)	WS-A V	VS-RM IMS H	aders IMS Pro	pperty (0)	Headers	(9) Attachments (0) SSL In	fo WSS (0) IMS (0)		
	Password			- re	sponse time	: 38ms (!	549 bytes)									8 : 20
	Properties				oopi II log	http.log	ietty log_error	log wern		log						

adımları takip edilir ve sonra ekrandaki xml talep ve yanıt penceresindeki yeşil butonla xml talebi gönderilir. Bu yapıldığında talebi localhost 8080 portunu dinleyen burpsuite alacaktır.





Yakalanan paketi repeater'a gönderelim ve yanıt paketlerini gözlemleyerek güvenlik testini uygulayalım.



(Not: Check\_User\_ID arguman değerleri kasıtlı zafiyetler içeren dvws web servisinin pdf dökümanından elde edilmiştir. Bkz. /var/www/dvws/Attacking Damn Vulnerable Web Services.pdf )

Bu şekilde burp'te talep paketinin gövdesindeki node'ların değerleri ile, paketin başlıkları ile, ve url'de yer alan parametreler ile oynanarak çeşitli güvenlik testi adımları uygulanabilir.

## Uygulama [SoapUI ile Rest Web Servis Test Etme]

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Bu uygulamada SoapUI yazılımı kullanılarak kasıtlı zafiyetler içeren DVWS web servisindeki bir ders sayfasında sunulan rest web servisini test etme yolu gösterilecektir.

Gereksinimler

// Ana Makine
// Web Servis Test Yazılımı
// Proxy Yazılımı
// Hedef Web Servisi - Sanal Makine

Not: SoapUI kurulumu ve başlatma Uygulama [SoapUI Yazılımı ile SOAP Web Servis Test Etme] başlığında bahsedilmiştir.

Not: Kasıtlı zafiyetler içeren DVWS web servisi outdated olduğundan sadece eski php versiyon 5.5.38'de her sayfası düzgün çalışırdır. Bu nedenle XAMPP php 5.5.38 kurulumu ile DVWS web servisi DVWS - Windows 7 Home Premium sanal makinesinde yayındadır.

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 soapui'ye arayüz / kapsam bu bir url ile yüklenecektir.

Öncelikle dvws web servisindeki ilgili sayfaya göz atalım.



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







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

SoapUI yazılımı ile REST web servisini bu arayüzü / kapsamı göstererek test edelim ve sql enjeksiyonu açıklığını tespit edelim.



Activiti	es 🗵	om-inst	all4j-runi	time-lau	ncher-Uni	xLauncher	*						Pzt 10:54						<b>v</b>	₹ 4≬ Ø ▼
. 🚍													SoapUI 5.6.0							000
	Empty Project	SOAP	REST	Step I	Save All	ktop <u>H</u> elp Forum pUI Start I	Trial	Preferences	Proxy	Endpoint E	Explorer						Search Forum	Try ReadyAPI	#	Online Help
							N6 N6 	ew SOAP Pr ew REST Pro The State of ipare 15 min he 2021 Stat o help us id rends in the ake The Su	oject of API S ns to take te of API S entify ma, industry.	urvey part in urvey or	All Ree Critical Creates a URI: http://	AddyAPI now supports to addyAPI now supports to the streaming platform eate test saseritons to a file endpoints with the More T project I with the stream of the stream (/192168.71.12/dws)	JPPORT esting for Apache Kaña. errity your ever REST Project athis workspace	G Sc Ri Sc Ar t	iet Started with Soapt ource EST API Sample Project OAP API Sample Project sers/2 import WADL	JI Open	Resources Test a REST API Test a SOAP API 10 Tips for Beginn Documentation Community Get Certified	ers		

Hedef web servisi tanımlama dosyası WADL sunmadığından sadece bir url ile arayüz / kapsam girilir ve Ok denir. Böylece örnek bir talep paketi oluşacaktır. Bu paket gönderilerek hedef web servisine talep yapılır ve yanıt döner.

Activiti	es 🗵 co	om-insta	ll4j-runI	ime-lau	ncher-U	nixLaunch	er 🔻						Pz	t 10:55					، 🧋	<b>?</b> €	e 👻
													Soap	UI 5.6.0							) 🗇 😣
E	ile Projec	ct Suite	Case	Step <u>I</u>	ools <u>D</u>	esktop <u>H</u> e	ilp														
- 💿	•	532 H 87	85 B 51	+	Ð	þ	1	•	0	Endpoin	Explorer						c	earch Forum	â	(2	į.
	Empty	SOAP	REST	Import	Save A	Forum	Trial	Preferences	Proxy											Online	Help
• 🍅 🗦					RE	Request	1													ೆ ದೆ	<b>X</b> 5
and a second	Projects	ST Projec	t 1			Met	hod	Endpoint					Resour	ce				Parameters		- 18 +	a Pec
		http://19	2.168.71	1.12		GET		http://192.168	.71.12				- /dvws/	ulnerabilities	/sqli/api.php/u	sers/2	2				_   9
		- 2 [/d	ws/vulne	rabilities/	lest .	+× *		· •								S ML					All .
0		L RE	Reques	t 1	Reg	·	Name		V	alue		Style		Leve	el	NO					
	🕀 🛅 Sa	mple SOA	P Project	Core												S					
					8											ITML					
-																1					
A																Ra					
E																					
144																					
8																					
• 🔍																					
Sec.																					
1																					
S																					
0																					
-																					
• 4						Required:		Sets if param	neter is re	quired											
						Type:						Ŧ									
• 🚬	4				Þ	Options:					Add										
	Reques	st Params									Edit										
• 🧐		Reques	t Propert	ies	_						Remo	ve									
	Pro	perty	Paquaet	alue							-										
	Descript	tion	request																		1 11 -
	Encoding	g it	http://19	92.168		Disable Er	codina:	Disables URL	-Encoding	of the paran	neter value										
	Timeout	drage						_													ě
	Follow Re	edirects	true			Auth Head	Headers (0) Attachments (0) Representations (0) IMS Headers IMS Properties (0) Headers (0) Attachments (0							eaders (0) Attachments (0) SSI Info. Benri	esentations (0) Schema IMS (0)			-			
	Usernam	ne rd				adri neau	na neuvora (a) neuvonana (a) nepraderkeuvora (a) pro neuvora pro neuvora (a) neuvo							sectored (b) scheme (c)		1:1	_				
	Bronor	rtine			ű –		http://og	isthules arres	100 more		e lea										
	rioper	1162			2	oaporiog	nech ind	percy log error	iog wsn	nog memo	.yy										



Şimdi 2 parametresine sql enjeksiyonu payload'ları girelim ve açıklık var mı tespit edelim.

Girilen Payload 1: '





# Girilen Payload 2: 1



Girilen Payload 3: 50-ASCII(1)


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 yine 1 kaydı yanıt olarak dönecektir. 1 payload'u ile 50-ASCII(1) payload'u aynı çıktıyı verdiğinden demek ki ASCII() sql ifadesi çalışmıştır. Sql enjeksiyonu açıklığı var tespiti sonrası sql ifadeleri uygun şekilde girilerek sql enjeksiyonu gerçekleştirilebilir.

Bilgi:

Netsparker ile bu rest web servis url'si taranmıştır (bkz. Uygulama [Netsparker ile REST Web Servis Test Etme]) ve uygun payload'lar ile veritabanı ismi, sürümü, veritabanı kullanıcısı gibi bilgiler elde edilmiştir.

Eğer WADL, OpenAPI (Swagger),... v.b. REST web servise ait arayüz / kapsam dosyası olsaydı bu arayüz / kapsam dosyası SoapUI'ye yüklendiğinde sol sütunda örnek talepler listelenecekti ve ona göre rest web servis güvenlik denetimleri uygulanabilecekti.

# Uygulama [Burpsuite WSDLER Eklentisi ile Soap Web Servis Test Etme]

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Bu uygulamada burpsuite'in wsdler eklentisi yardımıyla dvws kasıtlı zafiyetler içeren web servisinin bir ders sayfasındaki arka uçta yer alan hedef soap web servisi test edilecektir.

Gereksinimler

Ubuntu 18.04 LTS Burpsuite, Wsdler Plugin DVWS - Windows 7 Home Premium // Ana Makina // Güvenlik Testi Aracı // Web Servisi - Sanal Makine

Not: Kasıtlı zafiyetler içeren DVWS web servisi outdated olduğundan sadece eski php versiyon 5.5.38'de her sayfası düzgün çalışırdır. Bu nedenle XAMPP php 5.5.38 kurulumu ile DVWS web servisi DVWS - Windows 7 Home Premium sanal makinesinde yayındadır.

Öncelikle Burpsuite'e Wsdler eklentisini kuralım.



Bu kurulum sonrası Wsdler sekmesi burpsuite menülerine gelecektir.



Hedef dvws web servisinin ilgili sayfasına bir göz atalım.

Activ	ties 🛛 单 Firefox Web Browser 🔻	Paz 15:53	، چ	÷ 4		
	WSDL Enumeration × ©	3 Settings × +			00	
0	$\leftrightarrow$ $\rightarrow$ C $\textcircled{a}$	○ 월 192.168.0.37/dvws/vulnerabilities/wsdlenum/         □ ☆		$\bigtriangledown$	<b>0</b> =	
6	Home					
		WSDL Enumeration				
	ADOUL	Most SOAP services are deployed to process requests given by a user through a web application. In common scenarios, the WSDL file is not exposed to the public. However, if an attacker can access an application's WSDL file numerate and and look for hidden services used by the web andication.	le, he can try	to		
0	Setup Instructions	WSDL enumeration aims to discover non-public web services by retrieving their WSDL file.				
	PHP mormation	More Information				
	Vulnerabilities	https://www.owasp.org/index.php/Testing_WSDL_(OWASP-WS-002)				
E	WSDL Enumeration	http://www.ws-attacks.org/index.php/WSDL_Disclosure     The balance from pulmeting under to be prepared by the balance Child base to view the WCDL of the application     The balance from pulmeting under to be prepared by the COAD consistence Child base to view the WCDL of the application				
	XML Bomb Denial-of-Service	The between this statute to be processed by the back white Solar service. It is to scal the work, the and non-init other requests being processed by the Solar service click field to were where work, or the application. Smartphone OS Market Share				
Y	XML External Entity Injection	OAndroid Cios				
		Owindows Phone Oothers				
9		Submit Query				
9						
0	REST API SQL Injection					
	XML External Entity Injection 2					
. 👂						
• •						

DVWS'nin bu sayfasında arka uçta 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)

Activ	ities 🔰 com-install4j-runtime-launcher-UnixLauncher 👻	Paz 13:57	¢ (	Y 4
. 🚍	- 192.168.0.37/dvws/vulne × 😒 Settings × +			
0	← → × @ O & 192.168.0.37/dvws/vulnerabilities,	/wsdlenum/service.php?wsdl		
		Burp Suite Community Edition v1.7.36 - Temporary Project		0 😣
· 😂	This XML file does not appear to have any style information associate	Burp Intruder Repeater Window Help		
		Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Wsdler		
9	- <definitions targetnamespace="dywa:webservice"></definitions>	Intercept HTTP history WebSockets history Options		-
0	- <types></types>	Pequart to http://10.150.0.27.00		_
•	- <xsd:schema targetnamespace="dvwa:webservice"> <xsd:import http:="" namespace="http://schemas.ym/soan.org/soan&lt;/p&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;xsd:import namespace=" schemas.xmisoap.org="" th="" wsdl<=""><th>Forward Drop Intercept is on Action Comment this item</th><th></th><th>2</th></xsd:import></xsd:schema>	Forward Drop Intercept is on Action Comment this item		2
		Raw Params Headers Hex		
		CET /dvus/vulnerabilities/wsdlenum/service.php?wsdl HTTP/1.1		1
	<pre></pre>	Host: 192.1081.0.37 Uber-Adent: Mozilla/5.0 (X11: Linux X85 64: rv:91.0) Gecko/20100101 Firefox/91.0		- 11
Fz		Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,#/*;q=0.8		- 11
~	- <message name="Return_priceResponse"></message>	Accept-Language: en-US,er;q=U.S Accept-Encoding: qzib. deflate		- 11
۲¢	<pre><pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> <pre> &lt;</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>	Peferer: http://j92.168.0.37/dvws/vulnerabilities/wsdlenum/		- 11
	<pre>-<message name="check user idReguest"></message></pre>	Connection: close Uparade_Insecure-Requests: 1		- 11
•	<pre><part name="username" type="xsd:string"></part></pre>	Cache-Control: max-age=0		- 11
				- 11
9	- <message name="cneck_user_idkesponse"></message>			- 11
-				- 11
	- <message name="PopulationRequest"></message>			- 11
6	<pre><part name="value_one" type="xsd:string"></part></pre>			- 11
-				- 11
0	<pre><pre>cinessage name= ropulation(esponse &gt;</pre></pre>			- 11
				- 11
0	- <pre>-<porttype name="DVWA Web Service PortType"></porttype></pre>			- 11
•	<pre>-<operation name="keturn_price"></operation></pre>			- 11
	<output message="tns:Return priceResponse"></output>			- 11
<b>-</b>				- 11
2	- <operation name="check_user_id"></operation>			- 11
_	<ul> <li><ul> <li><ul> <li><ul></ul></li></ul></li></ul></li></ul>			- 11
				- 11
	- <operation name="Population"></operation>			- 11
	<input message="tns:PopulationRequest"/>			- 11
				- 11
				- 11
	- - binding name="DVWA Web Service Binding" type="tns:DVWA			- 11
	<soap:binding 192.168.0.37="" dvws="" http:="" style="rpc" th="" transport="http://schemas.xmlsor&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;_&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;soap:operation soapAction=" vul<=""><th>2 &lt; + &gt;</th><th>0 mate</th><th>ches</th></soap:binding>	2 < + >	0 mate	ches
	192 168 0 37			

(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 Suite	Communi	ity Edition	v1.7.36 - T	emporary Proje	ct			😑 🗉 😣
Burp Intruder Repeater Window H	ielp								
Target Proxy Spider Scanner	Intruder Repeater Sequencer D	Decoder	Comparer	Extender	Project options	User options	Alerts	Wsdler	
Intercept HTTP history WebSock	kets history Options								
Request to http://192.168.0.37:8	80								
Forward Drop Intercept is on Action								:	
Raw Params Headers Hex									
GET /dvws/vulnerabilities/wsdl	lenum/service.php?wsdl HTTP/1.1								4
User-Agent: Mozilla/5.0 (X11;	Linux x86_64; rv:91.0) Gecko/20	100101 F	irefox/91	.0					
Accept: text/html,application/	/xhtml+xml,application/xml;q=0.9	,image/w	ebp,*/*;q	=0.8					
Accept-Language: en-US,en;q=0. Accept-Encoding: gzip. defl	.D Cand to Caider		1						
Referer: http://192.168.0.3	De en estáre scen								
Connection: close	Send to Intruder	Ctrl+I							
Cache-Control: max-age=0	Send to Repeater	Ctrl+B							
	Send to Sequencer								
	Send to Comparer								
	Send to Decoder								
	Request in browser	•							
	Parse WSDL								
	Engagement tools [Pro version only]	Þ							
	Change request method								
	Change body encoding								
	Copy URL								
	Copy as curl command								
	Copy to file								
	Paste from file								
	Save item								
	Don't intercept requests	Þ							
	Do intercept	►							
	Convert selection	Þ							
	URL-encode as you type								
	Cut	Ctrl+X							
	Сору	Ctrl+C							
	Paste	Ctrl+V							
	Message editor help								
	Proxy interception help								
			-						
									v
? < + > Type a se	earch term								0 matches

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

Burp Suite Community Edition v1.7.36 - Temporary Project	- 8
Burp Intruder Repeater Window Help	
Target Prove Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Wsdler	
Intercept HTTP history WebSockets history Options	
Request to http://192.168.0.37:80	
Forward         Drop         Intercept is on         Action         Comment this item	- 1
Raw Params Headers Hex	
Host: 192.168.0.37 Wer-Agent: Wozilla/5.0 (X11; Linux x86_64; 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:-Encoding: gzip, deflate Referer: http://J92.168.0.37/dvws/vulnerabilities/wsdlenum/ Connection: close Upgrade-Insecure-Requests: 1] Cache-Control: max-age=0	
? < + > Type a search term	0 matche

( 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 Sui	te Commu	nity Editio	n v1.7.36 - T	emporary Proje	ct	<b>e</b> 🖲 🗧
Burp Intruder Repeater Window	Help ar Untruder	Beneater	Sequencer	Decoder	Comparer	Extender	Project options	Liser ontions Alerts Wedler	
service * service *	ar minudur	Repeater	ocquencer	Becoder	comparer	Enconder	rioject options	Cool options / Nerto	
Operation			Binding					Endpoint	
Beturn price check user_id Population			DVWA W	eb Service   leb Service   leb Service	Binding Binding Binding			http://192.168.0.37/dws/ulnerabilite http://192.168.0.37/dws/ulnerabilite http://192.168.0.37/dws/vulnerabilitie	: Wedlenum/Senvice.php s/wedlenum/Service.php s/wedlenum/Service.php
Request Raw Params Headers Hex	XML					<u></u>			
OST /dvws/vulnerabilities/ >wser-Agent: Mozilla/S.O (X11 &ccept: taty/hum, application &ccept-iencoding gzip, defla %eferer: http://102.1080.0.37 Connection: close gupgrade_insecure-Requests: 1 Zache-Control: max-age=0 SUMPAction: http://102.1080.0 SUMPAction: http://102.1080.0 Sumpaction: http://102.1080.0 Sumpaction: http://102.1080.0 Sumpaction: http://102.1080.0 Sumpactions: http://102.1080.0 Su	sdlenum/se sdlenum/se n/xhtml+xm 0.5 te /dvws/vuln .37/dvws/v et=UTF-8	rvice.php H 6_64; rv:9 l,applicat: erabilitie: ulnerabili	HTTP/1.1 1.0) Gecko, ion/xml;q≓ s/wsdlenum ties/wsdlen	/20100101 D.9,image, / num/servid	Firefox/9 /webp,*/*; ce.php/Ret	1.0 q=0.8 urn_price			
<pre>soapenv:Envelope xmlns:xsi= mlns:soapenv="http://schema <soapenv:header></soapenv:header> <soapenv:body></soapenv:body></pre>	"http://ww s.xmlsoap. encodingSt :string">g	w.w3.org/20 org/soap/er yle="http:, ero et <td>001/XMLSch nvelope/"&gt; //schemas. ne&gt;</td> <td>ema-instar xmlsoap.or</td> <td>nce" <mark>xmlns</mark> rg/soap/en</td> <td>:xsd="http coding/"&gt;</td> <td>://www.w3.org,</td> <td>/2001/XMLSchema*</td> <td></td>	001/XMLSch nvelope/"> //schemas. ne>	ema-instar xmlsoap.or	nce" <mark>xmlns</mark> rg/soap/en	:xsd="http coding/">	://www.w3.org,	/2001/XMLSchema*	

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 sayfasının sunduğu ekrandaki radio button'ların name attribute'unlarından elde edilmiştir).

Bu şekilde testler uygulanarak gelen yanıtlar izlenebilir ve bir 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.

## Uygulama [Burpsuite ile Rest Web Servis Test Etme]

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Bu uygulamada burpsuite ile kasıtlı zafiyetler içeren dvws web servisinin bir ders sayfasındaki arka uçta yer alan hedef rest web servisi test edilecektir. Not: Bu uygulama Burpsuite'in resmi sayfasında rest web servisleri test etme makalesinde uygulama olarak gösterilmektedir. (bkz. https:// portswigger.net/support/using-burp-to-test-a-rest-api)

Gereksinimler

Ubuntu 18.04 LTS Burpsuite DVWS - Windows 7 Home Premium // Ana Makina // Güvenlik Testi Aracı // Web Servisi - Sanal Makine

Not: Kasıtlı zafiyetler içeren DVWS web servisi outdated olduğundan sadece eski php versiyon 5.5.38'de her sayfası düzgün çalışırdır. Bu nedenle XAMPP php 5.5.38 kurulumu ile DVWS web servisi DVWS - Windows 7 Home Premium sanal makinesinde yayındadır.

Öncelikle dvws web servisindeki ilgili sayfaya bir göz atalım.



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.

Activities 🔰 com-install4j-runtime-launcher-UnixLauncher 👻	Paz 14:27	<b>\$</b>	6.94
• 192.168.0.37/dwws/vulne × 1© Settings × +			
← → X	ies/sqli/api.php/users/2		
("first name":"Gordon" "last name":"Brown")	Burp Suite Community Edition v1.7.36 - Temporary Project		
·	Burp Intruder Repeater Window Help		
	Target Prov Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts W	sdier	
<b>9</b>	Intercept HTTP history WebSockets history Options		
0	Request to http://192.168.0.37:80		
	Forward Drop Intercept is on Action	omment this item	
	Raw Headers Hex		
	GET /dvws/vulnerabilities/sqli/api.php/users/2 HTTP/1.1		-
	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0		
	Accept: text/ntml,application/xntml+xml,application/xml;qm0.9,image/webp,*/*;qm0.8 Accept-Language: en-US,en;q=0.5		
8	Accept-Encoding: gzip, deflate Referer: http://192.168.0.37/dvws/vulnerabilities/sqli/		
	Connection: close		
····	Cache-Control: max-age=0		
0			
6			
0			
U			
1 S S S S S S S S S S S S S S S S S S S			
5			
12.1			
			1
			omatches

(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 Payload: '



## Girilen Payload: 1



Girilen Payload: 50 - ASCII(1)

Burp Suite Community Ed	ition v1.7.36 - Temporary Project 🛛 🗎 🔿 🔿
Burp Intruder Repeater Window Help	
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comp	arer Extender Project options User options Alerts Wsdler
Go Cancel <   Y >   Y	Target: http://192.168.0.37 🖉 ?
Request	Response
Raw Headers Hex	Raw Headers Hex
<pre>GET /dws/vulnerabilities/sqli/api.php/users/50-ASCII(1) HTTP/1.1 Host: 192.168.0.37 User-Agent: Mozilla/5.0 (X1; Linux X86_64(0):91.0) Gecko/20100101 Firefox/91.0 Accept: Accept: Accept: accept</pre>	<pre>HTTP/1.1 200 0K Date: Sat. 14 Aug 2021 17:56:25 OMT Server: Apacher2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38 X-Powered-By: PHP/5.5.38 Content-Length: 43 Connection: close Content-Type: text/html {"first_name":"Darth","last_name":"Vader"}</pre>
?     +     >     Type a search term     0 matche       Done	s ? < + > Type a search term 0 matches 246 bytes   14 millis

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 demek ki ASCII() sql ifadesi çalışmıştır. Sql enjeksiyonu açıklığı var tespiti sonrası sql ifadeleri uygun şekilde girilerek sql enjeksiyonu gerçekleştirilebilir.

Bilgi:

Netsparker ile bu rest web servis url'si taranmıştır (bkz. Uygulama [Netsparker ile REST Web Servis Test Etme]) ve uygun payload'lar ile veritabanı ismi, sürümü, veritabanı kullanıcısı gibi bilgiler elde edilmiştir.

Bu şekilde Burpsuite ile rest web servisi güvenlik testleri uygulanabilir.

## Uygulama [Netsparker Yazılımı ile Soap Web Servis Test Etme]

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

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

Gereksinimler

Ubuntu 18.04 LTS	// Ana Makina
Netsparker	// Güvenlik Testi Aracı
DVWS - Windows 7 Home Premium	// Hedef Web Servisi - Sanal Makine

Not: Kasıtlı zafiyetler içeren DVWS web servisi outdated olduğundan sadece eski php versiyon 5.5.38'de her sayfası düzgün çalışırdır. Bu nedenle XAMPP php 5.5.38 kurulumu ile DVWS web servisi DVWS - Windows 7 Home Premium sanal makinesinde yayındadır.

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 Serv	vice Scan	o x
Target Website or Web Service	2 URL	
http://192.168.0.15/dvws/	- 💭 📀 Previous	Settings 👻
Options		
Scan Settings	Scan Policy	
🔑 General	Default Security Checks	· · · · · · · · · · · · · · · · ·
Scope	Periodic Security Checks	
🚷 Additional Websites	Report Policy	
餐 Imported Links	Default Report Policy	····
🍪 URL Rewrite	Custom Cookies	
<u> Pre-Request Script</u>		
), Shark (IAST)		
Authentication	Hedef Soap Web	<b>V</b>
🔚 Form	Crawling Servis	
Basic, NTLM/Kerberos	✓ Find & Follow New Links	
🔚 Header	Crawl & Attack at the Same Time	
Client Certificate	Incremental Scan	
5 Smart Card	incremental scan	
OAuth2		
😢 Manual		
	Crawl and Wait 👻	Cancel

Daha sonra hedef soap web servisin arayüzünü / kapsamını yükleyelim.





Start a New Website or Web Serv	ice Scan	• ×
Target Website or Web Service	URL	
http://192.168.0.15/dvws/	👻 💭 💽 Previous S	Settings 👻
Options		
Scan Settings	Imported Links	
🖋 General	O Add ✓ Edit X Delete S Clear Q Search Import From File - Entremain Clear C Search Import From File - Entremain Clear C Search Import From File - Entremain Clear C Search Import From File - Entremain Clear C Search Import From File - Entremain Clear C Search Import From File - Entremain Clear C Search Import From File - Entremain C Search Import From File - Entremain Clear C Search Import From File - Entremain C Search Import From File - Entr	er Links
Scope	Method UBI	
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	
左 Pre-Request Script		
🍌 Shark (IAST)		
Authentication	2	
📔 Form		
🔑 Basic, NTLM/Kerberos		
🔚 Header		
Client Certificate		
💼 Smart Card	1 3 link(s) successfully imported.	×
OAuth2		
📌 Manual	(i) Scan scope rules will be applied to imported links during the scan.	
	Crawl and Wait *	Cancel

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.

Start a New Website or Web Servic	ce Scan		
Target Website or Web Service U	JRL	Edit 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/servic	e.php
🖋 General	🗗 Add 🥒 Edit 🕽	Enabled Type 🛓 Name 🛓 Value	Encoded
Scope		Headers	
🚷 Additional Websites	Method URL	✓         Header → Host         192.168.0.15	
Imported Links (3)	POST http://1	Header         SOAPAction         "http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php/Return_price"	
💮 URL Rewrite	POST http://1		
💁 Pre-Request Script		Desket	
), Shark (IAST)		Header	
Authentication 1			
📔 Form			
Basic, NTLM/Kerberos		<soap:body soap:encodingstyle="http://schemas.xmlsoap.org/soap/encoding/"> <return_price></return_price></soap:body>	<b>^</b>
🔚 Header		<pre><name xsi:type="xsd:string">_NS_</name>  </pre>	
Client Certificate			
Smart Card			<b>T</b>
OAuth2	Scan scope rul	C Enable Raw Request Body	
Manual	U scan scope fui	Save	Cancel
		Crawl and Wait	Status

( Eklenen Birinci Örnek XML Talep Paketi )

Start a New Website or Web Service Scan		
Tanat Website on Web Cardina UDI	Edit Link	×
Target website or web Service UKL		
http://192.168.0.15/dvws/	Builder Raw Hex View	
Options	POST - HTTP - 192.168.0.15 80 C /dvws/vulnerabilities/wsdlenum/service.	.php
Scan Settings	in Enabled Type 🛓 Name 🛓 Value	Encoded
🖉 General	E v Headers	
♦ Scope	Header - Host 192,168,0.15	
Additional Websites Method	U V Header - SOAPAction "http://192.168.0.15/dvws/vulnerabilities/wsdlenum/service.php/check_user_id"	✓
Imported Links (3)     POST	ht	
GURL Rewrite	ht	
💁 Pre-Request Script	Packet	
),, Shark (IAST)	Header	
Authentication		
Form	<pre><soap:body soap:encodingstyle="http://schemas.xmlsoap.org/soap/encoding/"> </soap:body></pre>	
🔑 Basic, NTLM/Kerberos	<username xsitype="xsd:string">_NS_</username>	
🔁 Header	<pre>  </pre>	
🔂 Client Certificate		) <b>•</b>
Smart Car	✓ Enable Raw Request Body	
2 OAuth2		
🍄 Manual 🧭 Scan s	co Save	Cancel
	Crawl and Wait + Cancel Overall Activity	Status

# ( Eklenen İkinci Örnek XML Talep Paketi )

Start a New Website or Web Service Scan		Edit Link					×
Target Website or Web Service URL							
http://192.168.0.15/dvws/		Builder R	aw Hex V	ïew			
Options-		POST -	HTTP	+ 192.168.0.1	5	80 🗘 /dvws/vulnerabilities/wsdlenum/servic	e.php
Scan Settings	orted Links	Enabled	Type 🐘	Name 🖹	Value		Encoded
🖉 General	dd 🥜 Edit 🗙	✓ Headers					
♦ Scope		$\checkmark$	Header 👻	Host	192.168.0.15		
Additional Websites	hod URL	✓	Header 👻	SOAPAction	"http://192.168.0.15/dvws/vulne	rabilities/wsdlenum/service.php/Population"	✓
C Imported Links (3)	I http://1		*				
IRL Rewrite POS	T http://1						<u> </u>
🚽 Pre-Request Script 🖌						Packet	
), Shark (IAST)		1				Header	
Authentication	/						
E Form		<soap:body <populatio< td=""><td>soap:encodi n&gt;</td><td>ingStyle="http://</td><td>schemas.xmlsoap.org/soap/enco</td><td>ding/"&gt;</td><td></td></populatio<></soap:body 	soap:encodi n>	ingStyle="http://	schemas.xmlsoap.org/soap/enco	ding/">	
Basic, NTLM/Kerberos		<value_or< td=""><td>ne xsi:type="</td><td>xsd:string"&gt;_NS_</td><td></td><td>Packet</td><td></td></value_or<>	ne xsi:type="	xsd:string">_NS_		Packet	
🔚 Header		<td>y&gt;</td> <td></td> <td></td> <td>Body</td> <td></td>	y>			Body	
Client Certifi		<td>ope&gt;</td> <td></td> <td></td> <td><u> </u></td> <td>· ·</td>	ope>			<u> </u>	· ·
Smart Card		Cenable Rav	v Request Bo	dy			
2 OAuth2						Save	Cancel
😢 Manual 💋	Scan scope rul	_	_			Jure	
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.



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.

n 🍗 🖞 🖲 🔹 🔤 sa	an Tools Link Tools		192.168.0.15 - Netsparker 6.0.2.30446			<sup>0</sup> ≜ ≁ -	ø x
File Home View Reporting Help	Scan Link D Search					🙃 Sign-	in to Enterprise -
🔈 🚯 📑 🖆	) 🖆 🚺 🦉	3 ڬ					
Controlled Send to Request Go to Identification Copy UI Scan Builder Page Tools	RL Copy as Google Internet Mic CURL Chrome Explorer E Copy Open in Bros	crosoft Mozilla idge Firefox wser					
🔜 Sitemap - Previous Settings 🛛 🕸 🗙	HTTP Request / Response 🔒 Bi	rowser View 🛄 Knowledge Base Viewer				- 🍿 Knowledge Base (18)	8 ×
▼• 🔄 • 🕙 • 🔳 • Enter text to search 👂	Find: Enter text to search	Clear 🔄 Previous 🏵 Next 🔡 Save Report				😚 AJAX / XML HTTP Requests [2]	
<ul> <li>✓ 53 192.168.0.15:80/dvvs/ (94)</li> <li>✓ 56 dvvs</li> <li>✓ 67 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li> <li>✓ 70 dvvs</li></ul>	🚯 Web Servi	ces (SOAP)			(i) INFORMATION	Comments [142] Cookies [1] Crawling Performance [14]	
→ C33 jβ vuherabilities → modi biddendir → biddendir ↓ Tarama	SOAP Web Services found in Settings and make sure you	n the target application. You can use the para have selected <b>Exact</b> as the match type.	neter name listed here to provide a default value	while attacking. To add a default value, pleas	e use Form Values in your Scan Policy	Email Addresses [1]  File Extensions [6]  Interesting Headers [1]  Inconstruing Files [6]	
👌 🖬 🖓 Kapsamında 🔒	Operation	Parameter				MIME Types [12]	
> issif	abaali uuus Id	(anany Paus) and [1] (asany Badu [1] (a		,		Not Founds [28]	
v Servicephp	Reputation	/soap:Envelope[1]/soap:Body[1]/	consistion[1]/value one[1]/text()[1]	2		Scan Performance [1]	
ST 2vsdl	Population	/scap.Envelope(1)/scap.Body(1)/				(©) Site Profile [1]	
> Post <name></name>	Return_price	/scap:Enverope[1]/scap:Body[1]/F	decurn_price[1]/name[1]/text()[1]			Slowest Pages (10)	
value_one>	DVWA Web Service					Web Pages With inputs [1]	
(Described Craw site Research For	Operation	Parameter				Web Services (SOAP) [2]	
<ul> <li>[Possible] Phishing by Navigatin</li> </ul>	check_user_id	/soap:Envelope[1]/soap:Body[1]/o	heck_user_id[1]/username[1]/text()[1	1			_
> a xmlbomb	Population	/soap:Envelope[1]/soap:Body[1]/H	Population[1]/value_one[1]/text()[1]			Soap Web Serv	visi
s 🐂 yet 🔻	Return_price	/soap:Envelope[1]/soap:Body[1]/F	teturn price[1]/name[1]/text([1]			Tespit Edildi Bilgici	
Issues - Previous Settings     If a constant to courch						Diigisi	
<ul> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li> <li>Signature</li></ul>							
Out-of-date Version (Apache)     Password Transmitted over HTTP     Password Transmitted over HTTP     Out-of-date Version (Bootstrap) [Variations: 2]     Out-of-date Version (Query) (Variations: 3]     Cout-of-date Version (Query) (Variations: 2]							
> Minternal Server Error [Variations: 8]	Activity				3	×	
Possible] Cross-site Request Porgery (Variab      Possible] Internal IP Address Disclosure	Method Target	Parameter	Duration Current Activity	Overall Activity	Status		
Possible] Phishing by Navigating Browser Ta	Crawling [4]						
> Mining Output Detected	POST http://192.168.0.15/dvws/v     GFT http://192.168.0.15/dvws/v	vulnerabilities/xxe2/se (value=DVWS)	1s 1s		Loading (DOM/JS) Parsing (DOM/JS)		
Programming Error Message     Version Disclosure (Anache)	GET http://192.168.0.15/dvws/v	vulnerabilities/xpath/?	1 s		Loading (DOM/JS)		
> Version Disclosure (NuSOAP)	GET https://192.168.0.15/dvws/	/vulnerabilities/cmdi/	15		Analyzing		
O Content Security Policy (CSP) Not Implement     Missing X-XSS-Protection Header [Variations							
> 9 Referrer-Policy Not Implemented [Variations:							
<ul> <li>V SameSite Cookie Not Implemented [Variation</li> <li>Apache Web Server Identified</li> </ul>							
> f Directory Listing (Apache) [Variations: 8]							
Email Address Disclosure     A Scoeth CT Security Header Errors and Warnin	Activity 🗠 Progress 📗 Logs (	23)				🍿 Knowledge Base (18)   Netspar	ker Assistant (2)*
Auto save finished successfully - 7/17/2021 11:13:49 AM		Crawling (1/3) 6%	Previous Settings - 📄 Default Security Checks - 🔚 Default I	Report Policy - 🔒 1 🏴 1 🏴 10 🏓 49 🌵 37	22 VDB update check failed. Please check your i	nternet connection and logs for details.	Proxy: System
📲 🕾 😋 遒 🧐 🚍 🟥	· · · · · · · · · · · · · · · · · · ·					^ 1 d∎ 1 RQ 7/	17/2021

#### 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 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.

## Uygulama [Netsparker Yazılımı ile Rest Web Servis Test Etme]

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

Gereksinimler

Ubuntu 18.04 LTS	// Ana Makina
Netsparker	// Güvenlik Testi Aracı
DVWS - Windows 7 Home Premium	// Hedef Web Servisi - Sanal Makine

Not: Kasıtlı zafiyetler içeren DVWS web servisi outdated olduğundan sadece eski php versiyon 5.5.38'de her sayfası düzgün çalışırdır. Bu nedenle XAMPP php 5.5.38 kurulumu ile DVWS web servisi DVWS - Windows 7 Home Premium sanal makinesinde yayındadır.

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.



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.

tart a New Website or Web Se	ervice Scan	
Target Website or Web Servi	ice URL	
http://192.168.0.36/dvws/		👻 戻 Previous Settings 🕤
Options		
Scan Settings	Scan Policy Default Security Checks	• ×
🗘 Scope 🚡 Additional Websites	Report Policy	
Imported Links URL Rewrite Pre-Request Script	Default Report Policy Custom Cookles	•
Muthentication	Crawling	
Form Basic, NTLM/Kerberos	✓ Find & Follow New Links Crawl & Attack at the Same Time	
Client Certificate	Pause Scan After Crawling	
2 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.

tart a New Website or Web Se	ervice Scan							U	,
Target Website or Web Servi	ce URL								
http://192.168.0.36/dvws/						- 📕	Prev	ious Settings	5 -
Options									
Scan Settings	Imported	l Links							
🖉 General	• Add	/ Edit 🗙	Delete 🗟	5 Clear 🔾	Search	Import F	rom File •	Enter Links	5
🔿 Scope	Mathead	LIDI			-			-	7
Additional Websites	Method	UKL							
Market Links		Luuuuuuu							
ORL Rewrite     Dea Deavent Spirit									
Shark (IAST)									
Shark (IAST)									
Authentication	-								
Form									
Basic, NILM/Kerberos								2	,
Client Certificate									
Smart Card									
OAuth2									
Ø Manual	(i) Scan	scope rule	s will be a	plied to in	ported lin	ks during	the scan		
0									
· · · · ·						Start Sc	an	- Canc	el

(Web Servis Arayüz / Kapsam Yükleme Ekranına Gidilir)



(Endpoint URL'i Girilir)

http://192.168.0.36/dvws/   Options- ican Settings   General   Scope   Additional Websites   Imported Links (1)   URL Rewrite   Pre-Request Script   Shark (IAST)   Wthentication   Form   Basic, NTLM/Kerberos   Header   Client Certificate   Smart Card   OAuth2   Manual   (1) Scan scope rules will be applied to imported links during the scan.	Target Website or Web Servi	ce URL
Options   ican Settings   General   Scope   Add / Edit Delete Clear Search Import From File - Enter Links   Imported Links (1)   Imported Links (1)   URL Rewrite   Pre-Request Script   Shark (IAST)   Wthentication   Form   Basic, NTLM/Kerberos   Header   Client Certificate   Smart Card   OAuth2   Manual	http://192.168.0.36/dvws/	✓
Scan Settings   General   Scope   Additional Websites   Imported Links (1)   URL Rewrite   Pre-Request Script   Shark (IAST)   wthentication   Form   Basic, NTLM/Kerberos   Header   Client Certificate   Smart Card   OAuth2   Manual     Imported Links     Imported Links     Imported Links (1)     URL Rewrite     Pre-Request Script   Shark (IAST)     Imported Links (1)     Imported Links (1)     Imported Links (1)     URL     Get Http://192.168.0.36/dvws/vulnerabilities/sqli/api.php/users/2     Imported Links (1)     Imported Links (1)     URL     Get Http://192.168.0.36/dvws/vulnerabilities/sqli/api.php/users/2     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)     Imported Links (1)<	Options	
General         Scope         Additional Websites         Imported Links (1)         URL Rewrite         Pre-Request Script         Shark (IAST)         Wathentication         Form         Basic, NTLM/Kerberos         Header         Client Certificate         Smart Card         OAuth2         Manual	Scan Settings	Invested Date
<ul> <li>Scope</li> <li>Additional Websites</li> <li>Imported Links (1)</li> <li>URL Rewrite</li> <li>Pre-Request Script</li> <li>Shark (IAST)</li> <li>uthentication</li> <li>Form</li> <li>Basic, NTLM/Kerberos</li> <li>Header</li> <li>Client Certificate</li> <li>Smart Card</li> <li>OAuth2</li> <li>Manual</li> <li>Method URL</li> <li>GET http://192.168.0.36/dvws/vulnerabilities/sqli/api.php/users/2</li> </ul>	© General	Add      Edit      X Delete      Clear      Search Import From File      Enter Links
Client Certificate         Smart Card         OAuth2         Manual	Scope Additional Websites Umported Links (1) URL Rewrite Pre-Request Script Shark (IAST) Authentication Form Basic, NTLM/Kerberos Header Clicat Cast Cast	Method URL GET http://192.168.0.36/dvws/vulnerabilities/sqli/api.php/users/2
OAuth2         Manual	Smart Card	i 1 link(s) successfully imported.
	OAuth2 Manual	() Scan scope rules will be applied to imported links during the scan.

(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.

Start a New Website or Web Serv	ice Scan		o x
Target Website or Web Service	URL		
http://192.168.0.36/dvws/		👻 🛒 🛞 Previous	Settings 👻
Target Website or Web Service         http://192.168.0.36/dvws/         Options         Scan Settings         General         Scope         Additional Websites         Imported Links (1)         URL Rewrite         Pre-Request Links (1)         Shark (IAST)         Authentication         Form         Basic, NTLM/Kerberos         Header	URL Rewrite  URL Rewrite  URL Rewrite  Carter Analyzable Heuristic  Block Separators: Analyzable Extensions:  If your website uses URL Rewrit by choosing "Custom" URL Revini crease the coverage.	<ul> <li>► Frevious</li> <li>► Previous</li> <li>► E</li> <li>6</li> <li>3</li> <li>/\$.;!:</li> <li>htm,html</li> <li>te then you should configure the URL Rewrite Rules. This will make scans faster a</li> </ul>	Settings xclusions
<ul> <li>Header</li> <li>Client Certificate</li> <li>Smart Card</li> <li>OAuth2</li> <li>Manual</li> </ul>		2 Start Scan *	Cancel

New ile kural penceresi açılır.

Start a New Website or Web Ser	vice Scan	□ ×
Target Website or Web Service	e URL	
http://192.168.0.36/dvws/	- 🗾 📀 Prev	/ious Settings 👻
Options		
Scan Settings	IIRI Rewrite	
🖉 General	Enabled Custom      Copy Rules	Exclusions
<ul> <li>Scope</li> <li>Additional Websites</li> </ul>	🜞 New 💥 Delete 🔹 🔿 Up 🕑 Down http://example.com	🔀 Test
🔗 Imported Links (1)	Placeholder Pattern RegEx Pattern	
URL Rewrite		
💁 Pre-Request Script		
), Shark (IAST)		
Authentication		
📔 Form		
🔑 Basic, NTLM/Kerberos		
🔚 Header		
Client Certificate	✓ Enable Heuristic Rule Detection	
5 Smart Card	Use placeholder or regular expression patterns to define URL Rew	rite rules.
2 OAuth2	http://example.com/blog/news/welcome-to-my-blog	
💅 Manual	The following placeholder pattern can be used <b>/blog/{category}/</b> More Information	(title)
	Start Scan	

İlgili rest web servis url'si girilir.

Target website or web Servi	ce URL	
http://192.168.0.36/dvws/	- <b>-</b>	Previous Settinas
URL Rewrite Rule		
Configure Sample URL		
Enter a sample URL that r Example: http://www.exa Click Next to continue. URL: http://192.168.0.36/dvv	natches the URL rewrite rule you want to add. mple.com/products/123 vs/vulnerabilities/sqli/api.php/users/2 < Back	Next > Cance
Form		

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.

Target Website or Web Se	rvice URL			
http://192.168.0.36/dvws/ IRI Rewrite Rule			🗸 🧊 ( Prev	ious Settinas
Configure Parameters	5			
i Select the path segment	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	
Diaceholder Dattern: /duws/	vulnerabilities/soli/ani	nhn/users/2		
	vaniciabilities/squ/apiq	n no no		
Regex Pattern: ^/dvws/vuin	ierabilities/sqli/api\.php	/users/2/ (\$		
			< Back Finish	Cance
Manual	More Info	ormation		

http://192.168.0.36/dvws/ URL Rewrite Rule			→  →    (←) Previous Settings
Configure Parameters	5		
Calect the nath segme	ats which contain a par	ametervalue	
U select the path segmen	nts which contain a para		
Is URL Rewrite Parameter?	Parameter Type	Parameter Name	Path Segment
	Any		dvws
	Any		vulnerabilities
	Any		sqli
	Any		api.php
	Any		users
	Any	userID	2
Placeholder Pattern: /dvws/	/vulnerabilities/soli/api.	php/users/{userID}	
PegEv Dattern A/daus/uulr	orabilities (seli (ani) aba	/users/(2 <userid>[A/]+)/2\$</userid>	
Regex Pattern. 700005/000	ierabilities/ squ/ aproprie	/ users/ (1< userio>[ /]+//19	
		[	< Back Finish Cano
Ter 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 Servio	ce URL
http://192.168.0.36/dvws/	👻 🛒 🌔 Previous Settings
Options	
Scan Settings	URL Rewrite
General	🗸 Enabled Custom 🔻 😭 Copy Rules 🕒 Exclusion
O Scope	New Y Delete - A Un Down http://192.168.0.36/dows/
Additional Websites	
C Imported Links (1)	Placeholder Pattern RegEx Pattern
Dec Decivert Seriet	<ul> <li>- records connected in the desired of the second connected by the</li></ul>
Shark (IAST)	
Shark (MST)	
Authentication	
Form	
Basic, NTLM/Kerberos	
E Header	✓ Enable Heuristic Rule Detection
Client Certificate	() Use placeholder or regular expression patterns to define URI Rewrite rules.
Smart Card     OAuth2	For example if the target URL is
Manual	The following placeholder pattern can be used /blog/[category]/(title} More Information
	Start Scan 🔹 Canc

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

n 🐚 🗎 🖲 🔹 🛛 s	an Tools Link Tools Vulnerability Tools	192.168.0.37 - Netsparker 6.0.2.30446		<sup>0</sup> ≜≁ – ø ×
File Home View Reporting Help	Scan Link Vulnerability D Search			🝙 Sign-in to Enterprise -
	b 🗡 😽 😽			
PoC Commands LFI Sho	Names this Scan To Actions Application Firewall			
Tools	Send To WAF Rules			^
Sitemap - Previous Settings 🛛 🕸 🗙	Ullinerability			Netsparker Assistant (2)*     R ×
Y • [≤] • ⊙ • □ • Enter text to search A	COL Intention			Maximum Signature Exceeded 1h ago
- 🔂 client.php -	SQL Injection			Netsparker has detected that some of the visited
v 🔛 (name)				URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan
jsonRPCClient.php	URL : http://192.168.0.37/dvws/vulnerabilities/soli/api.php/users/-	1%20or%201=1%20and%20(SELECT%201%20and%20ROW(1,1)>(SELECT%20		policy is exceeded. This means Netsparker has
jsonRPCServer.php	COUNT(*), CONCAT(CHAR(95), CHAR(33), CHAR(64), CHAR(52), CHAR(100)	,CHAR(105),CHAR(108),CHAR(101),CHAR(109),CHAR(109),CHAR(97),	CLASSIFICATION	exact same path for those URLs.
process.php	0x3a,FLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.COLLATION	5%20GROUP%20BY%20x)a)	PCI DSS 2 2 65 1	You can increase Maximum Signature value in
server.php	Parameter Name : USenID		OWASP 2013	your Scan Policy. Also, this may occur if your
1 10 10	Attack Dattace	-CONCAT (CHAR (OF ) #2-CHAR (22) #2-CHAR (24) #2-CHAR (22) #2-CHAR (20)	OWASP 2017 A1	pages. You can enable Parameter Based
> hiddendir	0)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(105)	)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SC	CWE 89	Navigation for your scan to exclude requests made to the navigation parameter from this limit.
v 👦 api.php *	HEMA.COLLATIONS+GROUP+BY+x)a)		CAPEC 66	
v 📴 users			WASC 19	Increase Maximum Signatul Set up Parameter Based Na
> 10 2 > 51 (userID)	Proof of Exploit		HIPAA 164.306(A), 164.308(A)	Scan Policy Optimized Thago
SQL Injection	Here's I Bethere Maria		ISO27001 A.14.2.5	
Cross-site Scripting	Identified Database Name		ASVS 4.0 5.3.4	current scan and saved as Default Security
1 Database Detected (		• • •	NIST SP 800-53 SI-10	Checks (Optimized by Assistant) 11. Would you like to switch to the optimized policy?
P Database Error Message			DISA STIG 3.10.1	Warning: It is strongly advised to restart your scan
[Possible] Phishing by Navigatin	avus			to keep your scan coverage at its best after the
v 🐂 wsdlenum			CVSS 3.0 SCORE	scan policy is switched.
Issues - Previous Settings	Identified Database User			Switch to Optimized Policy
Y • M • ⊙ • ■ • Enter text to search A			Base 10 (Critical)	
O Command Injection			Temporal To (Critical)	
> () SQL Injection	root@localhost		Environmental To (Critical)	
Out-of-date Version (Apache)     Out-of-date Version (OnenSSI)				
> () 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:	
<ul> <li>Password Transmitted over HTTP [Variations:</li> </ul>			H/A:H	
> 🏲 [Possible] Password Transmitted over Query	10.1.19-MariaDB			
Out-of-date Version (Bootstrap) [Variations: 2]			CVSS 3.1 SCORE	
<ul> <li>Cookie Not Marked as HttpOnly [Variations: 3]</li> </ul>			Dear 10 (Critical)	
> Minternal Server Error	Vulnerability Details		Tamparal 10 (Critical)	
<ul> <li>Possible] Cross-site Kequest Forgery (Variati</li> <li>Possible] Internal IP Address Disclosure (Vari</li> </ul>	Netsparker identified an SQL Injection, which occurs when data input by a user is interp	preted as an SQL command rather than as normal data by the	Emironmental 10 (Critical)	
> 🏲 [Possible] Phishing by Navigating Browser Ta	backend database.		control (critical)	~
Possible] Windows Username Disclosure [Va     Apache MultiVieur Spahled IV/stiations: 2]	Activity		*	×
Database Error Message Disclosure [Variation	Method Target Parameter	Duration Current Activity Overall Activity	Status	
> 🎽 Database Name Disclosure (MySQL)				
Missing Content-Type Header [Variations: 4]     Missing X-Frame-Options Header [Variations:	Article or Branner El Los (20)			Res Kanudadan Para (20)
elseinfoll Outest Datested [2]	■ Activity			Netsparker Assistant (2)*
Auto save tihished successfully - 7/17/2021 633:17 PM	والمتحال المتكال البحادة ومحانيها والمتها المتهاك ومنافقات التقار	Attacking (2/3) 86% 🔝 Previous Settings - 📄 Default Secu	nty Checks - 🔛 Default Report Policy - 👥 6 🟴 7 🏴 13	79 🔻 38 🕕 38 VDB Status 🛄 Proxy: System

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.



# Uygulama [Chrome Web Tarayıcı Eklentisi İle Soap Web Servis Test Etme]

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

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

Gereksinimler

Ubuntu 18.04 LTS	// Ana Makina		
Boomerang SOAP and REST Client Plugin	// Web Servis Guvenlik // Testi Chrome Eklentisi		
DVWS - Windows 7 Home Premium	// Hedef Web Servisi - Sanal Makine		
	. 1 . 1 1		

Not: Kasıtlı zafiyetler içeren DVWS web servisi outdated olduğundan sadece eski php versiyon 5.5.38'de her sayfası düzgün çalışırdır. Bu nedenle XAMPP php 5.5.38 kurulumu ile DVWS web servisi DVWS - Windows 7 Home Premium sanal makinesinde yayındadır.

Soap web servisleri denetlerken daha önce SoapUI, Burpsuite ve Netsparker 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.





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



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.

Act	ivities 🛛 🌻 Google Chrome 👻	Pzt 15:16	- E 🎶 🖘 🧳
	💿 192.168.71.12/dvws/vulni × 🥃 Boomerang	× +	• • •
	← → C 介 🕭 Boomerang - SOAP & REST Client   chrome	-extension://eipdnjedkpcnlmmdfdkgfpljanehloah/app/workspace.html#	a 🖈 🐸 🖬 🗄 E
9	Boomerang	Request1 ×	=
· 😂	ODVWS Web Servis Testi     check_user_id	POST - http://192.168.71.12/dvws/vulnerabilities/wsdienum/service.php	- A Send Request Response
9	Population	BODY HEADERS PARAMS AUTH SCRIPT DOCS	XML - No Environment -
O	✓ Request1	1 * «x:Envelope xmlns:xx"http://schenas.xmlsoap.org/soap/envelope/" xmlns:dww"dwas:webservice"> 2 * «x:Moder/> 3 * «x:Moder/>	
		<pre>s countries(unt_put Less / durc name&gt;</pre>	
		<sup>2</sup> <sup>−</sup> <sup>−</sup>	
Fz			b)
Ŷ			D)
6			
		a)	
9			

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





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



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

## >>> Web Servisleri Saha Görevlerinde Test Etme Hakkında (Genel Değerlendirme)

# [Netsparker]

Web servis testlerinde eğer web servis arayüzü / kapsamı dosyası - soap için wsdl ve rest için wadl, openapi (swagger),.. - web servis url'si üzerinden indirilerek veya doğrudan web servis geliştiricilerinden alınarak elde edilebiliyorsa Netsparker'da kapsam ekranında import edilebilir ve tarama yapılabilir.

# [SoapUI]

Web servis testlerinde eğer web servis arayüzü / kapsamı dosyası - soap için wsdl ve rest için sadece wadl - web servis url'si üzerinden indirilerek veya doğrudan web servis geliştiricilerinden alınarak elde edilebiliyorsa SoapUI yazılımında kapsam olarak yüklenebilirler ve kapsama göre oluşacak örnek xml taleplerini değiştire değiştire göndererek testler yürütülebilir. Ayrıca SoapUI'de yapılacak proxy ayarı ile talep paketleri burpsuite'e yönlendirilerek test genişletilebilir.

## [Burpsuite]

Web servis testlerinde soap web servisler için wsdl dosyası "web servis url'si üzerinden" elde edilebiliyorsa burpsuite wsdler eklentisi ile arayüz / kapsam edinilebilir ve burpsuite üzerinden repeater, intruder, scan, ... gibi sekmelerden testler yürütülebilir.

## [Chrome & Firefox Plugin'leri]

Web servis testlerinde eğer web servis arayüzü / kapsamı dosyası örneğin wsdl elde edilebilmekteyse web tarayıcı eklentileri aracılığıyla da (örn; Boomerang Soap and REST Client -Chrome Eklentisi gibi) tanımlama dosyaları parse edilebilir ve oluşan örnek xml taleplerinde oynamalar yaparak gönderme ile güvenlik denetimleri uygulanabilir.

## [Wireshark]

Web servis testlerinde eğer web servis arayüzü / kapsamı dosyası mevcut değilse web servis geliştiricisinden web servisi tüketen / kullanan uygulama istenebilir. Bu şekilde uygulamayı kullanırken oluşan trafik wireshark ile okunabilir ve web servis web sunucu adresi filtrelemesine gidilerek "follow tcp stream" ile uygulamanın web servise yaptığı ham bir talep alınabilir. Bu ham talep Burpsuite'te repeater'a atılarak ve örneğin Intruder'a gönderilerek testler yürütülebilir. Aynı şekilde Netsparker'a atılarak sadece belirtilen ham paket üzerinden otomatize testler yürütülebilir.

## Not:

WSDL dosyası soap web servisler geliştirilir geliştirilmez oluşan dosyalardır. Bu nedenle soap için wsdl dosyası almak garanti olabilir, fakat rest için aynı şey söz konusu değildir.

# [Proxy]

Web servis testlerinde eğer web servis arayüzü / kapsamı dosyası mevcut değilse web servis geliştiricisinden web servisi tüketen / kullanan uygulama istenebilir. Bu şekilde uygulamayı kullanırken işletim sistemi /etc/hosts dosyasından ilgili hedef web servis urls'sine karşılık localhost verilerek uygulama trafiği lokalde burpsuite'e aktarılabilir ve uygulamadan gelen paketlerle web servis test edilebilir.

## Sonuç

Sonuç olarak web servisler ancak arayüzleri / kapsamları çıktığında taranabilir. Web uygulamalara göre manuel yollardan arayüzü / kapsamı çıkarmak güçtür. Bu nedenle manuel yollardan gidildiğinde arayüz / kapsam ancak çıktığı kadarıyla testler yürütülebilir. Yani ancak elde edilen talepler üzerinden açıklık denemeleri testleri uygulanabilir. Örneğin web servisi tüketen / kullanan uygulamanın trafiği wireshark ile dinlenerek elde edilen talepler kapsamınca testler uygulanması gibi. Bu şekilde web servis testi yürütülebilir. Eğer web servis geliştiricisinde arayüz / kapsam dosyaları mevcutsa elde edilecek talepler bütün kapsamı vereceğinden testler daha kaliteli yürütülebilir.

# Kaynaklar

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-serviceswith-burp/ https://www.smeegesec.com/2013/04/wsdl-wizard-burp-suite-plugin-for.html https://www.smeegesec.com/2012/10/automating-web-services-communication.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.voutube.com/watch?v=txGa3kGWI00&ab\_channel=JosephMcCrav 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-adatabase/

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-rewrite-rules-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-and-web-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/