BUGCROWD

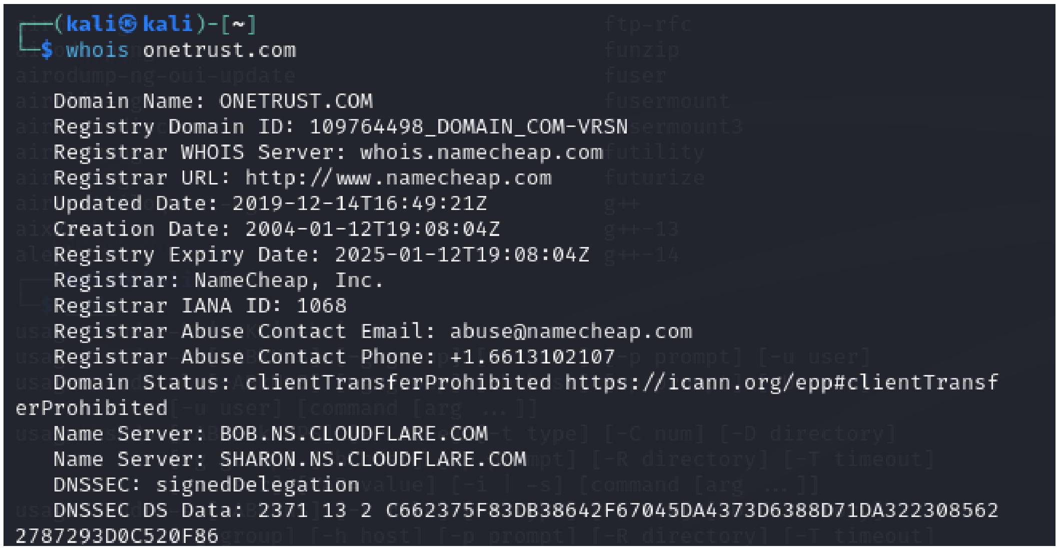
Target Report

Created by: Ziad Ahmed

At the first I made a reconnaissance step by whois command, and it was the summary of the result:

- Domain Information:
    - Domain Name/IP:
        - Name: onetrust.com
        - Address: 104.18.32.137, 172.64.155.119
    - Registrar Information:
        - Registrar: NameCheap, Inc.
        - Creation Date: 2004-01-12
        - Expiry Date: 2025-01-12
    - Name Servers:
        - bob.ns.cloudflare.com
        - sharon.ns.cloudflare.com

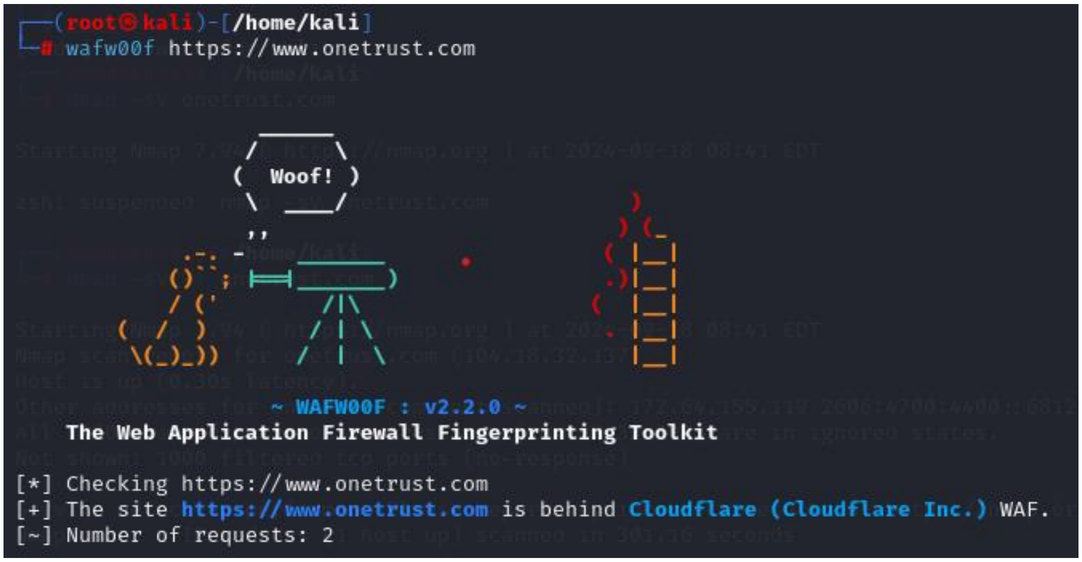
In details:



```
┌──(kali㉿kali)-[~]
└─$ whois onetrust.com

   Domain Name: ONETRUST.COM
   Registry Domain ID: 109764498_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namecheap.com
   Registrar URL: http://www.namecheap.com
   Updated Date: 2019-12-14T16:49:21Z
   Creation Date: 2004-01-12T19:08:04Z
   Registry Expiry Date: 2025-01-12T19:08:04Z
   Registrar: NameCheap, Inc.
   Registrar IANA ID: 1068
   Registrar Abuse Contact Email: abuse@namecheap.com
   Registrar Abuse Contact Phone: +1.6613102107
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
   Name Server: BOB.NS.CLOUDFLARE.COM
   Name Server: SHARON.NS.CLOUDFLARE.COM
   DNSSEC: signedDelegation
   DNSSEC DS Data: 2371 13 2 C662375F83DB38642F67045DA4373D6388D71DA322308562
2787293D0C520F86
```

Then used wafw00f command to detect the WAF:

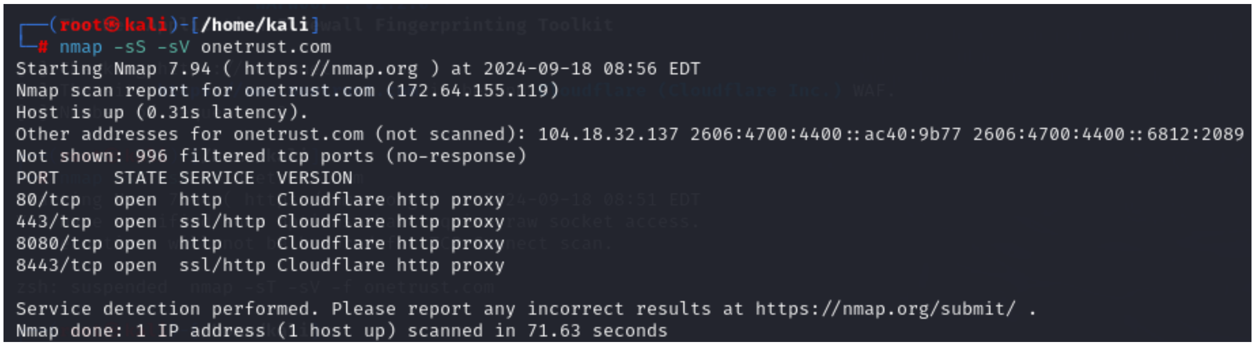
- It is Cloudflare.



```
┌──(root㉿kali)-[/home/kali]
└─# wafw00f https://www.onetrust.com

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.onetrust.com
[+] The site https://www.onetrust.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

Then tried to know the open ports by nmap -sS -sV command:

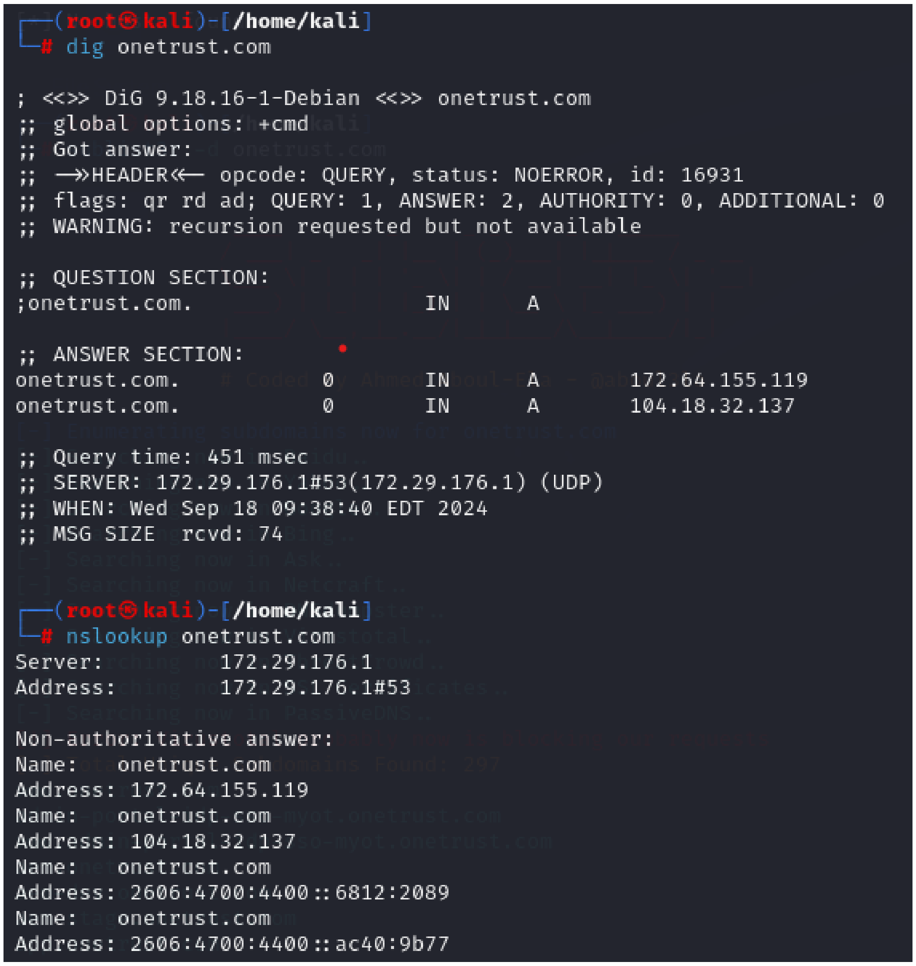
PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	ssl/http
8080/tcp	open	http
8443/tcp	open	ssl/http



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV onetrust.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-18 08:56 EDT
Nmap scan report for onetrust.com (172.64.155.119)
Host is up (0.31s latency).
Other addresses for onetrust.com (not scanned): 104.18.32.137 2606:4700:4400::ac40:9b77 2606:4700:4400::6812:2089
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
443/tcp  open  ssl/http Cloudflare http proxy
8080/tcp open  http     Cloudflare http proxy
8443/tcp open  ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.63 seconds
```

Then I get the DNS IPs by nslookup, dig commands:

- 172.64.155.119
- 104.18.32.137
- 2803:f800:50::6ca2
- 2606:4700:58::adf5:3b68

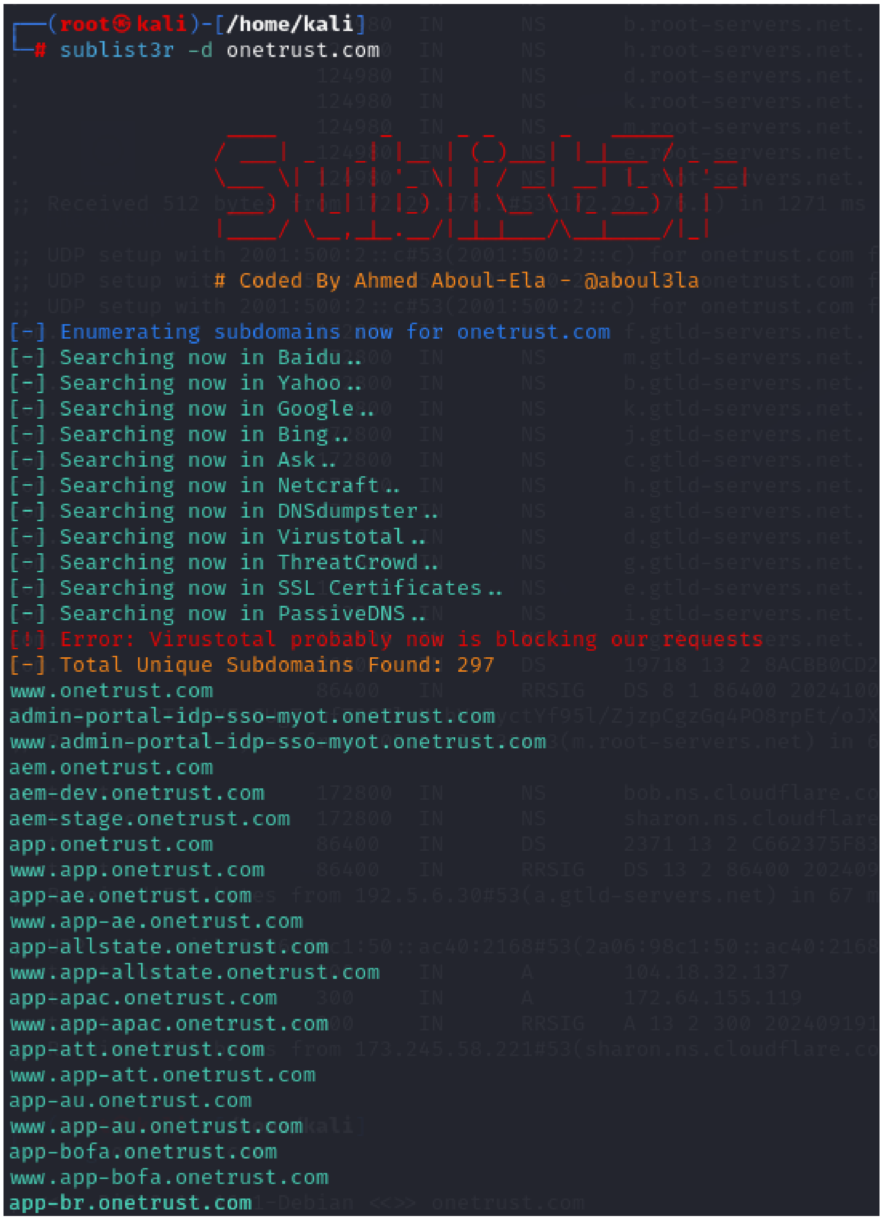


```
┌──(root㉿kali)-[/home/kali]
└─# dig onetrust.com

; <<>> DiG 9.18.16-1-Debian <<>> onetrust.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16931
;; flags: qr rd ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;onetrust.com.                  IN      A

;; ANSWER SECTION:
onetrust.com.           0       IN      A       172.64.155.119
onetrust.com.           0       IN      A       104.18.32.137

;; Query time: 451 msec
;; SERVER: 172.29.176.1#53(172.29.176.1) (UDP)
;; WHEN: Wed Sep 18 09:38:40 EDT 2024
;; MSG SIZE  rcvd: 74

┌──(root㉿kali)-[/home/kali]
└─# nslookup onetrust.com
Server:         172.29.176.1
Address:        172.29.176.1#53

Non-authoritative answer:
Name:   onetrust.com
Address: 172.64.155.119
Name:   onetrust.com
Address: 104.18.32.137
Name:   onetrust.com
Address: 2606:4700:4400::6812:2089
Name:   onetrust.com
Address: 2606:4700:4400::ac40:9b77
```

Then I get the subdomains by sublist3r command:

There are 297 subdomains, and I stored them in a file and here is an example of them:

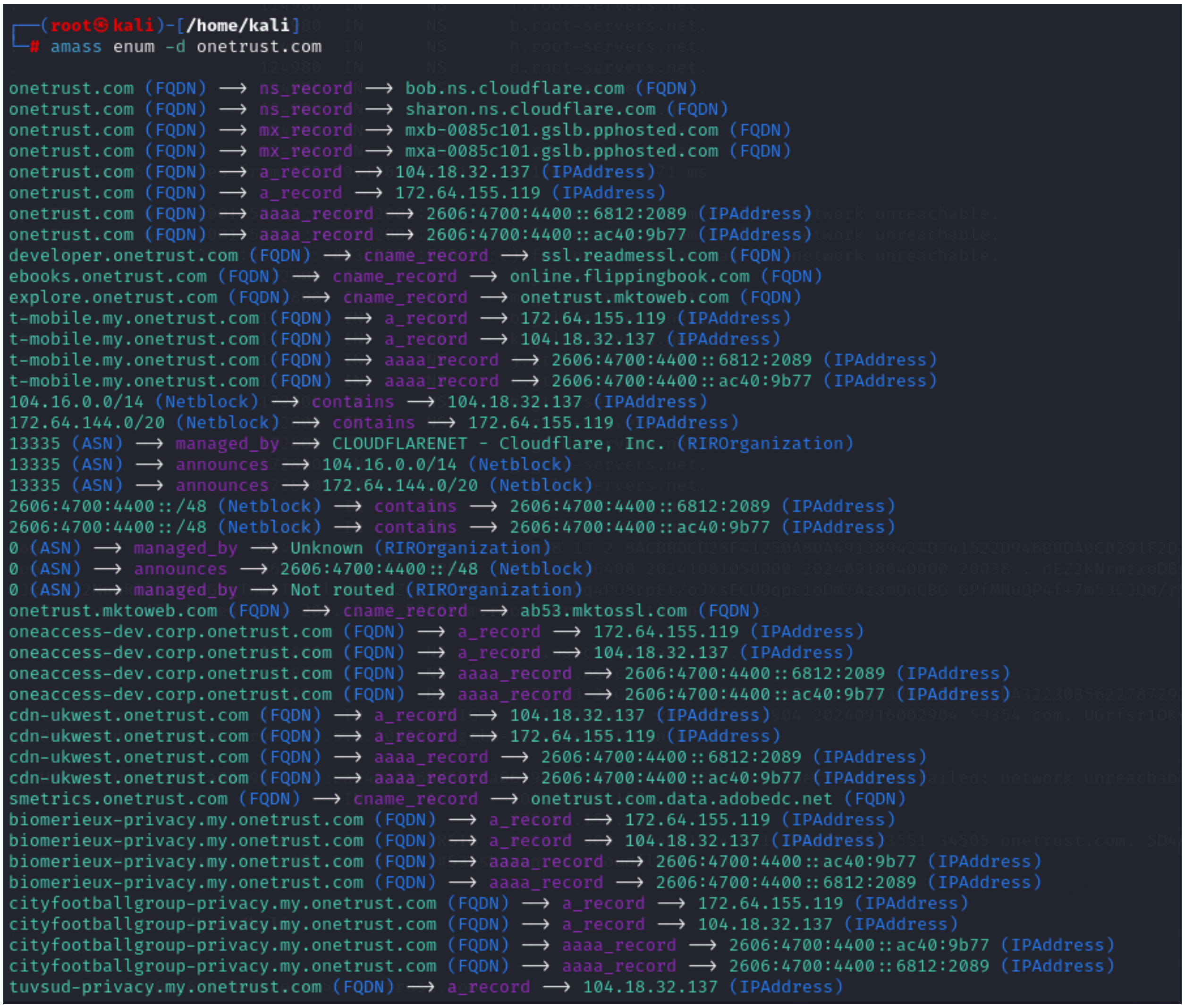
- www.app-jpmc.onetrust.com
- app-nbcu.onetrust.com
- www.app-nbcu.onetrust.com



```
┌──(root㉿kali)-[/home/kali]
└─# sublist3r -d onetrust.com

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for onetrust.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 297
www.onetrust.com
admin-portal-idp-sso-myot.onetrust.com
www.admin-portal-idp-sso-myot.onetrust.com
aem.onetrust.com
aem-dev.onetrust.com
aem-stage.onetrust.com
app.onetrust.com
www.app.onetrust.com
app-ae.onetrust.com
www.app-ae.onetrust.com
app-allstate.onetrust.com
www.app-allstate.onetrust.com
app-apac.onetrust.com
www.app-apac.onetrust.com
app-att.onetrust.com
www.app-att.onetrust.com
app-au.onetrust.com
www.app-au.onetrust.com
app-bofa.onetrust.com
www.app-bofa.onetrust.com
app-br.onetrust.com
```

And I tried amass command to get more detailed information about subdomains and dns records and here is an example:

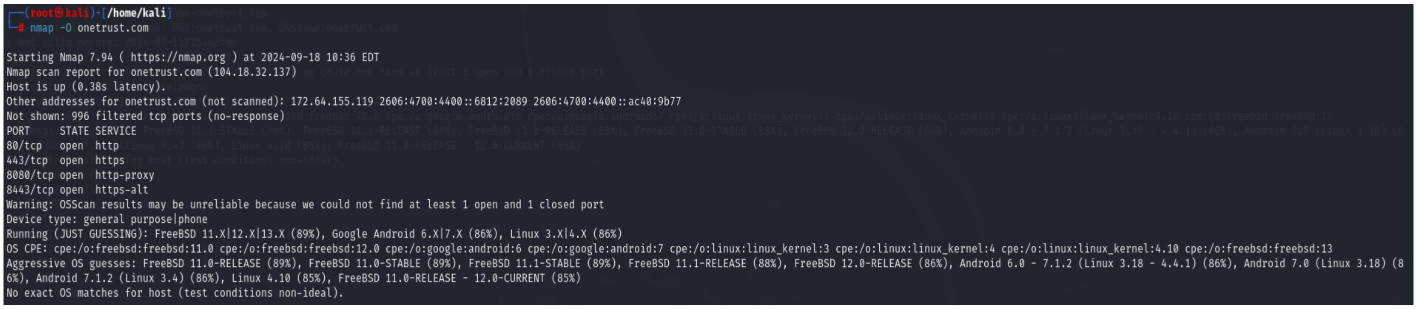
- vontier-privacy.my.onetrust.com (FQDN) --> a_record --> 104.18.32.137 (IPAddress)
- vontier-privacy.my.onetrust.com (FQDN) --> a_record --> 172.64.155.119 (IPAddress)
- vontier-privacy.my.onetrust.com (FQDN) --> aaaa_record --> 2a06:98c1:3122:e000::5 (IPAddress)
- vontier-privacy.my.onetrust.com (FQDN) --> aaaa_record --> 2a06:98c1:3123:e000::5 (IPAddress)



```
┌──(root㉿kali)-[/home/kali]
└─# amass enum -d onetrust.com

onetrust.com (FQDN) ⟶ ns_record ⟶ bob.ns.cloudflare.com (FQDN)
onetrust.com (FQDN) ⟶ ns_record ⟶ sharon.ns.cloudflare.com (FQDN)
onetrust.com (FQDN) ⟶ mx_record ⟶ mxb-0085c101.gslb.pphosted.com (FQDN)
onetrust.com (FQDN) ⟶ mx_record ⟶ mxa-0085c101.gslb.pphosted.com (FQDN)
onetrust.com (FQDN) ⟶ a_record ⟶ 104.18.32.137 (IPAddress)
onetrust.com (FQDN) ⟶ a_record ⟶ 172.64.155.119 (IPAddress)
onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::6812:2089 (IPAddress)
onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::ac40:9b77 (IPAddress)
developer.onetrust.com (FQDN) ⟶ cname_record ⟶ ssl.readmessl.com (FQDN)
ebooks.onetrust.com (FQDN) ⟶ cname_record ⟶ online.flippingbook.com (FQDN)
explore.onetrust.com (FQDN) ⟶ cname_record ⟶ onetrust.mktoweb.com (FQDN)
t-mobile.my.onetrust.com (FQDN) ⟶ a_record ⟶ 172.64.155.119 (IPAddress)
t-mobile.my.onetrust.com (FQDN) ⟶ a_record ⟶ 104.18.32.137 (IPAddress)
t-mobile.my.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::6812:2089 (IPAddress)
t-mobile.my.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::ac40:9b77 (IPAddress)
104.16.0.0/14 (Netblock) ⟶ contains ⟶ 104.18.32.137 (IPAddress)
172.64.144.0/20 (Netblock) ⟶ contains ⟶ 172.64.155.119 (IPAddress)
13335 (ASN) ⟶ managed_by ⟶ CLOUDFLARENET - Cloudflare, Inc. (RIROrganization)
13335 (ASN) ⟶ announces ⟶ 104.16.0.0/14 (Netblock)
13335 (ASN) ⟶ announces ⟶ 172.64.144.0/20 (Netblock)
2606:4700:4400::/48 (Netblock) ⟶ contains ⟶ 2606:4700:4400::6812:2089 (IPAddress)
2606:4700:4400::/48 (Netblock) ⟶ contains ⟶ 2606:4700:4400::ac40:9b77 (IPAddress)
0 (ASN) ⟶ managed_by ⟶ Unknown (RIROrganization)
0 (ASN) ⟶ announces ⟶ 2606:4700:4400::/48 (Netblock)
0 (ASN) ⟶ managed_by ⟶ Not routed (RIROrganization)
onetrust.mktoweb.com (FQDN) ⟶ cname_record ⟶ ab53.mktossl.com (FQDN)
oneaccess-dev.corp.onetrust.com (FQDN) ⟶ a_record ⟶ 172.64.155.119 (IPAddress)
oneaccess-dev.corp.onetrust.com (FQDN) ⟶ a_record ⟶ 104.18.32.137 (IPAddress)
oneaccess-dev.corp.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::6812:2089 (IPAddress)
oneaccess-dev.corp.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::ac40:9b77 (IPAddress)
cdn-ukwest.onetrust.com (FQDN) ⟶ a_record ⟶ 104.18.32.137 (IPAddress)
cdn-ukwest.onetrust.com (FQDN) ⟶ a_record ⟶ 172.64.155.119 (IPAddress)
cdn-ukwest.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::6812:2089 (IPAddress)
cdn-ukwest.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::ac40:9b77 (IPAddress)
smetrics.onetrust.com (FQDN) ⟶ cname_record ⟶ onetrust.com.data.adobedc.net (FQDN)
biomerieux-privacy.my.onetrust.com (FQDN) ⟶ a_record ⟶ 172.64.155.119 (IPAddress)
biomerieux-privacy.my.onetrust.com (FQDN) ⟶ a_record ⟶ 104.18.32.137 (IPAddress)
biomerieux-privacy.my.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::ac40:9b77 (IPAddress)
biomerieux-privacy.my.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::6812:2089 (IPAddress)
cityfootballgroup-privacy.my.onetrust.com (FQDN) ⟶ a_record ⟶ 172.64.155.119 (IPAddress)
cityfootballgroup-privacy.my.onetrust.com (FQDN) ⟶ a_record ⟶ 104.18.32.137 (IPAddress)
cityfootballgroup-privacy.my.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::ac40:9b77 (IPAddress)
cityfootballgroup-privacy.my.onetrust.com (FQDN) ⟶ aaaa_record ⟶ 2606:4700:4400::6812:2089 (IPAddress)
tuvsud-privacy.my.onetrust.com (FQDN) ⟶ a_record ⟶ 104.18.32.137 (IPAddress)
```

Then I used nmap -O to detect the Operating System and it is the summary of the result:

- Possible device types:
    - general purpose or phone
- Operating system guess:
    - FreeBSD 11.X, 12.X, 13.X (89%)
    - Google Android 6.X, 7.X (86%)
    - Linux 3.X, 4.X (86%)

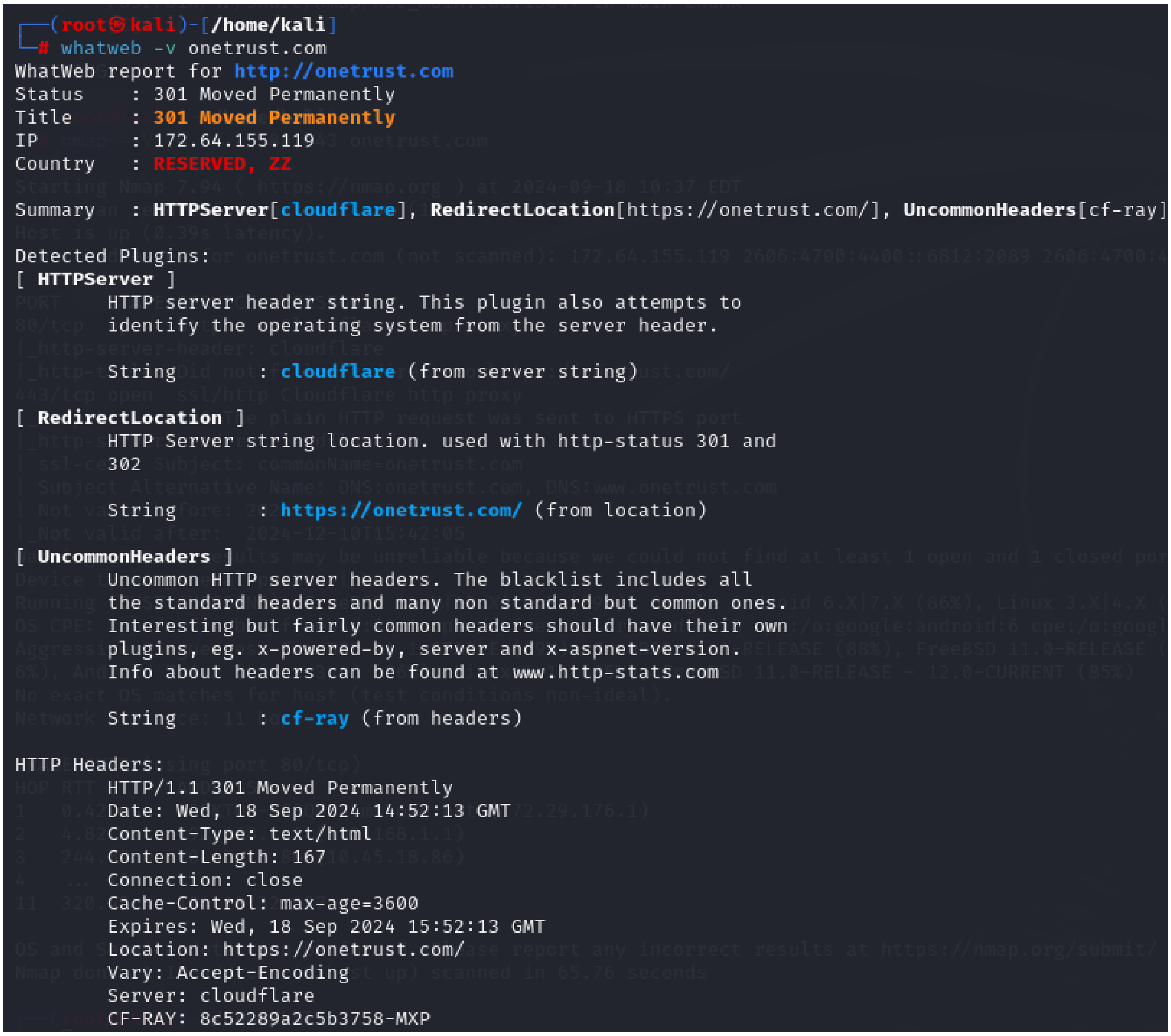


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O onetrust.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-18 10:36 EDT
Nmap scan report for onetrust.com (104.18.32.137)
Host is up (0.38s latency).
Other addresses for onetrust.com (not scanned): 172.64.155.119 2606:4700:4400::6812:2089 2606:4700:4400::ac40:9b77
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): FreeBSD 11.X|12.X|13.X (89%), Google Android 6.X|7.X (86%), Linux 3.X|4.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:11.0 cpe:/o:freebsd:freebsd:12.0 cpe:/o:google:android:6 cpe:/o:google:android:7 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:4.10 cpe:/o:freebsd:freebsd:13
Aggressive OS guesses: FreeBSD 11.0-RELEASE (89%), FreeBSD 11.0-STABLE (89%), FreeBSD 11.1-STABLE (89%), FreeBSD 11.1-RELEASE (88%), FreeBSD 12.0-RELEASE (86%), Android 6.0 - 7.1.2 (Linux 3.18 - 4.4.1) (86%), Android 7.0 (Linux 3.18) (8
6%), Android 7.1.2 (Linux 3.4) (86%), Linux 4.10 (85%), FreeBSD 11.0-RELEASE - 12.0-CURRENT (85%)
No exact OS matches for host (test conditions non-ideal).
```

And I used whatweb command to detect plugins and frameworks and it is the summary result of plugins:

- Adobe-Experience-Manager
    - Google Dorks: (1)
    - Website: https://www.adobe.com/marketing/experience-manager.html
- HTML5
    - HTML version 5, detected by the doctype declaration
- JQuery
    - Website: http://jquery.com/
- Script
    - String: module,x-template

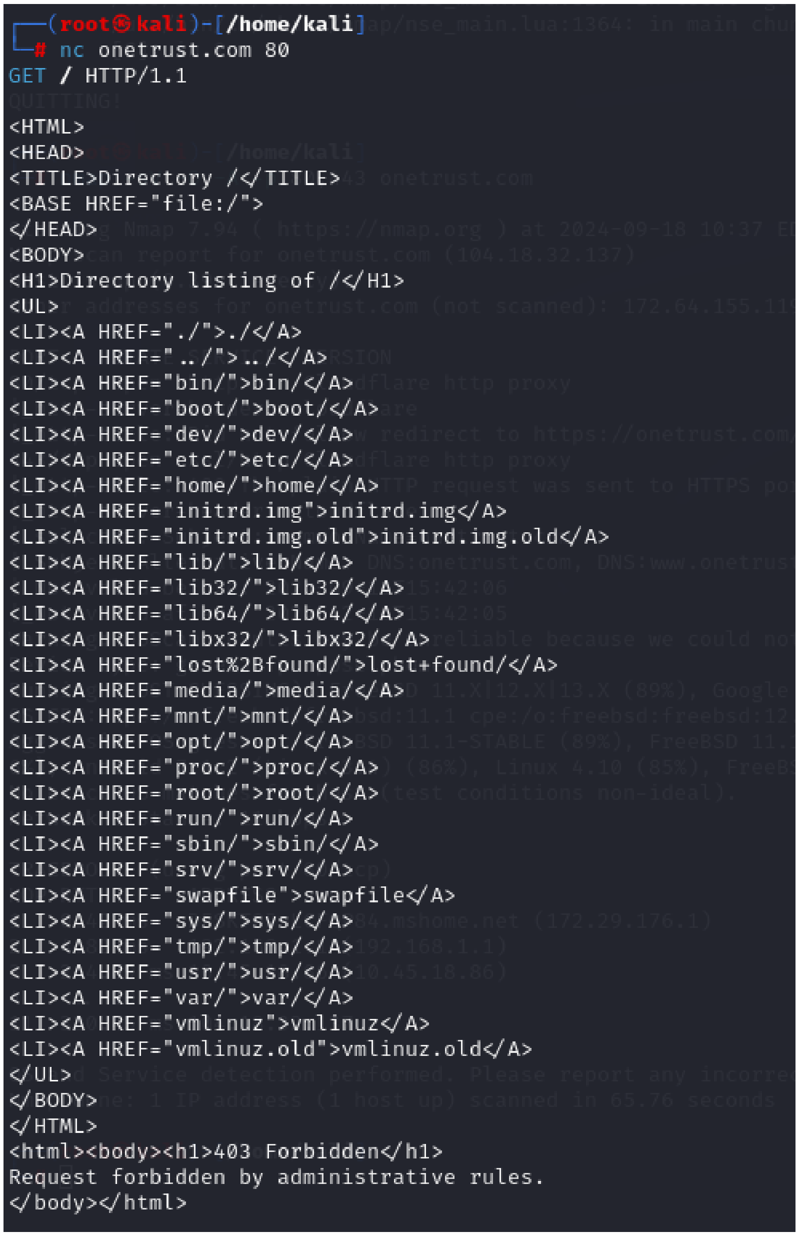
- Strict-Transport-Security
  - String: max-age=31536000; includeSubDomains; preload
- UncommonHeaders
  - String: x-sky-isauth, x-vhost, content-security-policy,x-content-type-options,x-served-by,x-timer,cf-cache-status,cf-ray (from headers)
- X-Frame-Options
  - String: SAMEORIGIN, SAMEORIGIN
- X-XSS-Protection
  - String: 1; mode=block



```
┌──(root㉿kali)-[/home/kali]
└─# whatweb -v onetrust.com
WhatWeb report for http://onetrust.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 172.64.155.119
Country   : RESERVED, ZZ

Summary   : HTTPServer[cloudflare], RedirectLocation[https://onetrust.com/], UncommonHeaders[cf-ray]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : cloudflare (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://onetrust.com/ (from location)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : cf-ray (from headers)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Date: Wed, 18 Sep 2024 14:52:13 GMT
        Content-Type: text/html
        Content-Length: 167
        Connection: close
        Cache-Control: max-age=3600
        Expires: Wed, 18 Sep 2024 15:52:13 GMT
        Location: https://onetrust.com/
        Vary: Accept-Encoding
        Server: cloudflare
        CF-RAY: 8c52289a2c5b3758-MXP
```

And I tried to get directory listing on port 80 by netcat command nc:

- It is the result of HTTP get request:



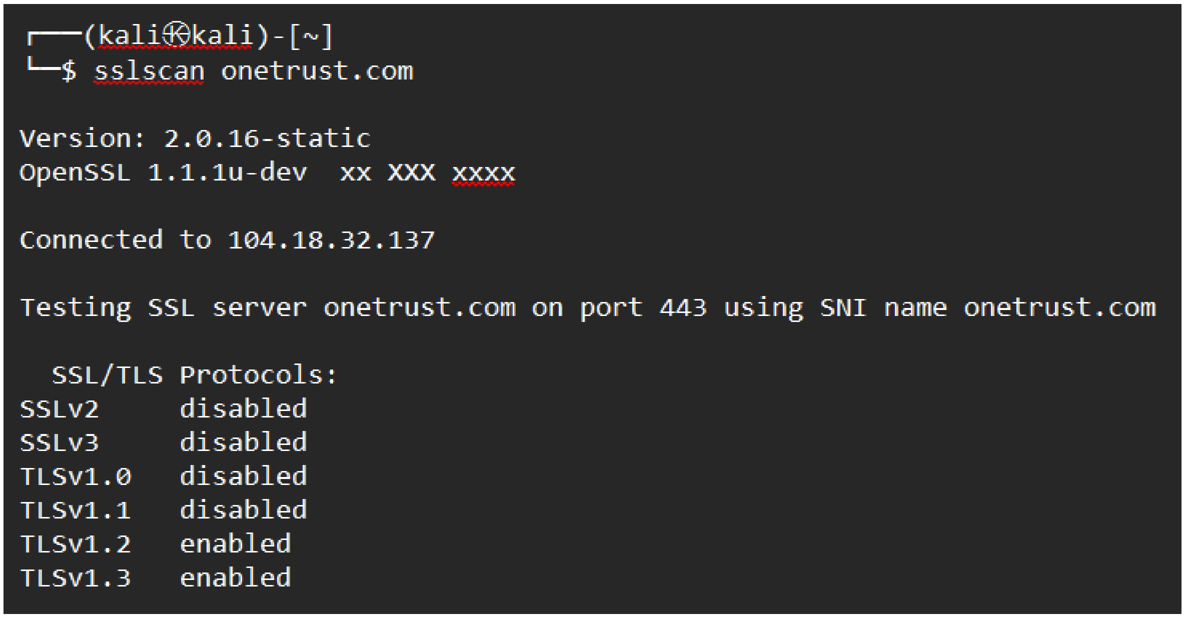
```
┌──(root㉿kali)-[/home/kali]
└─# nc onetrust.com 80
GET / HTTP/1.1
<HTML>
<HEAD>
<TITLE>Directory /</TITLE>
<BASE HREF="file:/">
</HEAD>
<BODY>
<H1>Directory listing of /</H1>
<UL>
<LI><A HREF="./">./</A>
<LI><A HREF="../">../</A>
<LI><A HREF="bin/">bin/</A>
<LI><A HREF="boot/">boot/</A>
<LI><A HREF="dev/">dev/</A>
<LI><A HREF="etc/">etc/</A>
<LI><A HREF="home/">home/</A>
<LI><A HREF="initrd.img">initrd.img</A>
<LI><A HREF="initrd.img.old">initrd.img.old</A>
<LI><A HREF="lib/">lib/</A>
<LI><A HREF="lib32/">lib32/</A>
<LI><A HREF="lib64/">lib64/</A>
<LI><A HREF="libx32/">libx32/</A>
<LI><A HREF="lost%2Bfound/">lost+found/</A>
<LI><A HREF="media/">media/</A>
<LI><A HREF="mnt/">mnt/</A>
<LI><A HREF="opt/">opt/</A>
<LI><A HREF="proc/">proc/</A>
<LI><A HREF="root/">root/</A>
<LI><A HREF="run/">run/</A>
<LI><A HREF="sbin/">sbin/</A>
<LI><A HREF="srv/">srv/</A>
<LI><A HREF="swapfile">swapfile</A>
<LI><A HREF="sys/">sys/</A>
<LI><A HREF="tmp/">tmp/</A>
<LI><A HREF="usr/">usr/</A>
<LI><A HREF="var/">var/</A>
<LI><A HREF="vmlinuz">vmlinuz</A>
<LI><A HREF="vmlinuz.old">vmlinuz.old</A>
</UL>
</BODY>
</HTML>
<html><body><h1>403 Forbidden</h1>
Request forbidden by administrative rules.
</body></html>
```

Finally, I used sslscan command to detect SSL protocols and its version and its cipher algorithms and it is the summary of the result:

“Before”

- OpenSSL version: 1.1.1u-dev
- TLSv1.2 and TLSv1.3 are enabled.
- SSLv2, SSLv3, TLSv1.0, and TLSv1.1 are disabled.

It is a vulnerability in this version:

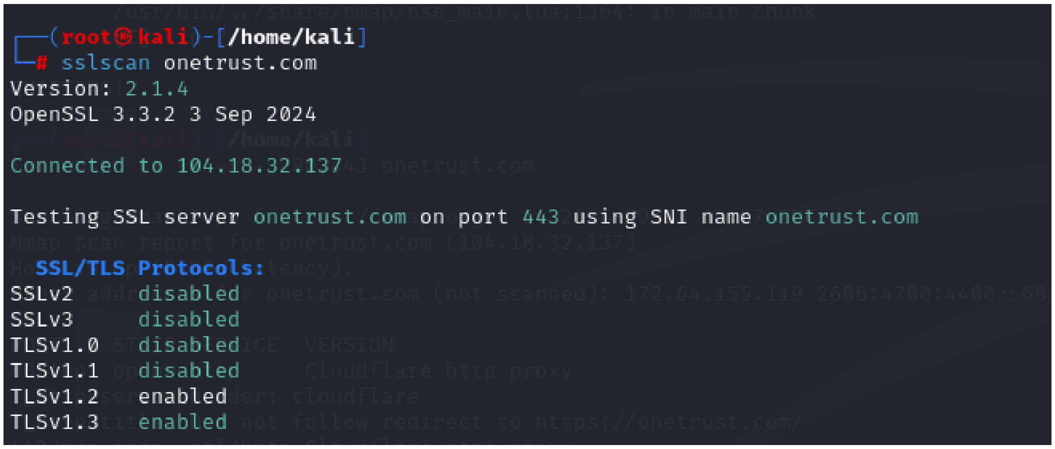


```
┌──(kali㉿kali)-[~]
└─$ sslscan onetrust.com

Version: 2.0.16-static
OpenSSL 1.1.1u-dev  xx XXX xxxx

Connected to 104.18.32.137

Testing SSL server onetrust.com on port 443 using SNI name onetrust.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled
```

And on the second day, the vulnerability was mitigated, and the OpenSSL version was updated to 3.3.2, as shown below:

“After”

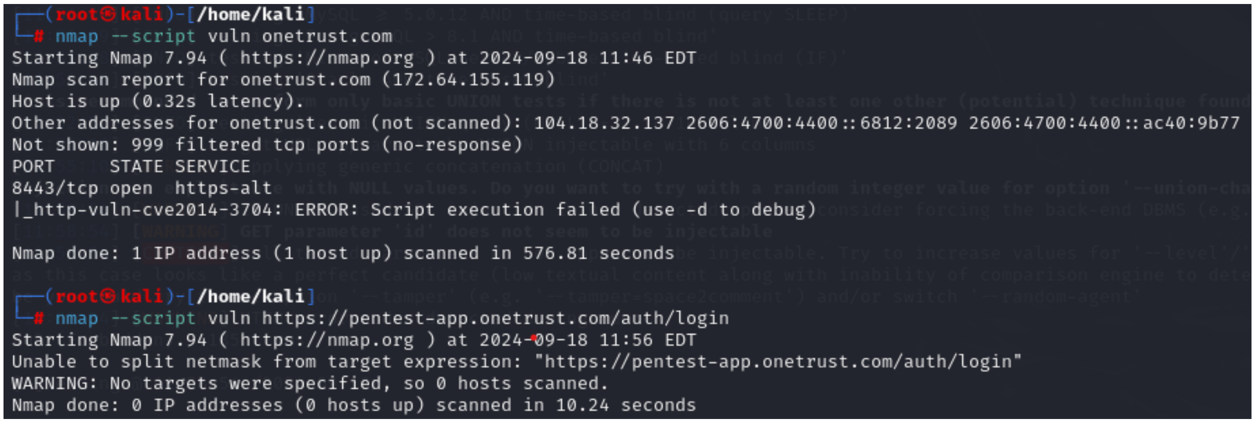
- OpenSSL version: 3.3.2
- TLSv1.2 and TLSv1.3 are enabled.
- SSLv2, SSLv3, TLSv1.0, and TLSv1.1 are disabled.



```
┌──(root㉿kali)-[/home/kali]
└─# sslscan onetrust.com
Version: 2.1.4
OpenSSL 3.3.2 3 Sep 2024

Connected to 104.18.32.137

Testing SSL server onetrust.com on port 443 using SNI name onetrust.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled
```

Then I tried nmap - -script for automatic vulnerability detection and didn’t find:

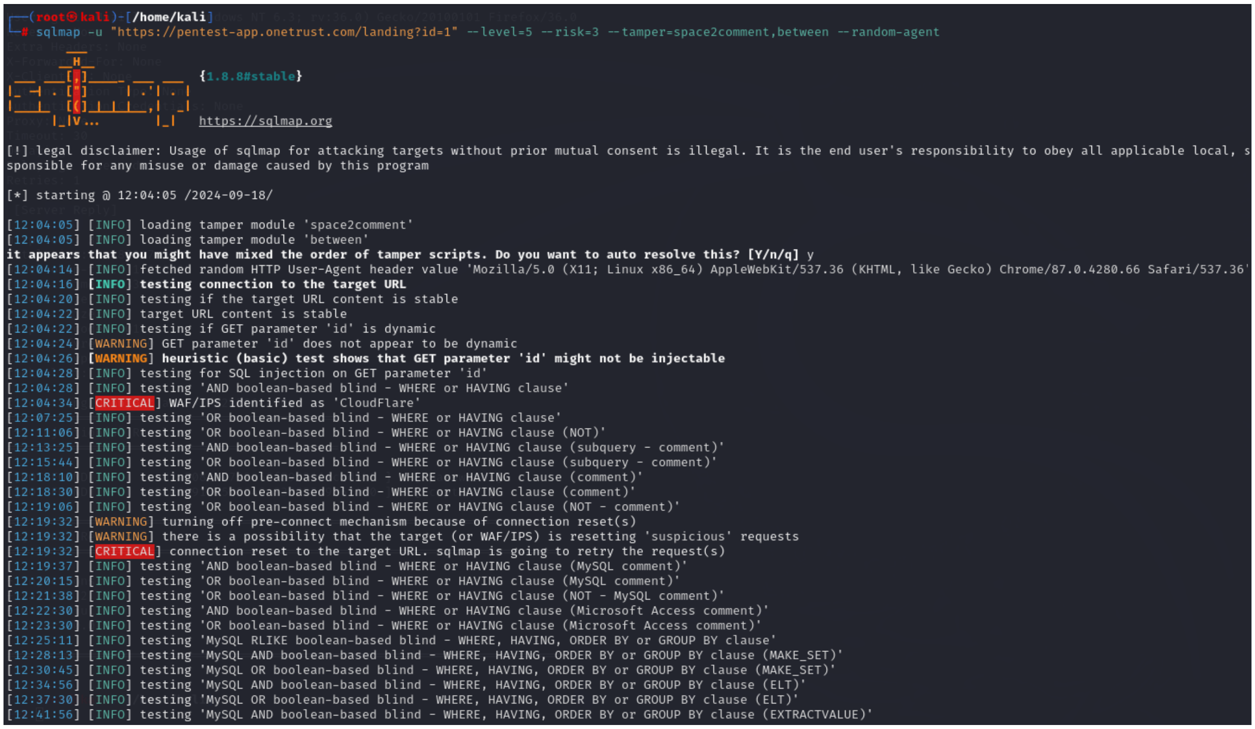
Ex:



```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script vuln onetrust.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-18 11:46 EDT
Nmap scan report for onetrust.com (172.64.155.119)
Host is up (0.32s latency).
Other addresses for onetrust.com (not scanned): 104.18.32.137 2606:4700:4400::6812:2089 2606:4700:4400::ac40:9b77
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
8443/tcp open  https-alt
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 576.81 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap --script vuln https://pentest-app.onetrust.com/auth/login
Starting Nmap 7.94 ( https://nmap.org ) at 2024-09-18 11:56 EDT
Unable to split netmask from target expression: "https://pentest-app.onetrust.com/auth/login"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.24 seconds
```

And tried sqlmap tool for any SQL injection type vulnerability and it wasn’t any of it:

Ex:

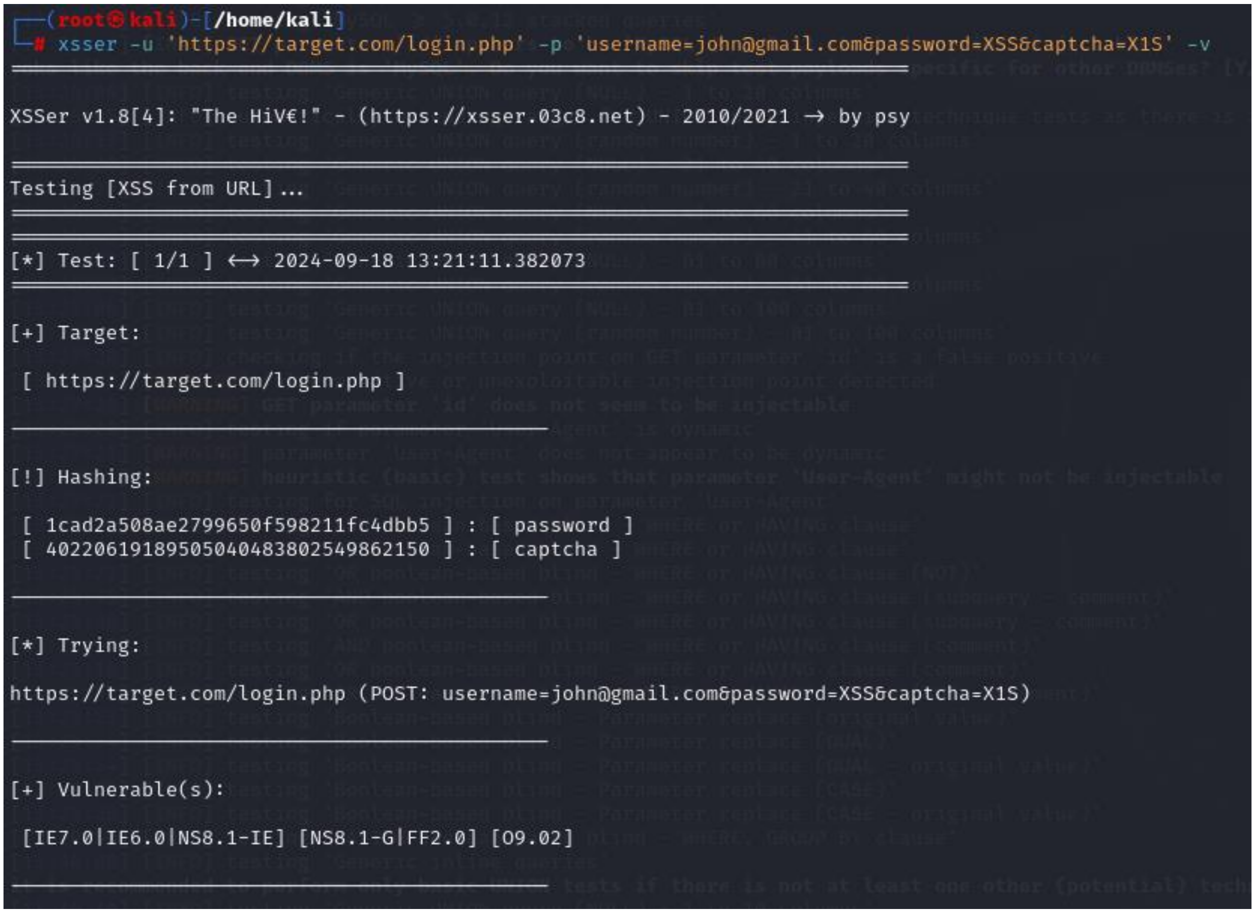


```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "https://pentest-app.onetrust.com/landing?id=1" --level=5 --risk=3 --tamper=space2comment,between --random-agent
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.8#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, s
sponsible for any misuse or damage caused by this program

[*] starting @ 12:04:05 /2024-09-18/

[12:04:05] [INFO] loading tamper module 'space2comment'
[12:04:05] [INFO] loading tamper module 'between'
it appears that you might have mixed the order of tamper scripts. Do you want to auto resolve this? [Y/n/q] y
[12:04:14] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36'
[12:04:16] [INFO] testing connection to the target URL
[12:04:20] [INFO] testing if the target URL content is stable
[12:04:22] [INFO] target URL content is stable
[12:04:22] [INFO] testing if GET parameter 'id' is dynamic
[12:04:24] [WARNING] GET parameter 'id' does not appear to be dynamic
[12:04:26] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[12:04:28] [INFO] testing for SQL injection on GET parameter 'id'
[12:04:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:04:34] [CRITICAL] WAF/IPS identified as 'CloudFlare'
[12:07:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[12:11:06] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[12:13:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[12:15:44] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[12:18:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[12:18:30] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[12:19:06] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[12:19:32] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[12:19:32] [WARNING] there is a possibility that the target (or WAF/IPS) is resetting 'suspicious' requests
[12:19:32] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[12:19:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[12:20:15] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[12:21:38] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[12:22:30] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[12:23:30] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[12:25:11] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[12:28:13] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[12:30:45] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[12:34:56] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[12:37:30] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[12:41:56] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
```

And tried xsser tool for xss vulnerability and didn’t find:

Ex:

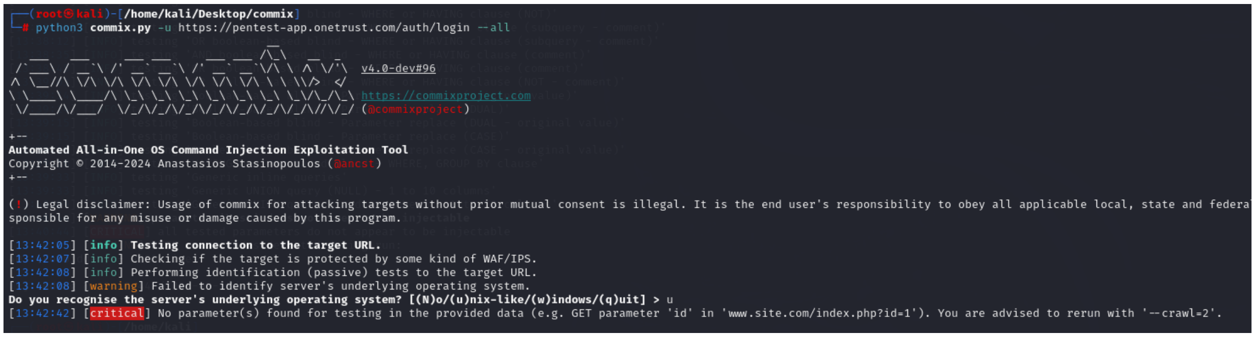
- Final Results:
  - Injections: 2
  - Failed: 2
  - Successful: 0
  - Accur: 0.0 %



```
┌──(root㉿kali)-[/home/kali]
└─# xsser -u 'https://target.com/login.php' -p 'username=john@gmail.com&password=XSS&captcha=X1S' -v
===========================================================================

XSSer v1.8[4]: "The HiV€!" - (https://xsser.03c8.net) - 2010/2021 → by psy

===========================================================================
Testing [XSS from URL]...
===========================================================================
===========================================================================
[*] Test: [ 1/1 ] <-> 2024-09-18 13:21:11.382073
===========================================================================

[+] Target:

 [ https://target.com/login.php ]

---------------------------------------------

[!] Hashing:

 [ 1cad2a508ae2799650f598211fc4dbb5 ] : [ password ]
 [ 4022061918950504048380254986215O ] : [ captcha ]

---------------------------------------------

[*] Trying:

https://target.com/login.php (POST: username=john@gmail.com&password=XSS&captcha=X1S)

---------------------------------------------

[+] Vulnerable(s):

 [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]

---------------------------------------------
```

And tried commix tool for command injection vulnerability and didn't find any parameter:

Ex:



```
┌──(root㉿kali)-[/home/kali/Desktop/commix]
└─# python3 commix.py -u https://pentest-app.onetrust.com/auth/login --all
                                      __
   ___   ___     ___ ___     ___ ___ /\_\   __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v4.0-dev#96
/\ \__//\ \/\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \\/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_/\//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2024 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federa
sponsible for any misuse or damage caused by this program.

[13:42:05] [info] Testing connection to the target URL.
[13:42:07] [info] Checking if the target is protected by some kind of WAF/IPS.
[13:42:08] [info] Performing identification (passive) tests to the target URL.
[13:42:08] [warning] Failed to identify server's underlying operating system.
Do you recognise the server's underlying operating system? [(N)o/(u)nix-like/(w)indows/(q)uit] > u
[13:42:42] [critical] No parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--crawl=2'.
```

Tools Used:

- Reconnaissance Tools:
  - whois: To gather domain registration and owner information.
  - wafw00f: To detect the presence of a Web Application Firewall (WAF).
  - nslookup: To gather DNS records and IP addresses.
  - dig: To perform detailed DNS queries.
  - sublist3r: For subdomain discovery.
  - amass: To discover additional subdomains and DNS records.

- Enumeration Tools:
  - nmap -sS -sV: For service version detection and port scanning.
  - nmap -O: For operating system detection.
  - whatweb: For identifying web technologies, plugins, and frameworks.
  - netcat (nc): To test for open services, such as HTTP, and attempt directory listing.
  - sslscan: To scan for SSL/TLS protocols and cipher suites.

- Exploitation Tools:
  - nmap --script: To run automated vulnerability detection scripts.
  - sqlmap: To check for SQL injection vulnerabilities.
  - xsser: To test for cross-site scripting (XSS) vulnerabilities.
  - commix: To check for command injection vulnerabilities.

Reference: https://openssl-library.org/news/secadv/20230328.txt