Fırat Üniversitesi

Muş Ticaret ve Sanayi Odası Test Raporu

İçindekiler

Özet

Muş Ticaret ve Sanayi Odası websitesine kara kutu olacak şekilde penetrasyon testi uygulamaya çalıştık. Çıktılarda önemli gördüğümüz kısımları rapor haline getirdik. Kali ve web araçları üzerinden bulabildiğimiz kadar bilgi toplamaya çalıştık.

Takım Rehberi

1-) Hidayet Can ULUBAŞ - Maltego, SQL Injection ve Dökümanı hazırlama
2-) Furkan BAŞAN - Synk, Dimitry ve HostedScan
3-) Hazel OKTAY -
4-) Halil Ibrahim YILDIZ - Hackbar ve SQL Injection
5-) Utku Enes ALAGÖZ - Nmap, Dirb ve Legion
6-) Mücahit Eren ÖZCAN
7-) Hamit Batuhan ÖZMEN - Nmap
8-) Uğur Can IŞILDAR
9-) Ahmet Furkan BOZKURT
10-) Mert ÇEVİK - Nesus
11-) Abdullah GÜNAN - Nesus
12-) Ece DOĞAN - Nesus
13-) Uğur Umur ZELCEK - AQUATONE, TheHarvester, Nikto, MetaSploit ve Racoon
14-) Tahir BAYRAKTAR
15-) Hassan Sanusi BEYERO
16-) Muhammed Talha BAYSAL - NetSparker

NOT : Yapılanlar listesi son 2 gündür araştırılan ve bulunun bulgulardır. Önceki haftalarda kişiler sunum yapacakları konular hakkında araştırma yapıp sunum hazırlamıştır.

Maltego

Öncelikle Maltego Pentestlerde en önemli kısımlarından biri olan bilgi toplama kısmıdır. Maltego'da aktif ve pasif bilgi toplama özelliği olan bir bilgi toplama aracıdır. Biz Maltego aracını kullanarak elde ettiğimiz önemli kısımların ekran görüntüleri aşağıdaki gibidir.

Telefon Numaraları :

Phone Number	+90 312 988 11 06
Phone Number	+90 312 988 11 06
Phone Number	+90 422 323 99 45
Phone Number	+90 422 323 99 45

E - mail Adresleri :

Email Addresses (14)	
abuse@ovh.net	abuse@ripe.net
abuse@web.com	admin@dns.com.
domain.operations@web.com	giresun@giresun-tso.org.tr
giresuntso@tobb.org.tr	hello@thebookmerchantjenkins.com
hostmaster@ripe.net	mendes.ahmet@hotmail.com
mustso@tobb.org.tr	sales@zz-2.com

Bağlı DNS İsimleri ve Şirketler :

Websitesinin Mimarisi Hakkında Bilgiler :

Websitesine Bağlı Resim Dosyaları :

Netsparker

Netsparker, web uygulamalarındaki güvenlik açıklarını tespit edebilmek için kullanılan bir yazılımdır. Netsparker webdeki güvenlik açıklıklarını bulmakla birlikte sisteme gelebilecek herhangi bir saldırı karşında ne kadar güvende olduğunu da tespit eder. Bizim Netsparken kullanarak bulabildiklerimiz aşağıdaki gibidir.

- http://tv.tobb.org.tr/
- https://www.tobb.org.tr/FuarlarM
- http://www.eximbank.gov.tr/
- https://www.tobb.org.tr/Sayfalar
- https://www.tuik.gov.tr/
- https://www.tobb.org.tr/BilgiEris
- https://www.tobb.org.tr/BilgiEris
- https://tobb.org.tr/MaliveSosyall
- https://www.tobb.org.tr/KamuPc
- https://www.tuik.gov.tr/Kurumsa
- http://www.resmigazete.gov.tr/d
- https://www.tobb.org.tr/HukukM
- https://www.tobb.org.tr/HukukM
- https://www.tobb.org.tr/HukukM
- http://www.mevzuat.gov.tr/Meti MevzuatKod=1.5.6102&Me
- http://www.ekonomi.gov.tr/port _afrLoop=891193306660909&ar st
- http://www.mirsoft.com.tr

8.1. https://www.mustso.org.tr/

External Links

- https://uye.tobb.org.tr/organizasyon/firma-index.jsp
- https://uye.tobb.org.tr/organizasyon/firma-index.jsp
- https://mersis.gtb.gov.tr/
- https://youtu.be/sjf6AzBvico
- http://www.tobb.org.tr
- http://www.resmigazete.gov.tr
- http://www.balo.tc
- http://www.gtias.com.tr
- http://tv.tobb.org.tr
- http://www.tepav.org.tr/tr
- http://www.turkiye100.org
- http://www.tobb.org.tr/FuarlarMudurlugu/Sayfalar/AnaSayfa.php
- http://www.tobb.org.tr/Sayfalar/TOBBIstatistikleri.php
- http://www.kosgeb.gov.tr
- http://www.rekabet.gov.tr/
- http://www.ilan.gov.tr/
- http://www.mus.bel.tr/
- http://www.alparslan.edu.tr/
- http://www.mus.gov.tr/
- http://www.daka.org.tr/
- http://www.kosgeb.gov.tr/site
- http://www.iskur.gov.tr/
- https://www.ombudsman.gov.tr/
- http://icc.tobb.org.tr/
- https://www.deik.org.tr/
- https://www.cimer.gov.tr/
- http://meybem.com.tr/

&No=6102
zuati?
rWindowId%3Dnull%26_afrLoo

Company	
Company	
Company	
Company	
Company	
Company	TOBB Hukuk Müşavirliği
Company	TOBB TV

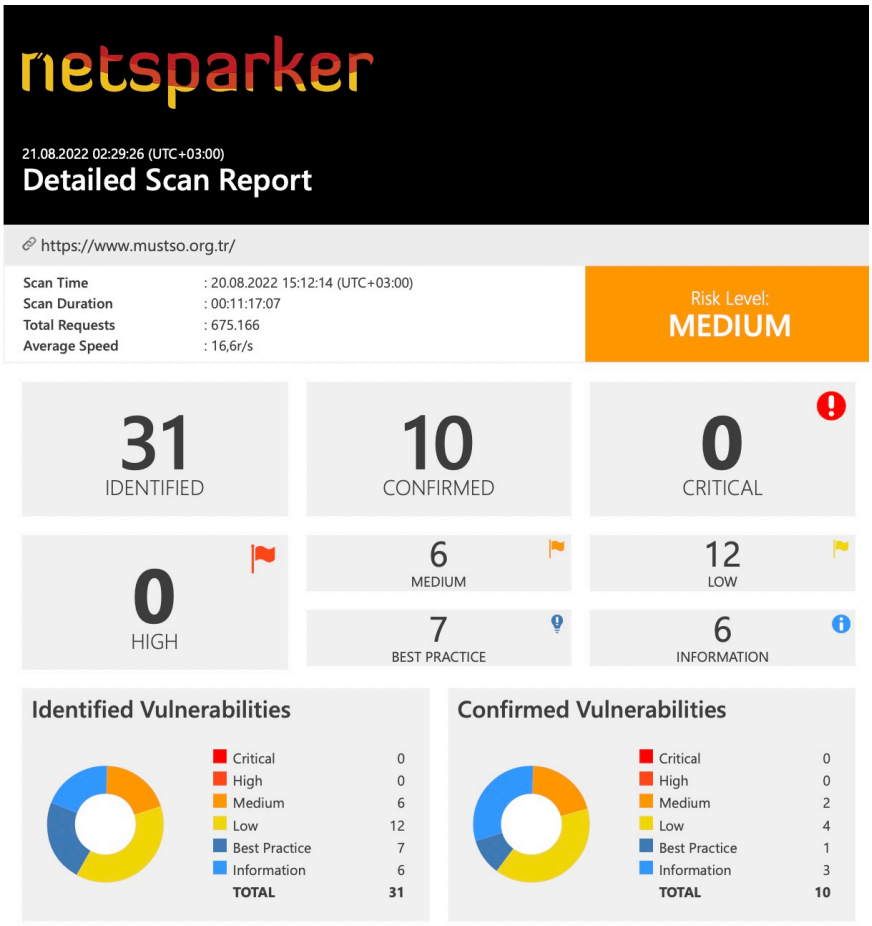
Vulnerabilities

6.1. https://www.mustso.org.tr/

CONFIRMED

List of Supported Weak Ciphers

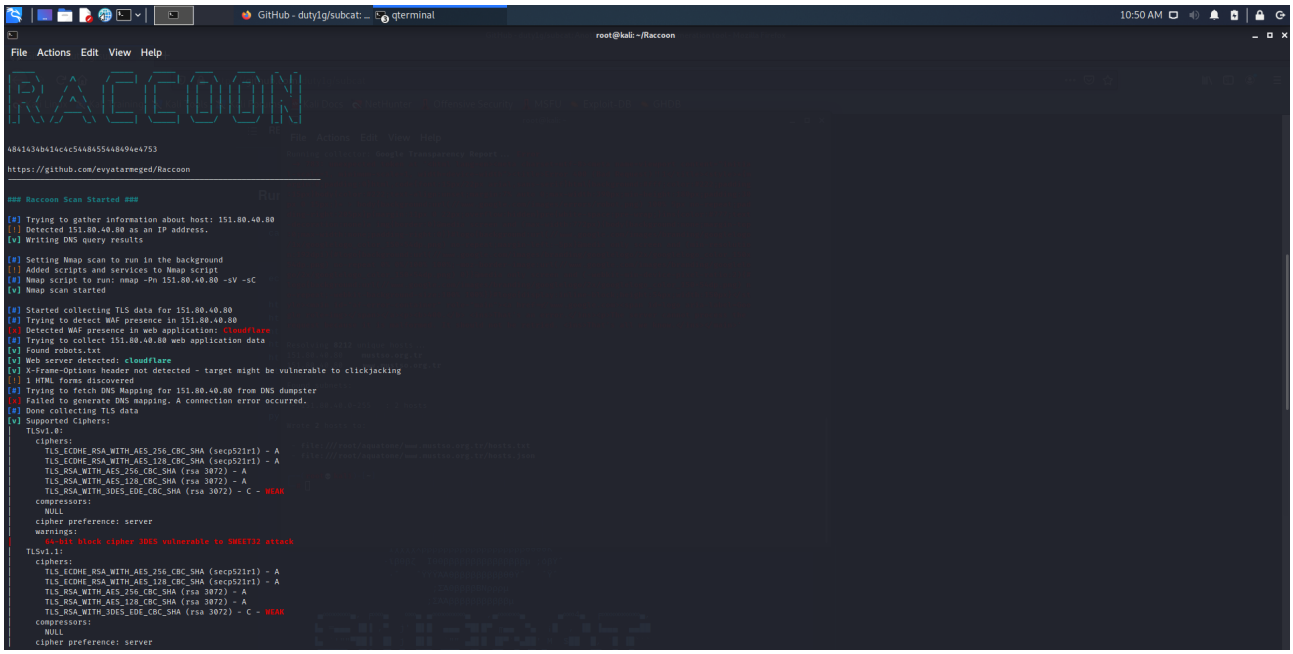
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

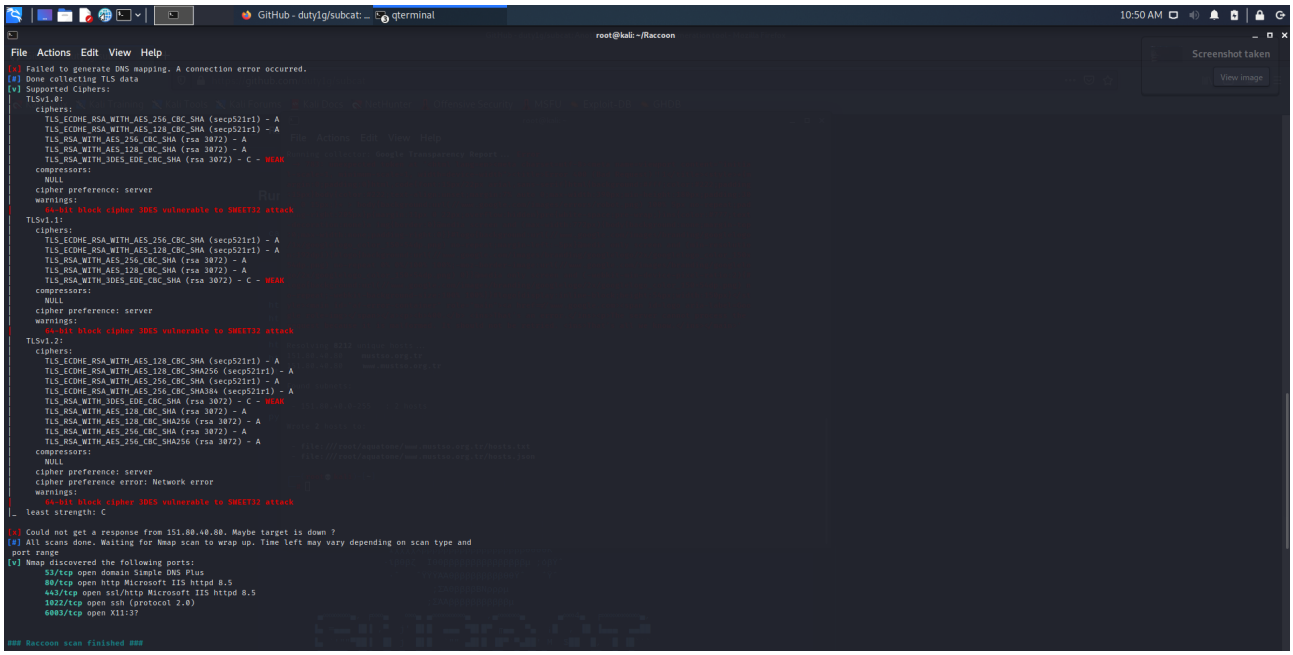


Racoon

Raccoon, Github'da bulunan ücretsiz ve açık kaynaklı bir araçtır. Bu araç keşif ve bilgi toplama için kullanılır. Bu araç whois bilgisi, TLS verisi DNS kayıtları alma, subdomain

numaralandırma, threaded dir busting gibi farklı işlemleri gerçekleştiren çeşitli modüllere sahiptir. Farklı modüller farklı işlemler gerçekleştirir. Aracı kullanabilmeniz için sisteminizde python kurulu olmalıdır. Bu araç aynı zamanda URL fuzzling de yapabilir. Rakun, eksiksiz bir bilgi toplama araçları paketi olarak da bilinir. Racoon'dan elde ettiklerimiz :





Nesus

Plugin Output

mustso.org.tr (tcp/443/www)

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                            Code              KEX            Auth      Encryption                MAC
    ------------------------------- ----------------- -------        --------- ------------------------- -------
    DES-CBC3-SHA                    0x00, 0x0A        RSA            RSA       3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                            Code              KEX            Auth      Encryption                MAC
 ------------------------------------------------------------------ ---------- ------------------------- -------
    ECDHE-RSA-AES128-SHA            0xC0, 0x13        ECDH           RSA       AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA            0xC0, 0x14        ECDH           RSA       AES-CBC(256)
 SHA1
    AES128-SHA                      0x00, 0x2F        RSA            RSA       AES-CBC(128)
 SHA1
    AES256-SHA                      0x00, 0x35        RSA            RSA       AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256         0xC0, 0x27        ECDH           RSA       AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384         0xC0, 0x28        ECDH           RSA       AES-CBC(256)
 SHA384
    RSA-AES128-SHA256               0x00, 0x3C        RSA            RSA       AES-CBC(128)
 SHA256
    RSA-AES256-SHA256               0x00, 0x3D        RSA            RSA       AES-CBC(256)
 SHA256
```

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                            Code              KEX            Auth      Encryption                MAC
    ------------------------------- ----------------- -------        --------- ------------------------- -------
    DES-CBC3-SHA                    0x00, 0x0A        RSA            RSA       3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

Nessus, dünyada birçok kullanıcısı bulunan güvenlik zafiyeti tarama programıdır. Nessus Professional, Nessus Manager, Nessus Home ve Nessus Cloud sürümleri mevcuttur. Fiziksel, sanal ve bulut ortamlarında güvenlik zafiyetlerinin ve zararlı yazılımların tespitini sağlar. Nesus bulgularımız :

NMap

Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. İsmini Network Mapper'in kısaltmasından almaktadır. Ağ yöneticileri nmap'i sistemlerinde hangi cihazların çalıştığını belirlemek, mevcut ana makineleri ve sundukları hizmetleri keşfetmek, açık bağlantı noktaları bulmak ve güvenlik risklerini taramak için kullanırlar. Nmap, yüz binlerce cihazı ve alt ağı kapsayan geniş ağların yanı sıra tek ana bilgisayarı izlemek için kullanılabilir. Bulgularımız :

NOT : Terminal kodları tam döküman içindedir.

Bu taramada Bitvise ssh server aracının kullanıldığı görüntülenmiştir.

```
1022/tcp open  ssh      (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-9.99 FlowSsh: Bitvise SSH Server (WinSSHD) : free only for persona
l non-commercial use
| ssh-hostkey:
|_  1024 d5:79:ca:d5:94:16:9e:15:67:ba:a0:5a:05:de:69:ee (DSA)
6003/tcp open  X11:3?
|_x11-access: ERROR: Script execution failed (use -d to debug)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port1022-TCP:V=7.92%I=7%D=8/19%Time=62FFC408%P=aarch64-unknown-linux-gn
SF:u%r(NULL,60,"SSH-2\.0-9\.99\x20FlowSsh:\x20Bitvise\x20SSH\x20Server\x20
SF:\(WinSSHD\)\x20:\x20free\x20only\x20for\x20personal\x20non-commercial\x
SF:20use\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

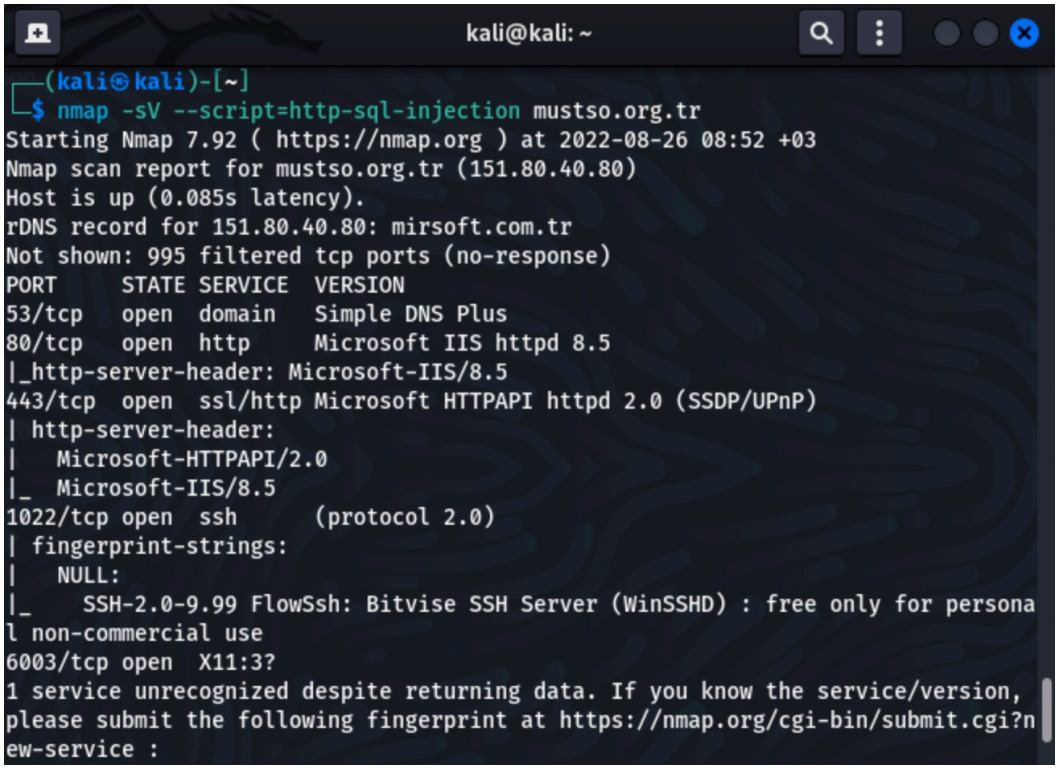
TLSv1.3:

- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256

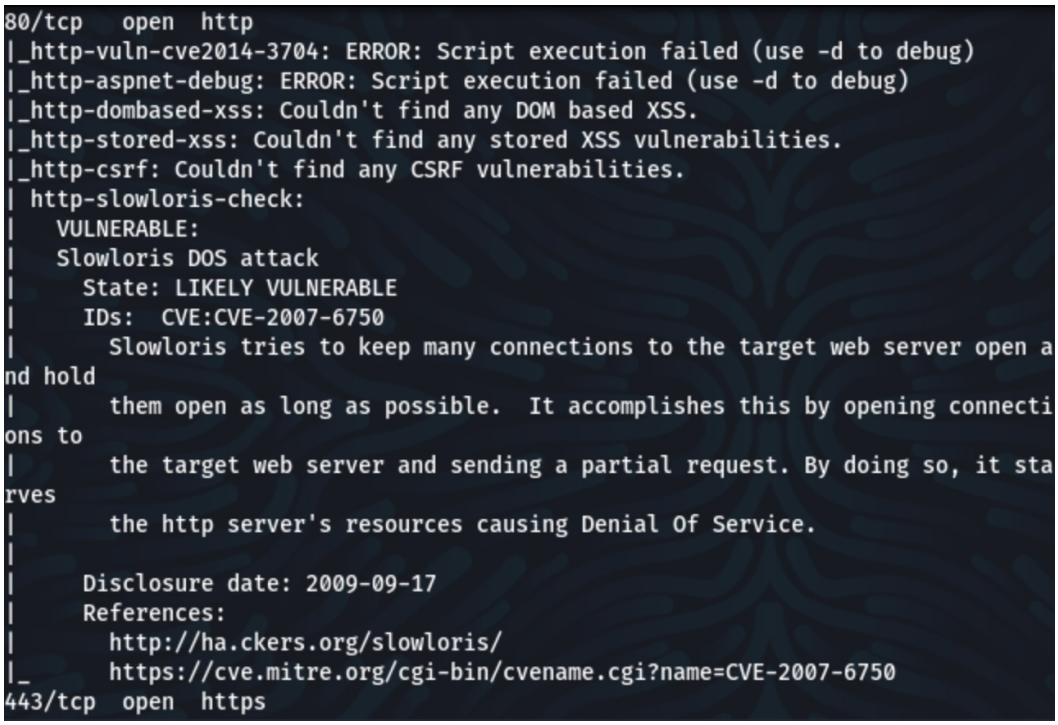
TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

Bu taramada sql açığı var mı diye kontrol edilmiştir ve bulunmamıştır.

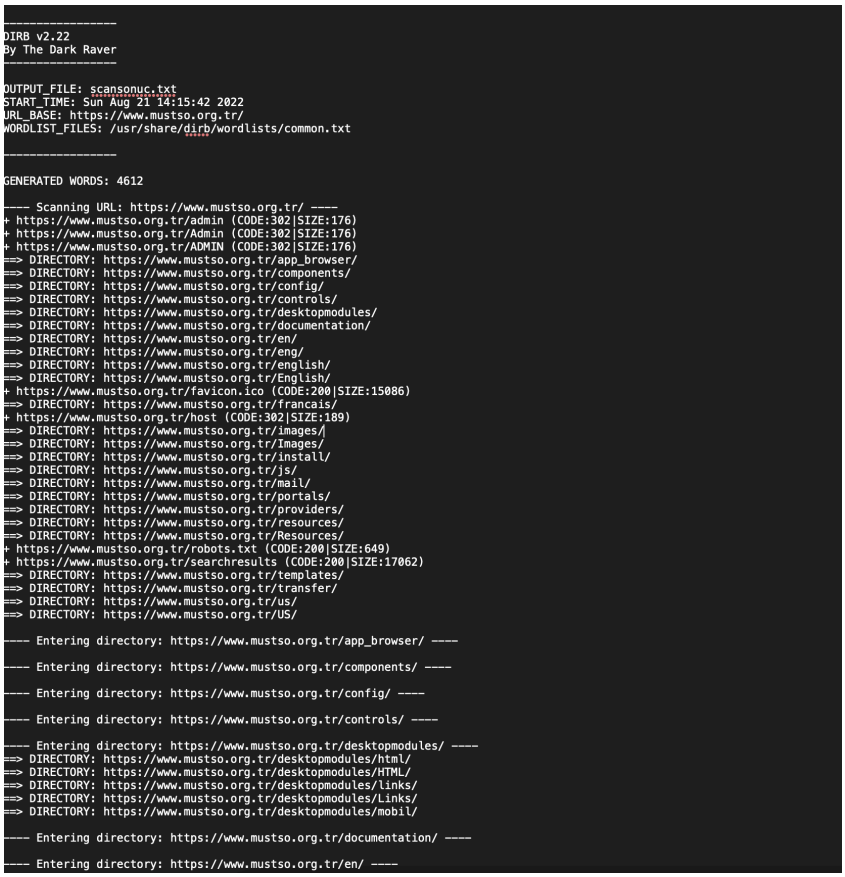


Bu taramada slowloris dos saldırısının yapılabilir olduğu görüntülenmiştir.



Dirb

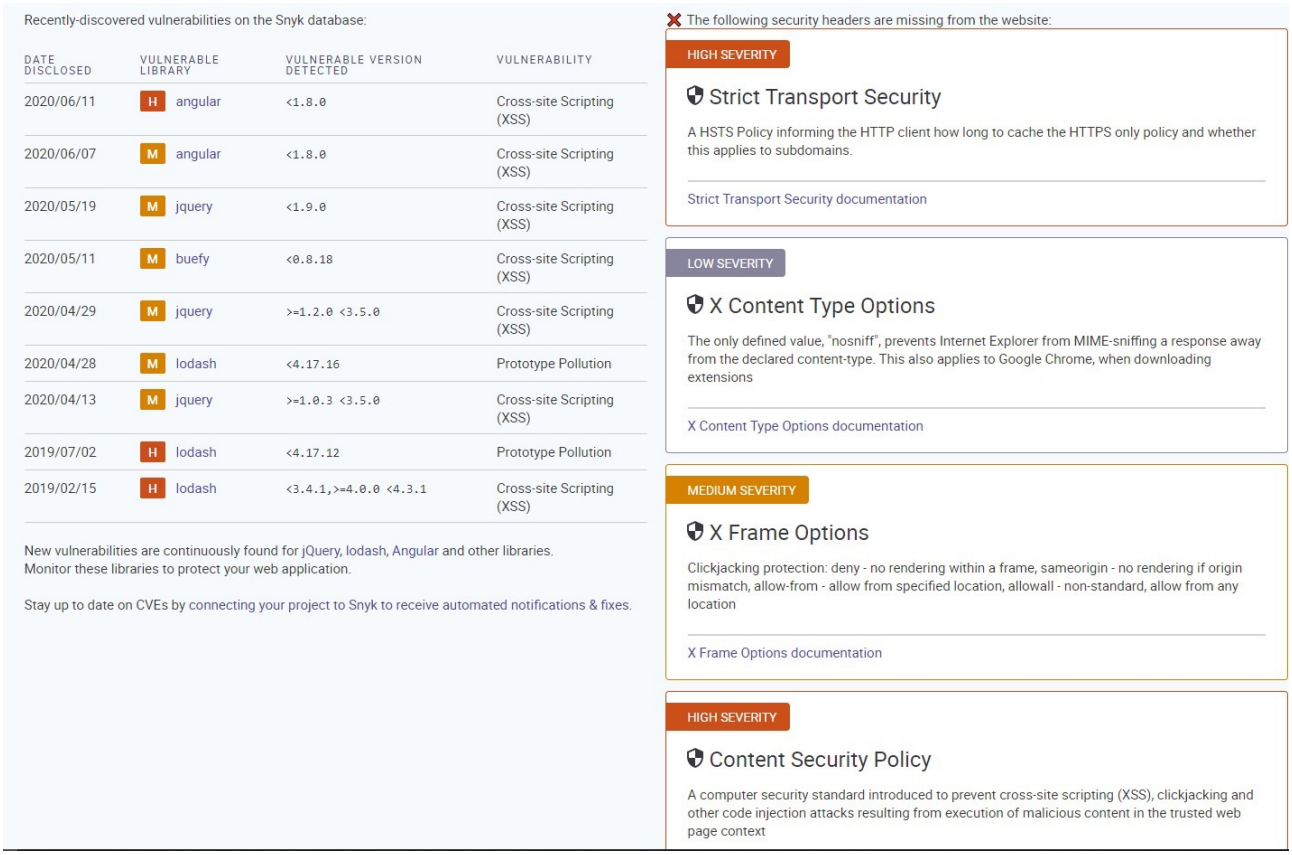
Bizim ufak tefek dostumuz olan DIRB **bir Web içerik tarayıcısıdır**. Yani sizin ona vereceğiniz link sözlük bazlı olarak tarayarak bütün içerikleri, linkleri vb. çıkarıp size listeleyen bir araçtır. Bulgularımız :



```
---- Entering directory: https://www.mustso.org.tr/eng/ ----

---- Entering directory: https://www.mustso.org.tr/english/ ----

---- Entering directory: https://www.mustso.org.tr/English/ ----

---- Entering directory: https://www.mustso.org.tr/francais/ ----

---- Entering directory: https://www.mustso.org.tr/images/ ----
==> DIRECTORY: https://www.mustso.org.tr/images/filemanager/
==> DIRECTORY: https://www.mustso.org.tr/images/flags/
==> DIRECTORY: https://www.mustso.org.tr/images/icon/
==> DIRECTORY: https://www.mustso.org.tr/images/search/
==> DIRECTORY: https://www.mustso.org.tr/images/Search/

---- Entering directory: https://www.mustso.org.tr/Images/ ----
==> DIRECTORY: https://www.mustso.org.tr/Images/filemanager/
==> DIRECTORY: https://www.mustso.org.tr/Images/flags/
==> DIRECTORY: https://www.mustso.org.tr/Images/icon/
==> DIRECTORY: https://www.mustso.org.tr/Images/search/
==> DIRECTORY: https://www.mustso.org.tr/Images/Search/

---- Entering directory: https://www.mustso.org.tr/install/ ----
==> DIRECTORY: https://www.mustso.org.tr/install/language/
==> DIRECTORY: https://www.mustso.org.tr/install/module/
==> DIRECTORY: https://www.mustso.org.tr/install/package/
==> DIRECTORY: https://www.mustso.org.tr/install/portal/
==> DIRECTORY: https://www.mustso.org.tr/install/scripts/
==> DIRECTORY: https://www.mustso.org.tr/install/Scripts/
==> DIRECTORY: https://www.mustso.org.tr/install/skin/
==> DIRECTORY: https://www.mustso.org.tr/install/template/

---- Entering directory: https://www.mustso.org.tr/js/ ----

---- Entering directory: https://www.mustso.org.tr/mail/ ----
==> DIRECTORY: https://www.mustso.org.tr/mail/mobile/
==> DIRECTORY: https://www.mustso.org.tr/mail/sms/
==> DIRECTORY: https://www.mustso.org.tr/mail/web2/

---- Entering directory: https://www.mustso.org.tr/portals/ ----
==> DIRECTORY: https://www.mustso.org.tr/portals/0/
==> DIRECTORY: https://www.mustso.org.tr/portals/103/
==> DIRECTORY: https://www.mustso.org.tr/portals/13/
==> DIRECTORY: https://www.mustso.org.tr/portals/15/
==> DIRECTORY: https://www.mustso.org.tr/portals/21/
==> DIRECTORY: https://www.mustso.org.tr/portals/22/
==> DIRECTORY: https://www.mustso.org.tr/portals/23/
==> DIRECTORY: https://www.mustso.org.tr/portals/24/
==> DIRECTORY: https://www.mustso.org.tr/portals/25/
==> DIRECTORY: https://www.mustso.org.tr/portals/64/

---- Entering directory: https://www.mustso.org.tr/providers/ ----

---- Entering directory: https://www.mustso.org.tr/resources/ ----
==> DIRECTORY: https://www.mustso.org.tr/resources/search/
==> DIRECTORY: https://www.mustso.org.tr/resources/Search/
==> DIRECTORY: https://www.mustso.org.tr/resources/shared/

---- Entering directory: https://www.mustso.org.tr/Resources/ ----
==> DIRECTORY: https://www.mustso.org.tr/Resources/search/
==> DIRECTORY: https://www.mustso.org.tr/Resources/Search/
==> DIRECTORY: https://www.mustso.org.tr/Resources/shared/

---- Entering directory: https://www.mustso.org.tr/templates/ ----

---- Entering directory: https://www.mustso.org.tr/transfer/ ----

---- Entering directory: https://www.mustso.org.tr/us/ ----

---- Entering directory: https://www.mustso.org.tr/US/ ----

---- Entering directory: https://www.mustso.org.tr/desktopmodules/html/ ----
==> DIRECTORY: https://www.mustso.org.tr/desktopmodules/html/providers/

---- Entering directory: https://www.mustso.org.tr/desktopmodules/HTML/ ----
==> DIRECTORY: https://www.mustso.org.tr/desktopmodules/HTML/providers/

---- Entering directory: https://www.mustso.org.tr/desktopmodules/links/ ----
==> DIRECTORY: https://www.mustso.org.tr/desktopmodules/links/providers/

---- Entering directory: https://www.mustso.org.tr/desktopmodules/Links/ ----
==> DIRECTORY: https://www.mustso.org.tr/desktopmodules/Links/providers/

---- Entering directory: https://www.mustso.org.tr/desktopmodules/mobil/ ----

---- Entering directory: https://www.mustso.org.tr/images/filemanager/ ----
==> DIRECTORY: https://www.mustso.org.tr/images/filemanager/files/
==> DIRECTORY: https://www.mustso.org.tr/images/filemanager/icons/

---- Entering directory: https://www.mustso.org.tr/images/flags/ ----

---- Entering directory: https://www.mustso.org.tr/images/icon/ ----
==> DIRECTORY: https://www.mustso.org.tr/images/icon/announcement/
==> DIRECTORY: https://www.mustso.org.tr/images/icon/arrow/

---- Entering directory: https://www.mustso.org.tr/images/search/ ----

---- Entering directory: https://www.mustso.org.tr/images/Search/ ----

---- Entering directory: https://www.mustso.org.tr/Images/filemanager/ ----
==> DIRECTORY: https://www.mustso.org.tr/Images/filemanager/files/
==> DIRECTORY: https://www.mustso.org.tr/Images/filemanager/icons/

---- Entering directory: https://www.mustso.org.tr/Images/flags/ ----

---- Entering directory: https://www.mustso.org.tr/Images/icon/ ----
==> DIRECTORY: https://www.mustso.org.tr/Images/icon/announcement/
==> DIRECTORY: https://www.mustso.org.tr/Images/icon/arrow/

---- Entering directory: https://www.mustso.org.tr/Images/search/ ----

---- Entering directory: https://www.mustso.org.tr/Images/Search/ ----
```

Synk

Güvenlik testi yapan online bir websitesi aracıdır Çıktı ekranı :



Recently-discovered vulnerabilities on the Snyk database:

DATE DISCLOSED	VULNERABLE LIBRARY	VULNERABLE VERSION DETECTED	VULNERABILITY
2020/06/11	H angular	<1.8.0	Cross-site Scripting (XSS)
2020/06/07	M angular	<1.8.0	Cross-site Scripting (XSS)
2020/05/19	M jquery	<1.9.0	Cross-site Scripting (XSS)
2020/05/11	M buefy	<0.8.18	Cross-site Scripting (XSS)
2020/04/29	M jquery	>=1.2.0 <3.5.0	Cross-site Scripting (XSS)
2020/04/28	M lodash	<4.17.16	Prototype Pollution
2020/04/13	M jquery	>=1.0.3 <3.5.0	Cross-site Scripting (XSS)
2019/07/02	H lodash	<4.17.12	Prototype Pollution
2019/02/15	H lodash	<3.4.1,>=4.0.0 <4.3.1	Cross-site Scripting (XSS)

New vulnerabilities are continuously found for jQuery, lodash, Angular and other libraries.
Monitor these libraries to protect your web application.

Stay up to date on CVEs by connecting your project to Snyk to receive automated notifications & fixes.

The following security headers are missing from the website:

HIGH SEVERITY

Strict Transport Security

A HSTS Policy informing the HTTP client how long to cache the HTTPS only policy and whether this applies to subdomains.

Strict Transport Security documentation

LOW SEVERITY

X Content Type Options

The only defined value, "nosniff", prevents Internet Explorer from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions

X Content Type Options documentation

MEDIUM SEVERITY

X Frame Options

Clickjacking protection: deny - no rendering within a frame, sameorigin - no rendering if origin mismatch, allow-from - allow from specified location, allowall - non-standard, allow from any location

X Frame Options documentation

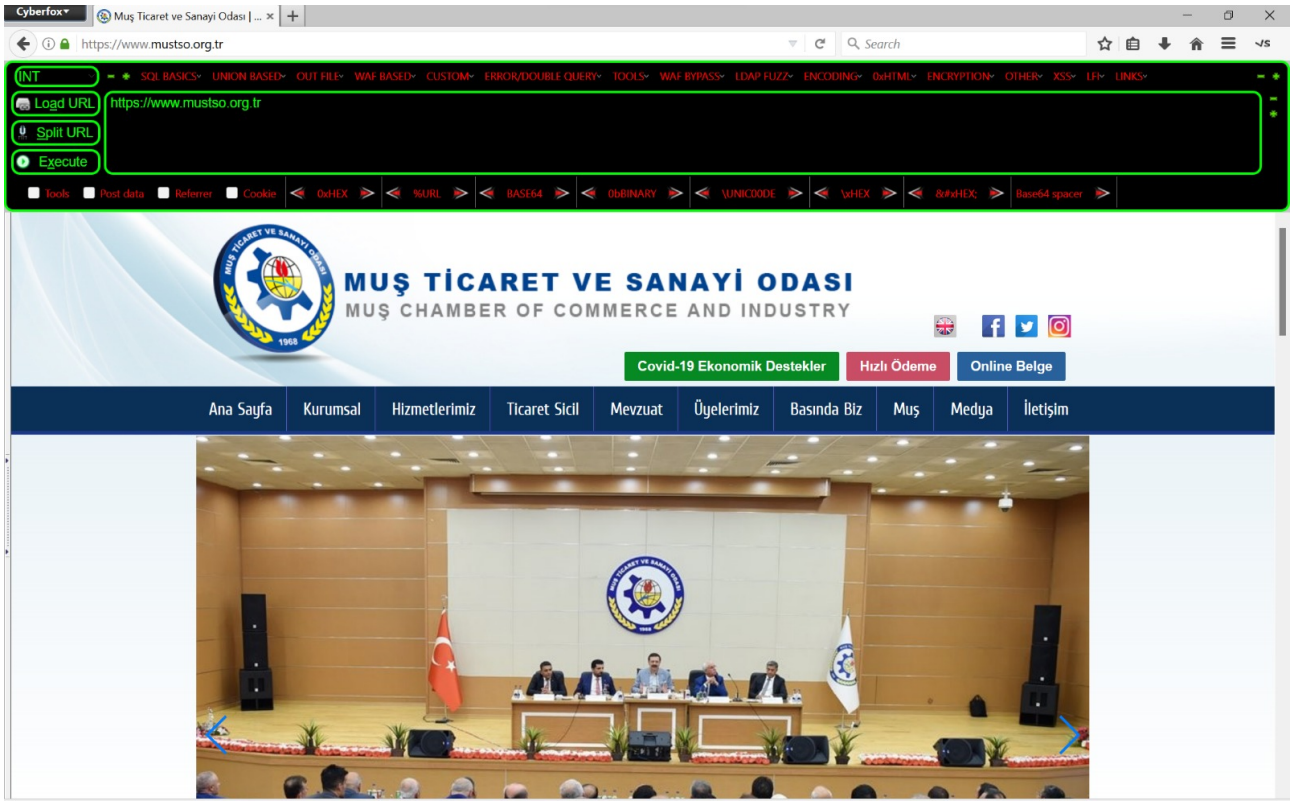
HIGH SEVERITY

Content Security Policy

A computer security standard introduced to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content in the trusted web page context

HACKBAR

HACKBAR: Hackbar firefoxa bağlı bir eklentidir. Hackbar sayesinde Sql , Xss, Lfi gibi güvenlik zafiyetlerini kullanabiliyoruz.



Kolon bulmak için ‘ORDER BY’ komutu ve ‘UNION SELECT’ komutunu kullandım fakat sql açığı olmadığından herhangi bir sonuç alamadım.