

BİLGİ SİSTEMLERİ VE GÜVENLİĞİ DERSİ

BİREYSEL SUNUMU

ÖĞRENCİ ADI: UĞUR UMUR ZELCEK

ÖĞRENCİ NUMARASI: 170541058

GRUP NUMARASI : 1. GRUP

ANLATTIĞI ARAÇ: NETSPARKER

NETSPARKER SUNUMU

Grup olarak toplantıktan sonra araçları adil bir şekilde grup sıralamamıza göre ayırdık ve Netsparker grubunda Muhammed Talha Baysal, Tahir Bayraktar ve Hassan Sanusi Bayero arkadaşlarım ile beraber Netsparker aracı ile ilgili planlama yapmak için toplantı yaptık. Araç ile ilgili grup dağılımında ben ve Tahir Bayraktar arkadaşım Netsparker hakkında bilgi toplama, Hassan Sanusi Bayero arkadaşımız slayt'ı yapma, Muhammed Talha Baysal arkadaşımız ise sunumu yapacak arkadaşımız olarak ayarladık. Tahir arkadaşım ile birlikte çeşitli internet sitelerinden topladığımız bilgiler ile bir dosya hazırladık ayrı olarak. Daha sonrasında hazırladığımız dosyayı kendi oluşturduğumuz Netsparker grubu içine attık ve Hassan arkadaşımıza işi devrettik. Daha sonrasında Hassan arkadaşımız gerekli sunumu hazırlayıp bize attı. Hep beraber tekrardan toplantı yaptık ve eksik yönleri hakkında fikir alışverişi yaptık. Eksik kısımları düzelttikten sonra tekrardan grubun onayına sunduk ve slayt'ı onayladık. Sunum yapacağım gün geldiğinde ise Muhammed Talha Baysal arkadaşımız sınıfa sunumunu yaptı.

BÜYÜK NETSPARKER SUNUMU

4 grubun toplandığı netsparker sunumunda ise arkadaşlarımız ile birlikte tarama sonucunda çıkan sorunları paylaştık. Bana düşen hatalar ise OUT-OF-DATE VERSION (ISS), Güncel olmayan sürüm ile OUT-OF-DATE VERSION (JQUERY) Güncel olmayan sürümdü. Bu iki sorun üzerinde araştırma yaptım.

Aşağıda sorunların çözümünü bırakıyorum:

Out-of-date Version (IIS), Güncel Olmayan Sürüm

MEDIUM  1

Özet

Invicti, hedef web sitesinin IIS kullandığını belirledi ve güncel olmadığını tespit etti.

Etki

Bu, yazılımın eski bir sürümü olduğundan saldırılara açık olabilir.

Düzeltilme

IIS'yi daha yüksek bir sürüme yükseltmek, bağımsız bir işlem değildir. IIS sürümü, büyük ölçüde sunucumakinenizde kullandığınız Windows işletim sistemi sürümüne bağlıdır.

Bu tür bir nedenle IIS'yi daha yüksek bir sürüme yükseltmek mümkün değilse, satıcı tarafından yayınlanan yamaları izlemenizi ve uygulamanızı şiddetle tavsiye ederiz.

Lütfen tüm IIS güncellemelerinin ve yamalarının Windows Güncellemeleri olarak geldiğini unutmayın. Ayrıca, hangi güncelleme paketinin/paketlerinin uygulanacağını da seçebilirsiniz.

Out-of-date Version (jQuery) Güncel Olmayan Sürüm

MEDIUM  1

Özet

Invicti, hedef web sitesinin jQuery kullandığını belirledi ve güncel olmadığını tespit etti.

Etki

Bu, yazılımın eski bir sürümü olduğundan saldırılara açık olabilir.

Düzeltilme

Lütfen jQuery kurulumunuzu en son kararlı sürüme yükselt

MUŞ TİCARET ODASI TARAMASI

Hocamızın bize verdiği ödevden sonra 1. Grup olarak toplandık ve görev dağılımı yaptık. Çalışma arkadaşlarımız ile tarama için kullanacağımız araçları ayırdık ve görev dağılımını yaptık. Ben tarama sonuçlarında daha fazla veri almak ve kullandığımız araçları çeşitlendirmek amacıyla Aquatone, Nikto, Raccon, TheHarvester, Owasp-zap ve Virüs Total üzerinden taramalar yapacağıma karar verdim ve grup arkadaşlarımı bilgilendirdim. Grup arkadaşlarımda onayladıktan sonra. Kullanacağım araçları Kali üzerinden kurmaya başladım. Tüm araçlarımı kurduktan sonra araçların sağlıklı bir sonuç çıkardığını emin olmak için farklı bir internet sitesi üzerinden tarama yaptım. Araçların düzgün çalıştığından emin olduktan sonra Muş Ticaret Odasının internet sitesi üzerinden taramalar yapmaya başladım.

Not: Aşağıda kullandığım araçların ne yaptığını ve çıkan sonuçlarının ekran görüntülerini paylaşıyorum.

AQUATONE : Subdomain enum, subdomain port scan, subdomain takeover ve subdomain raporlama üzerine bir çok yönlü özellikleri mevcuttur.

NİKTO : Nikto, web server üzerinde bulunan güvenlik açığı tarama uygulamasıdır. Web sayfasında

bulunabilecek XSS, SQL Injection gibi bazı güvenlik açıklarını tespit eder.

RACCON : Bu araç keşif ve bilgi toplama için kullanılır. Bu araç whois bilgisi, TLS verisi DNS kayıtları

alma, subdomain gibi farklı işlemleri yapar.

THEHARVESTER : theHarvester aracı ile pasif olarak Google, Bing gibi farklı arama motorları araçları

ile LinkedIn gibi kurum çalışanları bilgilerinin yer aldığı platformlardan kullanıcı profillerini, e-posta

adreslerini ve hostları tespit etmeye yarayan aynı zamanda aktif olarak DNS adlarını ve alt alan

adlarını bulmaya yönelik kaba kuvvet saldırıları gerçekleştirebilen bir python scriptidir.

OWASP ZAP : web zafiyetlerini otomatik olarak tespit etmeyi sağlayan açık kaynak kodlu ve ücretsiz

bir web güvenlik tarayıcısıdır.

VİRÜS TOTAL: Virüs Total temel olarak yüklenen bir dosyanın zararlı olup olmadığını anti-virüsler ile taratarak veya kendi üzerindeki veritabanında bulunan imzalarla karşılaştırarak gerçekleştirir. Şu anda 50 kadar anti-virüs firmasının imzalarını kullanmaktadır.

TARAMA SONUÇLARI

```
-> 783: unexpected token at '<html lang=en><meta charset=utf-8><meta name=viewport
content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 400 (Bad
Request)!!1</title><style>{* margin:0;padding:0}html,code{ font:15px/22px arial,sans-
serif}html{ background:#fff;color:#222;padding:15px}body{ color:#222;text-
align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* >
body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-
repeat;padding-right:205px}p{ margin:11px 0 22px;overflow:hidden}pre{ white-space:pre-
wrap; }ins{ color:#777;text-decoration:none}a img{ border:0} @media screen and (max-
```

```
width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><a href="//www.google.com"><span id=logo aria-label=Google role=img></span></a><p><b>400.</b> <ins>That's an error.</ins><p>The server cannot process the request because it is malformed. It should not be retried. <ins>That's all we know.</ins></main>'
```

Resolving 8212 unique hosts...

151.80.40.80 mustso.org.tr

151.80.40.80 www.mustso.org.tr

Found subnets:

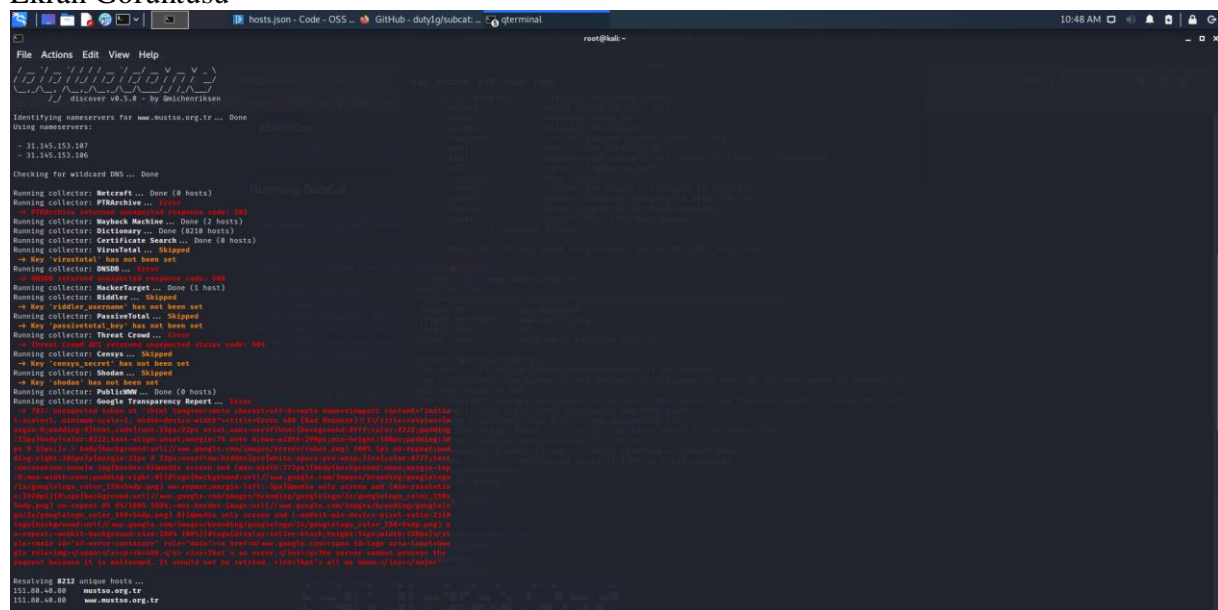
- 151.80.40.0-255 : 2 hosts

Wrote 2 hosts to:

- file:///root/aquatone/www.mustso.org.tr/hosts.txt

- file:///root/aquatone/www.mustso.org.tr/hosts.json

Ekran Görüntüsü



```
File Actions Edit View Help
root@kali: ~
Identifying nameservers for www.mustso.org.tr ... Done
Using nameservers:
- 31.145.153.107
- 31.145.153.106
Checking for wildcard DNS ... Done
Running collector: Netcraft ... Done (0 hosts)
Running collector: PTHArchive ... error
  -> PTHArchive: error: status code: 404
Running collector: Wayback Machine ... Done (2 hosts)
Running collector: Blatnary ... Done (8212 hosts)
Running collector: Certificate Search ... Done (0 hosts)
Running collector: VirusTotal ... Skipped
  -> Key 'virustotal' has not been set
Running collector: DNSDB ... error
  -> DNSDB: error: status code: 400
Running collector: HackerTarget ... Done (1 host)
Running collector: Riddler ... Skipped
  -> Key 'riddler_username' has not been set
Running collector: PassiveTotal ... Skipped
  -> Key 'passivetotal_key' has not been set
Running collector: Threat Crowd ... error
  -> Threat Crowd: error: status code: 404
Running collector: Censys ... Skipped
  -> Key 'censys_secret' has not been set
Running collector: Shodan ... Skipped
  -> Key 'shodan' has not been set
Running collector: PublicWWW ... Done (0 hosts)
Running collector: Google Transparency Report ... error
  -> Google Transparency Report: error: status code: 400
Resolving 8212 unique hosts ...
151.80.40.80 mustso.org.tr
151.80.40.80 www.mustso.org.tr
```

Araç İsmi: NIKTO

nikto -host www.mustso.org.tr

- Nikto v2.1.6

+ Target IP: 151.80.40.80

+ Target Hostname: www.mustso.org.tr

+ Target Port: 80

+ Start Time: 2022-08-20 10:15:04 (GMT-4)

```
-----
+ Server: Microsoft-IIS/8.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.mustso.org.tr/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved x-aspnet-version header: 4.0.30319
+ 7967 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:      2022-08-20 10:31:57 (GMT-4) (1013 seconds)
-----
+ 1 host(s) tested
```

Araç İsmi: RACCON

```
[#] Trying to gather information about host: 151.80.40.80
[!] Detected 151.80.40.80 as an IP address.
[v] Writing DNS query results

[#] Setting Nmap scan to run in the background
[!] Added scripts and services to Nmap script
[#] Nmap script to run: nmap -Pn 151.80.40.80 -sV -sC
[v] Nmap scan started

[#] Started collecting TLS data for 151.80.40.80
[#] Trying to detect WAF presence in 151.80.40.80
[x] Detected WAF presence in web application: Cloudflare
[#] Trying to collect 151.80.40.80 web application data
[v] Found robots.txt
[v] Web server detected: cloudflare
[v] X-Frame-Options header not detected - target might be vulnerable to clickjacking
[!] 1 HTML forms discovered
[#] Trying to fetch DNS Mapping for 151.80.40.80 from DNS dumpster
[x] Failed to generate DNS mapping. A connection error occurred.
[#] Done collecting TLS data
[v] Supported Ciphers:
| TLSv1.0:
|   ciphers:
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp521r1) - A
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp521r1) - A
|     TLS_RSA_WITH_AES_256_CBC_SHA (rsa 3072) - A
```

```

|   TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3072) - A
|   TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 3072) - C - WEAK
| compressors:
|   NULL
| cipher preference: server
| warnings:
|   64-bit block cipher 3DES vulnerable to SWEET32 attack
| TLSv1.1:
| ciphers:
|   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp521r1) - A
|   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp521r1) - A
|   TLS_RSA_WITH_AES_256_CBC_SHA (rsa 3072) - A
|   TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3072) - A
|   TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 3072) - C - WEAK
| compressors:
|   NULL
| cipher preference: server
| warnings:
|   64-bit block cipher 3DES vulnerable to SWEET32 attack
| TLSv1.2:
| ciphers:
|   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp521r1) - A
|   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp521r1) - A
|   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp521r1) - A
|   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp521r1) - A
|   TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 3072) - C - WEAK
|   TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3072) - A
|   TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 3072) - A
|   TLS_RSA_WITH_AES_256_CBC_SHA (rsa 3072) - A
|   TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 3072) - A
| compressors:
|   NULL
| cipher preference: server
| cipher preference error: Network error
| warnings:
|   64-bit block cipher 3DES vulnerable to SWEET32 attack
|_ least strength: C

```

[x] Could not get a response from 151.80.40.80. Maybe target is down ?

[#] All scans done. Waiting for Nmap scan to wrap up. Time left may vary depending on scan type and port range

[v] Nmap discovered the following ports:

```

53/tcp open domain Simple DNS Plus
80/tcp open http Microsoft IIS httpd 8.5
443/tcp open ssl/http Microsoft IIS httpd 8.5
1022/tcp open ssh (protocol 2.0)
6003/tcp open X11:3?

```

Raccoon scan finished

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title bar reads "root@kali: ~/Raccoon". Inside the terminal, the user has run the command `raccoon -u 151.80.40.88`. The output of the tool is displayed as follows:

```
##### RACCOON #####
[+] https://github.com/evyatarereg/Raccoon

### Raccoon Scan Started ###

[*] Trying to gather information about host: 151.80.40.88
[*] Detected 151.80.40.88 as an IP address.
[*] Waiting DNS query results
[*] Setting Nmap scan to run in the background
[*] Added scripts and services to Nmap script
[*] Nmap script to run: nmap -p 151.80.40.88 -v -sC
[*] Nmap scan started

[*] Started collecting TLS data for 151.80.40.88
[*] Trying to detect WMF presence in 151.80.40.88
[*] Detected WMF presence in web application: Microsoft
[*] Trying to collect 151.80.40.88 web application data
[*] Found robots.txt
[*] Web server detected: cloudflare
[*] X-Frame-Options header not detected - target might be vulnerable to clickjacking
[*] IWMF frame discovered
[*] Trying to fetch DNS Mapping for 151.80.40.88 from DNS dumpster
[*] Failed to generate DNS mapping: A connection error occurred.
[*] Done collecting TLS data
[*] Supported Ciphers:
    TLSv1.0:
      ciphers:
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secsp2121) - A
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secsp2121) - A
        TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 3872) - A
        TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3872) - A
        TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 3872) - C - MAND
        compressors:
          NULL
      cipher preference: server
      warnings:
        No-DLL Black cipher DSS vulnerable to DHSE23 attack
    TLSv1.1:
      ciphers:
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secsp2121) - A
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secsp2121) - A
        TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 3872) - A
        TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3872) - A
        TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 3872) - C - MAND
        compressors:
          NULL
      cipher preference: server
      warnings:
        No-DLL Black cipher DSS vulnerable to DHSE23 attack
    TLSv1.2:
      ciphers:
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secsp2121) - A
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secsp2121) - A
        TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 3872) - A
        TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3872) - A
        TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 3872) - C - MAND
        compressors:
          NULL
      cipher preference: server
      warnings:
        No-DLL Black cipher DSS vulnerable to DHSE23 attack
    TLSv1.3:
      ciphers:
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secsp2121) - A
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secsp2121) - A
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secsp2121) - A
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secsp2121) - A
        TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 3872) - A
        TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 3872) - A
        TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 3872) - A
        TLS_RSA_WITH_AES_256_CBC_SHA384 (rsa 3872) - A
        compressors:
          NULL
      cipher preference: server
      cipher preference error: Network error
      warnings:
        No-DLL Black cipher DSS vulnerable to DHSE23 attack
    least strength: C

[-] Could not get a response from 151.80.40.88. Maybe target is down ?
[*] All scan done. Waiting for Nmap scan to wrap up. Time left may vary depending on scan type and port range
[*] Nmap discovered the following ports:
    80/tcp open http Microsoft .NET Httpd 8.5
    443/tcp open ssl/http Microsoft .NET Httpd 8.5
    1022/tcp open ssh (protocol 2.0)
    8082/tcp open http-113f

### Raccoon scan finished ###
```

theHarvester -d www.mustso.org.tr -l 500 -b google

```

*      - -      *
* | | | | _ _ ^ ^ _ _ _ _ | | _ _ _ _ *
* | | _ \ / \ / / / \ ' _ \ \ / \ V _ | / \ _ \ ' | *
* | | | | / / _ / ( | | \ V / _ ^ \ \ / / | *
* \ | | | \ | V / \ | | \ V \ | | _ ^ \ | | *
*
*
* theHarvester 3.2.4
*
```

*
*

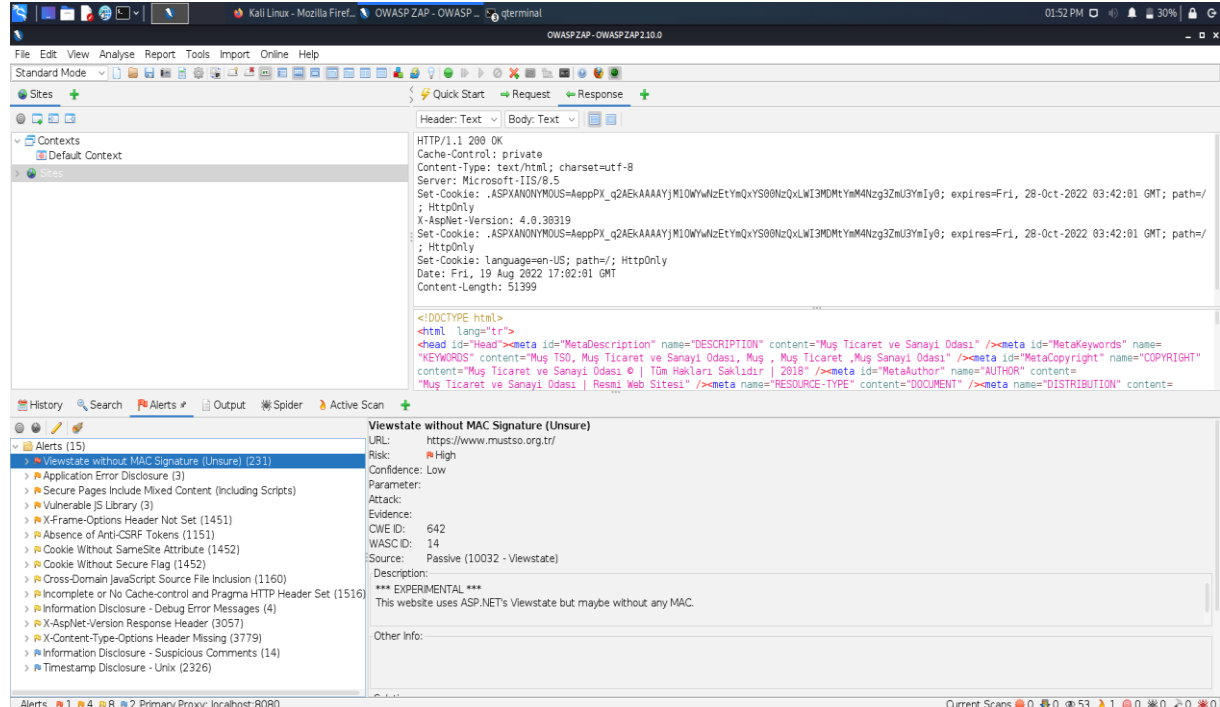
*

Searching 0 results.
Searching 100 results.
Searching 200 results.
Searching 300 results.
Searching 400 results.
Searching 500 results.

[*] No IPs found.

[*] No hosts found.

Ekran Görüntüleri:



OWASP ZAP - OWASP ZAP 2.10.0

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

Contexts

Default Context

Quick Start Request Response

Header: Text Body: Text

HTTP/1.1 400 Bad Request
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
Date: Sat, 20 Aug 2022 15:29:18 GMT
Content-Length: 3787

<style>
body {font-family:"Verdana";font-weight:normal;font-size:.7em;color:black;}
p {font-family:"Verdana";font-weight:normal;color:black;margin-top:-5px}
b {font-family:"Verdana";font-weight:bold;color:black;margin-top:-5px}
H1 {font-family:"Verdana";font-weight:normal;font-size:18pt;color:red }
H2 {font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon }
pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:8px;padding:8.5em;line-height:14pt}

History Search Alerts Output Spider Active Scan

Alerts (15)

- Viewstate without MAC Signature (Unsure) (23)
- Application Error Disclosure (3)
- Secure Pages Include Mixed Content (Including Scripts) (1)
- Vulnerable JS Library (3)
- X-Frame-Options Header Not Set (1451)
- Absence of Anti-CSRF Tokens (1151)
- Cookie Without Secure Flag (1452)
- Cookie without SameSite Attribute (1452)
- Cross-Domain JavaScript Source File Inclusion (1)
- Incomplete or No Cache-control Header Set (15)
- Information Disclosure - Debug Error Messages
- X-AspNet-Version Response Header (3057)
- X-Content-Type-Options Header Missing (3779)
- Information Disclosure - Suspicious Comments
- Timestamp Disclosure - Unix (2326)

Application Error Disclosure

URL: https://www.mustso.org.tr/?ctl=profile

Risk: Medium

Confidence: Medium

Parameter:

Attack: ASP.NET is configured to show verbose error messages

Evidence: CWE ID: 200
WASC ID: 13
Source: Passive (90022 - Application Error Disclosure)

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Other Info:

Solution: Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.

Alerts 1 4 8 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 3467 0 0 0 0 0 0 0 0

OWASP ZAP - OWASP ZAP 2.10.0

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

Contexts

Default Context

Quick Start Request Response

Header: Text Body: Text

Last-Modified: Thu, 30 Nov 2017 13:12:03 GMT
Accept-Ranges: bytes
ETag: "80d329d0dc69d31:0"
Server: Microsoft-IIS/8.5
Date: Sat, 20 Aug 2022 15:29:21 GMT
Content-Length: 799

<script src="http://code.jquery.com/jquery-2.2.4.min.js" integrity="sha256-8bhdvQ1/xTY99q3HwQFBLacRTx2KxRutl44=" crossorigin="anonymous"></script>
<script type="text/javascript" src="http://paracevrici.com/servis/widget/widget.js"></script>
<script type="text/javascript">

History Search Alerts Output Spider Active Scan

Alerts (15)

- Viewstate without MAC Signature (Unsure) (23)
- Application Error Disclosure (3)
- Secure Pages Include Mixed Content (Including Scripts) (1)
- Vulnerable JS Library (3)
- X-Frame-Options Header Not Set (1451)
- Absence of Anti-CSRF Tokens (1151)
- Cookie Without Secure Flag (1452)
- Cookie without SameSite Attribute (1452)
- Cross-Domain JavaScript Source File Inclusion (1)
- Incomplete or No Cache-control Header Set (15)
- Information Disclosure - Debug Error Messages
- X-AspNet-Version Response Header (3057)
- X-Content-Type-Options Header Missing (3779)
- Information Disclosure - Suspicious Comments
- Timestamp Disclosure - Unix (2326)

Secure Pages Include Mixed Content (Including Scripts)

URL: https://www.mustso.org.tr/Portals/326/Skins/bucak/bucak_doviz.html

Risk: Medium

Confidence: Medium

Parameter:

Attack: http://code.jquery.com/jquery-2.2.4.min.js

Evidence: CWE ID: 311
WASC ID: 4
Source: Passive (10040 - Secure Pages Include Mixed Content)

Description: The page includes mixed content, that is content accessed via HTTP instead of HTTPS.

Other Info: tag=script src=http://code.jquery.com/jquery-2.2.4.min.js
tag=script src=http://paracevrici.com/servis/widget/widget.js

Solution: A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.

Alerts 1 4 8 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 2900 0 0 0 0 0 0 0 0

OWASP ZAP - OWASP ZAP 2.10.0

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

Contexts

Default Context

Quick Start Request Response

Header: Text Body: Text

HTTP/1.1 200 OK
Cache-Control: max-age=604800
Content-Type: application/javascript
Last-Modified: Tue, 17 Jan 2017 14:45:36 GMT
Accept-Ranges: bytes
ETag: "0e8d25cd970d21:0"
Server: Microsoft-IIS/8.5
Date: Sat, 20 Aug 2022 15:30:33 GMT

/* jQuery v1.7 jquery.com | jquery.org/license */
(function(a,b){function c(a){return f.l9dindow(a)?a.nodeType===9?a.defaultView[a.parentWindow]:function cx(a){if(!c[a]){var b=c.body,d=f("<+>").appendTo(b),e=d.css("display");d.remove();if(a==="none"){e="none"}if(c[c.createElement("iframe"),cn=FrameBorder="ch",width=cn,height=0],b.appendChild(cn);if(!c[c.createElement].co=[cn,contentDocument],document.co.write(c.compatMode=="CSS1Compat"?<doctype html>:"")+"<html><body>"),co.close();d=co.createElement(d),e=f.css(d,"display"),b.removeChild(cn);c[a]=e}return c[a]}function e(a,b){var c=f.each(a.concat.apply([],cs.slice(0,b)),function(){c(function cv(){ct=b;function cu(){setTimeout(cv,0);return ct=f.now()})function cl(){try{return new a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ck(){try{return new a.

History Search Alerts Output Spider Active Scan

Alerts (15)

- Viewstate without MAC Signature (Unsure) (23)
- Application Error Disclosure (3)
- Secure Pages Include Mixed Content (Including Scripts) (1)
- Vulnerable JS Library (3)
- X-Frame-Options Header Not Set (1451)
- Absence of Anti-CSRF Tokens (1151)
- Cookie Without Secure Flag (1452)
- Cookie without SameSite Attribute (1452)
- Cross-Domain JavaScript Source File Inclusion (1)
- Incomplete or No Cache-control Header Set (15)
- Information Disclosure - Debug Error Messages
- X-AspNet-Version Response Header (3057)
- X-Content-Type-Options Header Missing (3779)
- Information Disclosure - Suspicious Comments
- Timestamp Disclosure - Unix (2326)

Vulnerable JS Library

URL: https://www.mustso.org.tr/Portals/348/Skins/mustso/jquery.js

Risk: Medium

Confidence: Medium

Parameter:

Attack: jQuery v1.7

Evidence: CWE ID: 829
WASC ID: 829
Source: Passive (10003 - Vulnerable JS Library)

Description: The identified library jquery, version 1.7 is vulnerable.

Other Info: CVE-2020-11023
CVE-2020-11022
CVE-2015-9251

Solution: Please upgrade to the latest version of jquery.

Alerts 1 4 8 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 2660 0 0 0 0 0 0 0 0

OWASP ZAP - OWASP ZAP 2.10.0

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

Contexts

Default Context

Quick Start Request Response

Header: Text Body: Text

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
Set-Cookie: .ASPXANONYMOUS=1wKScjvr2AEKAAANzZlNDYyOTkzM2I3OC08ZmNjLTg1OWEtMTAzOTESMzgWYjM40; expires=Sat, 29-Oct-2022 02:09:16 GMT; path=/; HttpOnly
X-AspNet-Version: 4.0.30319
Set-Cookie: .ASPXANONYMOUS=1wKScjvr2AEKAAANzZlNDYyOTkzM2I3OC08ZmNjLTg1OWEtMTAzOTESMzgWYjM40; expires=Sat, 29-Oct-2022 02:09:16 GMT; path=/; HttpOnly

<!DOCTYPE html>
<html lang="tr">
<head id="Head"><meta id="MetaDescription" name="DESCRIPTION" content="Muş Ticaret ve Sanayi Odası" /><meta id="MetaKeywords" name="KEYWORDS" content="Muş TSO, Muş Ticaret ve Sanayi Odası, Muş - Muş Ticaret, Muş Sanayi Odası" /><meta id="MetaCopyright" name="COPYRIGHT" content="Muş Ticaret ve Sanayi Odası © | Tüm Hakları Saklıdır | 2018" /><meta id="MetaAuthor" name="AUTHOR" content="Muş Ticaret ve Sanayi Odası | Resmi Web Sitesi" /><meta name="RESOURCE-TYPE" content="DOCUMENT" /><meta name="DISTRIBUTION" content="GLOBAL" /><meta name="ROBOTS" content="INDEX, FOLLOW" /><meta name="REVISIT-AFTER" content="1 DAYS" /><meta name="RATING" content="GENERAL" /><meta http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /><style id="StylePlaceholder" type="text/css"></style><link id="http-equiv="PAGE-ENTER" content="RevealTrans(Duration=0,Transition=1)" /></head></html>

History Search Alerts Output Spider Active Scan

Alerts (15)

- Viewstate without MAC Signature (Unsure) (23)
- Application Error Disclosure (3)
- Secure Pages Include Mixed Content (Including Vulnerable JS Library) (3)
- X-Frame-Options Header Not Set (1451)**
- Absence of Anti-CSRF Tokens (1151)
- Cookie Without Secure Flag (1452)
- Cookie without SameSite Attribute (1452)
- Cross-Domain JavaScript Source File Inclusion (1)
- Incomplete or No Cache-control Header Set (15)
- Information Disclosure - Debug Error Messages
- X-AspNet-Version Response Header (3057)
- X-Content-Type-Options Header Missing (3779)
- Information Disclosure - Suspicious Comments
- Timestamp Disclosure - Unix (2326)

X-Frame-Options Header Not Set

URL: https://www.mustso.org.tr/
Risk: Medium
Confidence: Medium
Parameter: X-Frame-Options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - X-Frame-Options Header)
Description:
X-Frame-Options header is not included in the HTTP response to protect against 'Clickjacking' attacks.
Other Info:
Solution:
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site. If you expect the page to be framed only by pages on your server (e.g. https://www.example.com/), then you should use the 'DENY' value. If you expect the page to be framed only by a specific page on your server (e.g. https://www.example.com/iframe.html), then you should use the 'ALLOW-FROM https://www.example.com/iframe.html' value.

Alerts 1 4 8 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 2220 0 0 0 0 0 0

OWASP ZAP - OWASP ZAP 2.10.0

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

Contexts

Default Context

Quick Start Request Response

Header: Text Body: Text

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
Set-Cookie: .ASPXANONYMOUS=1wKScjvr2AEKAAANzZlNDYyOTkzM2I3OC08ZmNjLTg1OWEtMTAzOTESMzgWYjM40; expires=Sat, 29-Oct-2022 02:09:16 GMT; path=/; HttpOnly
X-AspNet-Version: 4.0.30319
Set-Cookie: .ASPXANONYMOUS=1wKScjvr2AEKAAANzZlNDYyOTkzM2I3OC08ZmNjLTg1OWEtMTAzOTESMzgWYjM40; expires=Sat, 29-Oct-2022 02:09:16 GMT; path=/; HttpOnly

</div>
<div class="art-box art-blockcontent">
<div class="art-box-body art-blockcontent-body">
<div id="dnn_ctr24235_ContentPane1" class="DNNAlignLeft"><!-- Start Module_24235 --><div id="dnn_ctr24235_ModuleContent">
<div id="fb-root"></div>
<script async defer crossorigin="anonymous" src="https://connect.facebook.net/tr_TR/sdk.js#xfbml=1&version=v9.0" nonce="tUEeNzfW"></script>

History Search Alerts Output Spider Active Scan

Alerts (15)

- Viewstate without MAC Signature (Unsure) (23)
- Application Error Disclosure (3)
- Secure Pages Include Mixed Content (Including Vulnerable JS Library) (3)
- X-Frame-Options Header Not Set (1451)
- Absence of Anti-CSRF Tokens (1151)
- Cookie Without Secure Flag (1452)
- Cookie without SameSite Attribute (1452)
- Cross-Domain JavaScript Source File Inclusion (1)**
- Incomplete or No Cache-control Header Set (15)
- Information Disclosure - Debug Error Messages
- X-AspNet-Version Response Header (3057)
- X-Content-Type-Options Header Missing (3779)
- Information Disclosure - Suspicious Comments
- Timestamp Disclosure - Unix (2326)


Cross-Domain JavaScript Source File Inclusion

URL: https://www.mustso.org.tr/
Risk: Low
Confidence: Medium
Parameter: https://connect.facebook.net/tr_TR/sdk.js#xfbml=1&version=v9.0
Attack:
Evidence: <script async defer crossorigin="anonymous" src="https://connect.facebook.net/tr_TR/sdk.js#xfbml=1&version=v9.0" nonce="tUEeNzfW"></script>
CWE ID: 829
WASC ID: 15
Source: Passive (10017 - Cross-Domain JavaScript Source File Inclusion)
Description:
The page includes one or more script files from a third-party domain.
Other Info:
Solution:
Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Alerts 1 4 8 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 1883 0 0 0 0 0 0

Araç İsmi: Virüs Total

Ekran Görüntüleri

 <https://www.mustso.org.tr/>

Did you intend to search across the file corpus instead? [Click here](#)

0

/ 88

?

Community Score

✓

No security vendors flagged this URL as malicious

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


www.mustso.org.tr

200

Status

2022-08-20 13:30:03 UTC

a moment ago



×

✓

DETECTION

DETAILS

LINKS

COMMUNITY

Categories

Forcepoint ThreatSeeker

news and media

Comodo Valkyrie Verdict

media sharing

History

First Submission

2022-08-20 13:30:03 UTC

Last Submission

2022-08-20 13:30:03 UTC

Last Analysis

2022-08-20 13:30:03 UTC

HTTP Response

Final URL

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

Serving IP Address


151.80.40.80

Status Code

200

Body Length

50.19 KB

 <https://www.mustso.org.tr/>

Body Length

50.19 KB

Body SHA-256

5c58f83f1608139c4770029ad40937bc00e9fa78123d92a1f17dcb8c8cf86c8

Headers

Content-Length

13238

Content-Encoding

gzip

Set-Cookie

.ASFXANONYMIOUS=9VZy2SrZAEKAAAANDYzYzYOMWUJZDjmNi00Mmi4LTg2ZTkMTU1MzdMmizMjNj0; expires=Sat, 29-Oct-2022 00:10:00 GMT; path=/; HttpOnly, .ASFXANONYMIOUS=9VZy2SrZAEKAAAANDYzYzYOMWUJZDjmNi00Mmi4LTg2ZTkMTU1MzdMmizMjNj0; expires=Sat, 29-Oct-2022 00:10:00 GMT; path=/; HttpOnly, language=en-US; path=/;

X-AspNet-Version

4.0.30319

Vary

Accept-Encoding

Server

Microsoft-IIS/8.5

Cache-Control

private

Date

Sat, 20 Aug 2022 13:30:00 GMT

Content-Type

text/html; charset=utf-8

HTML Info

Title

MuAİ Ticaret ve Sanayi Odası | Resmi Web Sitesi > Ana Sayfa

Meta Tags

RATING

GENERAL

DESCRIPTION

MuAİ Ticaret ve Sanayi Odası

COPYRIGHT

MuAİ Ticaret ve Sanayi Odası & © | TÂ'ım HaklarÄs SaklÄsdÄr | 2018

AUTHOR

MuAİ Ticaret ve Sanayi Odası | Resmi Web Sitesi

RESOURCE-TYPE

DOCUMENT

ROBOTS

INDEX,FOLLOW

REVISIT-AFTER

1 DAYS

KEYWORDS

MuAİ TSO, MuAİ Ticaret ve Sanayi Odası, MuAİ , MuAİ Ticaret ,MuAİ Sanayi Odası

DISTRIBUTION

GLOBAL

Tarama Hakkında Çıkan Sonuç

Yukarıda belirttiğim taramalar sonucunda tatmin edici sonuçlar elde edemedim. Fakat Owasp-zap üzerinde belirtilen alertler incelendiğinde işimize yarayabileceği bilgiler bulabileceğimizi düşünüyorum. Raccon ile yaptığım taramalar sonucunda ise bana 53 (DNS), 80 (HTTP), 443 (HTTPS), 1022 (SSH) ve 6003 (X11 : 3 ?) portlarının açık olduğunu bana belirtti. Özellikle 1022(SSH) portunun açık olması beni şaşırttı ve bu port üzerinden ssh bağlantıları yapmayı denedim. Fakat giriş yapamadım. Daha sonrasında Metasploitable aracı içerisinde bulunan ssh scriptleri ile oturum açıp sızmayı denedim. Toplamda 5 farklı exploit ile giriş denemelerimde başarısızlık ile sonuçlandı. Neden giremediğimi düşündüm ve metasploitable içerisindeki exploitlerin eski scriptler olduğu için günümüz şifreleme ile giriş yapamayacağını düşünüyorum. Bu taramalardan kendime edindiğim güzel sonuç ise sadece birkaç herkes tarafından bilinen araçlar ile denemek değil daha farklı araçlar ile de deneme yapıp hem çıkan sonuçları görmek hemde daha fazla araç ile tanışmak oldu.