IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

Report 04 - Ubisoft

Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

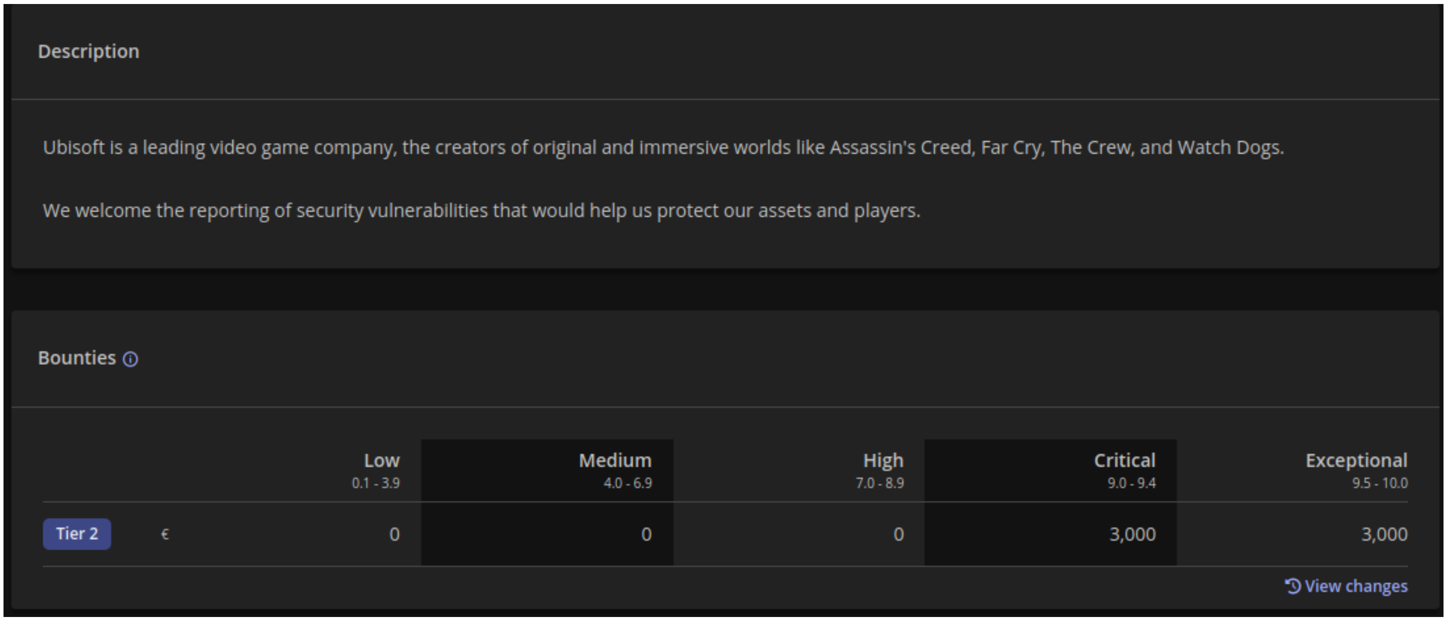
Contents

1. Ubisoft/Ubisoft VDP/Detail

Public Open

Ubisoft / Ubisoft VDP / Detail

1.1. Overview



Description

Ubisoft is a leading video game company, the creators of original and immersive worlds like Assassin's Creed, Far Cry, The Crew, and Watch Dogs.

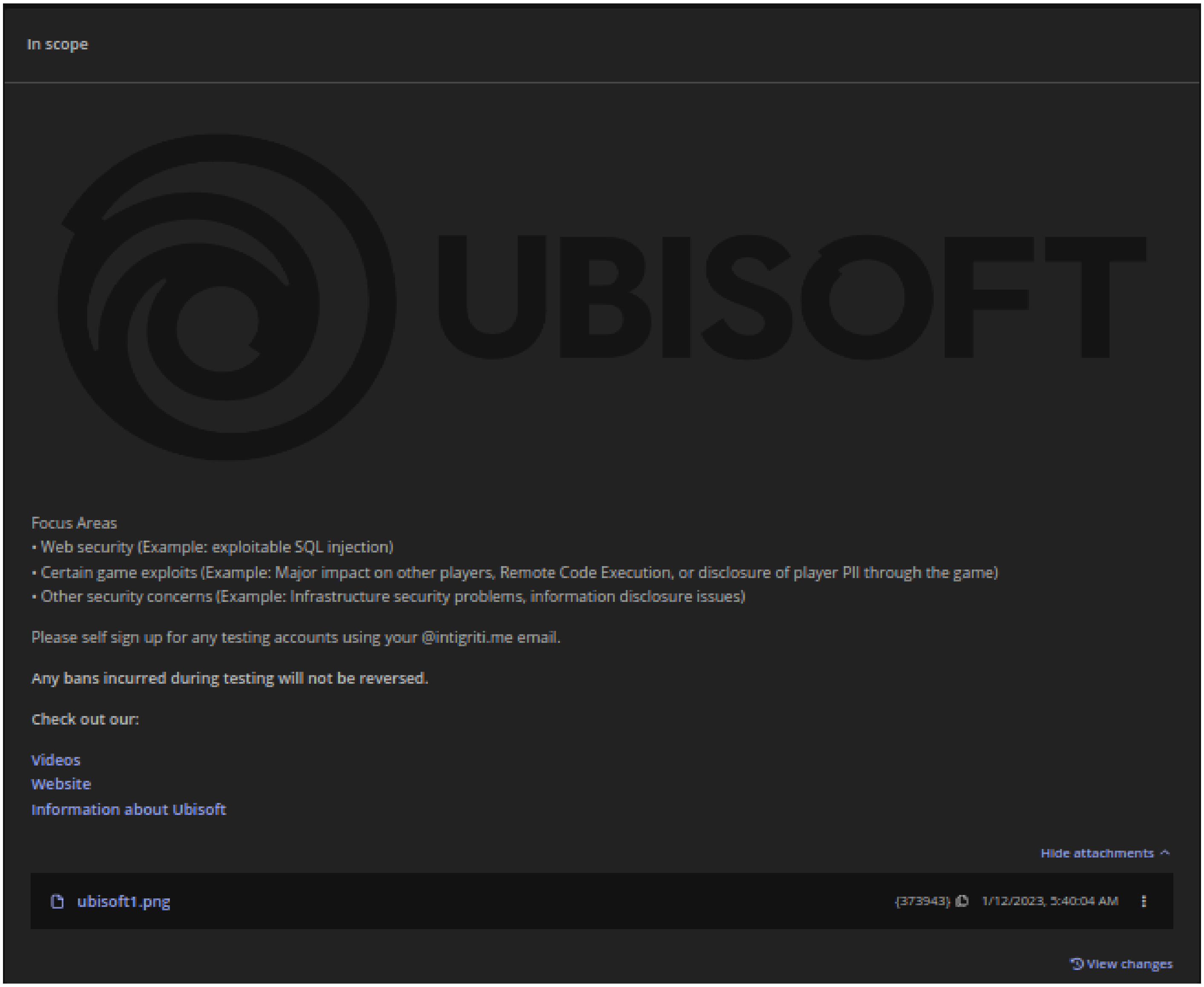
We welcome the reporting of security vulnerabilities that would help us protect our assets and players.

Bounties ⓘ

		Low 0.1 - 3.9	Medium 4.0 - 6.9	High 7.0 - 8.9	Critical 9.0 - 9.4	Exceptional 9.5 - 10.0
Tier 2	€	0	0	0	3,000	3,000

View changes

1.2.Scope



Focus Areas
- Web security (Example: exploitable SQL injection)
- Certain game exploits (Example: Major impact on other players, Remote Code Execution, or disclosure of player PII through the game)
- Other security concerns (Example: Infrastructure security problems, information disclosure issues)

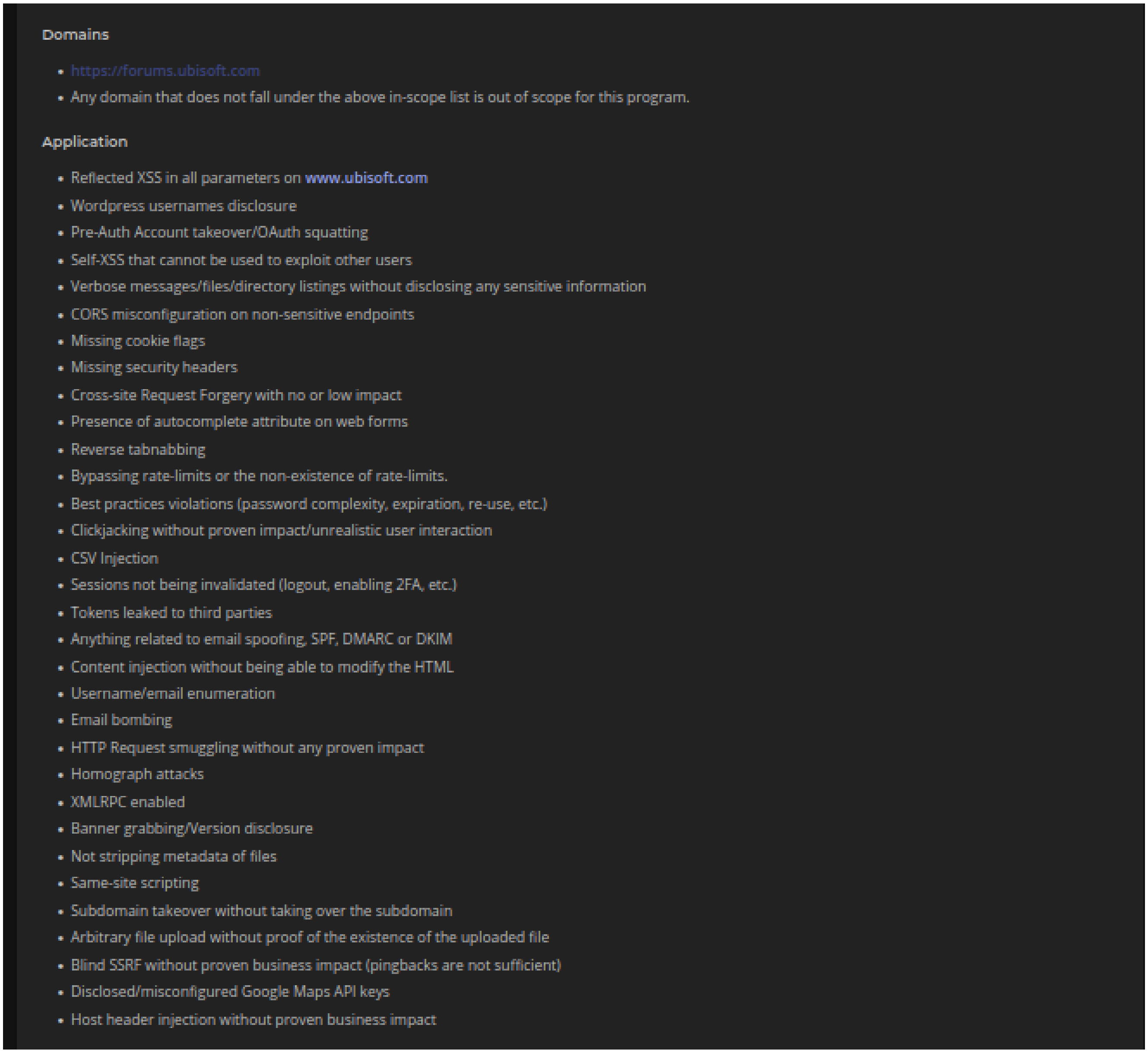
Please self sign up for any testing accounts using your @intigriti.me email.

Any bans incurred during testing will not be reversed.

Check out our:

Videos
Website
Information about Ubisoft

1.3.Out of Scope

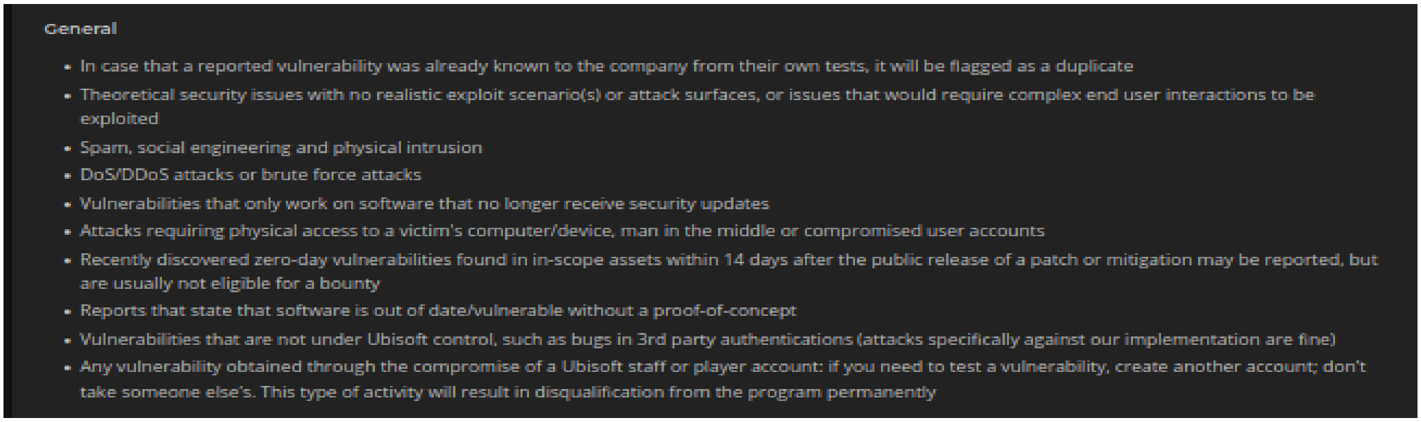


Domains

- https://forums.ubisoft.com
- Any domain that does not fall under the above in-scope list is out of scope for this program.

Application

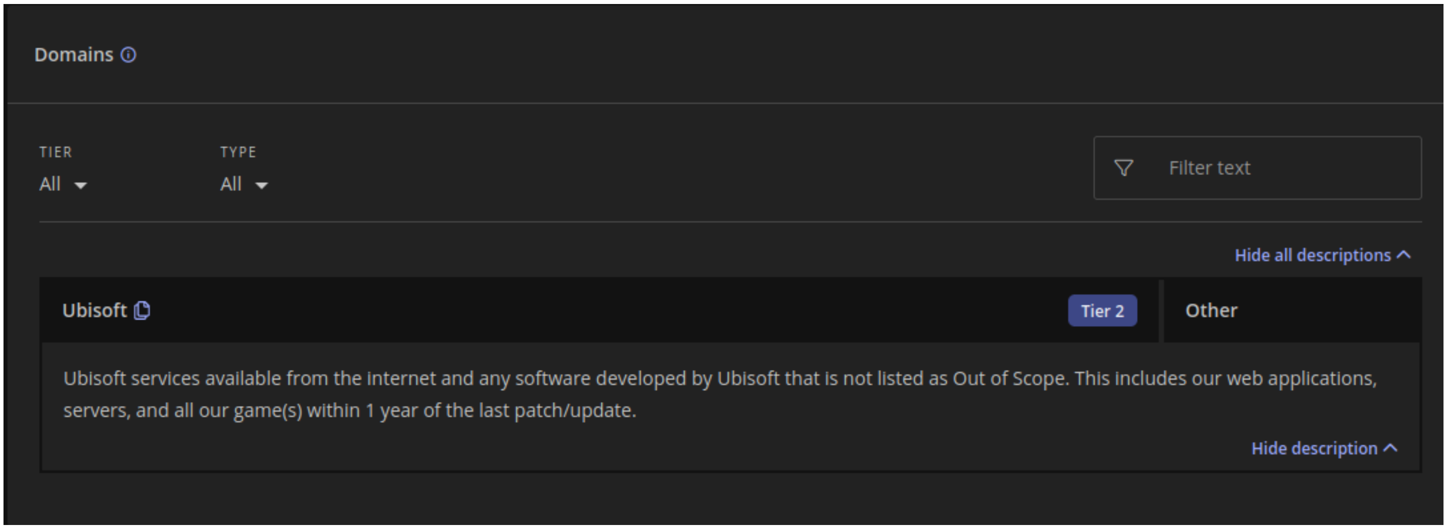
- Reflected XSS in all parameters on www.ubisoft.com
- Wordpress usernames disclosure
- Pre-Auth Account takeover/OAuth squatting
- Self-XSS that cannot be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non-sensitive endpoints
- Missing cookie flags
- Missing security headers
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking without proven impact/unrealistic user interaction
- CSV Injection
- Sessions not being invalidated (logout, enabling 2FA, etc.)
- Tokens leaked to third parties
- Anything related to email spoofing, SPF, DMARC or DKIM
- Content injection without being able to modify the HTML
- Username/email enumeration
- Email bombing
- HTTP Request smuggling without any proven impact
- Homograph attacks
- XMLRPC enabled
- Banner grabbing/Version disclosure
- Not stripping metadata of files
- Same-site scripting
- Subdomain takeover without taking over the subdomain
- Arbitrary file upload without proof of the existence of the uploaded file
- Blind SSRF without proven business impact (pingbacks are not sufficient)
- Disclosed/misconfigured Google Maps API keys
- Host header injection without proven business impact



General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks
- Vulnerabilities that only work on software that no longer receive security updates
- Attacks requiring physical access to a victim's computer/device, man in the middle or compromised user accounts
- Recently discovered zero-day vulnerabilities found in in-scope assets within 14 days after the public release of a patch or mitigation may be reported, but are usually not eligible for a bounty
- Reports that state that software is out of date/vulnerable without a proof-of-concept
- Vulnerabilities that are not under Ubisoft control, such as bugs in 3rd party authentications (attacks specifically against our implementation are fine)
- Any vulnerability obtained through the compromise of a Ubisoft staff or player account: if you need to test a vulnerability, create another account; don't take someone else's. This type of activity will result in disqualification from the program permanently

1.4.Selected Domains



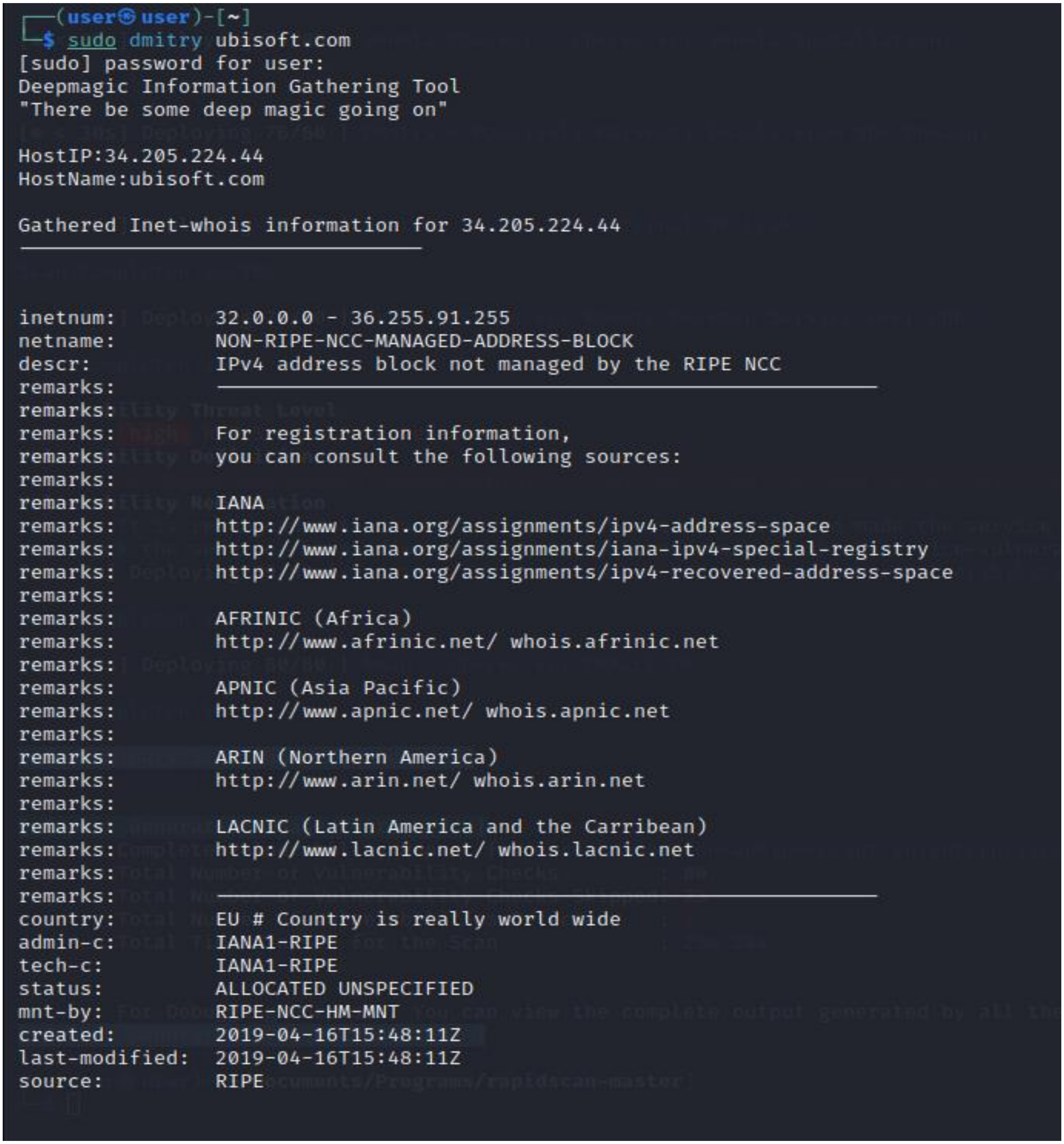
Ubisoft Tier 2 Other

Ubisoft services available from the internet and any software developed by Ubisoft that is not listed as Out of Scope. This includes our web applications, servers, and all our game(s) within 1 year of the last patch/update.

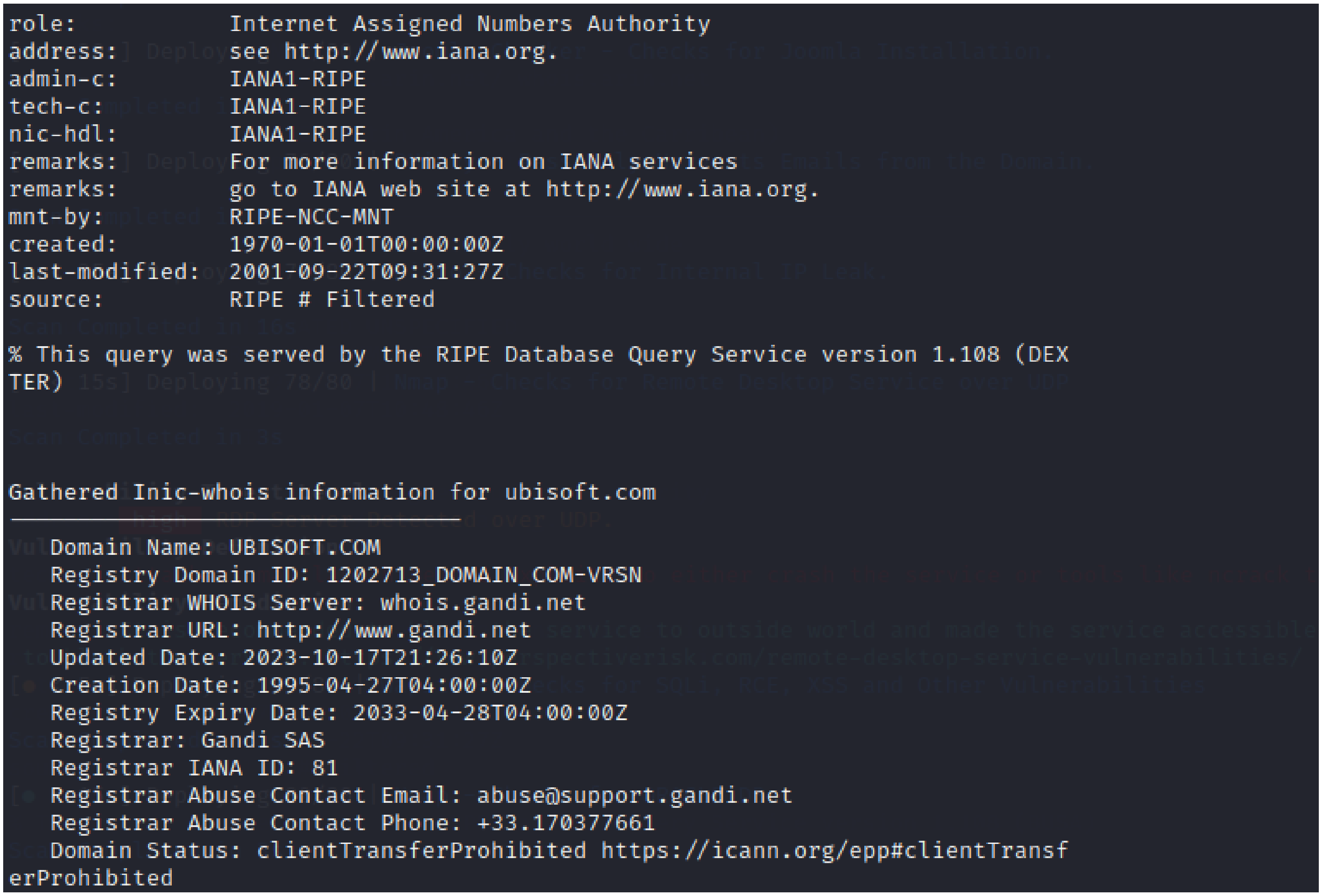
This URL https://www.ubisoft.com/en-us/ used in this report

2. Information Gathering

1.1.Using Dimity

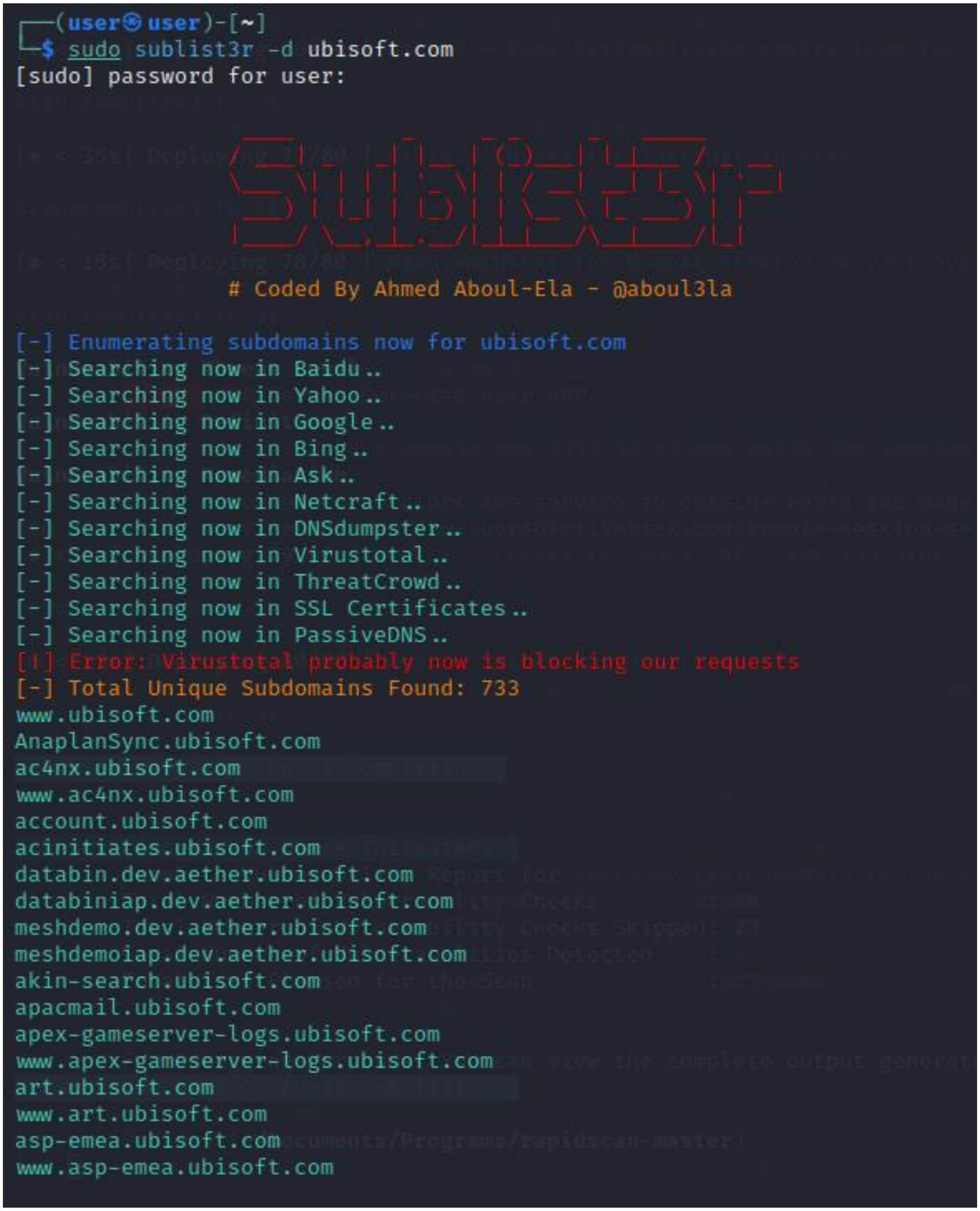


```
┌──(user㉿user)-[~]
└─$ sudo dmitry ubisoft.com
[sudo] password for user:
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:34.205.224.44
HostName:ubisoft.com

Gathered Inet-whois information for 34.205.224.44
─────────────────────────────────


inetnum:        32.0.0.0 - 36.255.91.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ──────────────────────────────────────────────────────
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ──────────────────────────────────────────────────────
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2019-04-16T15:48:11Z
last-modified:  2019-04-16T15:48:11Z
source:         RIPE
```

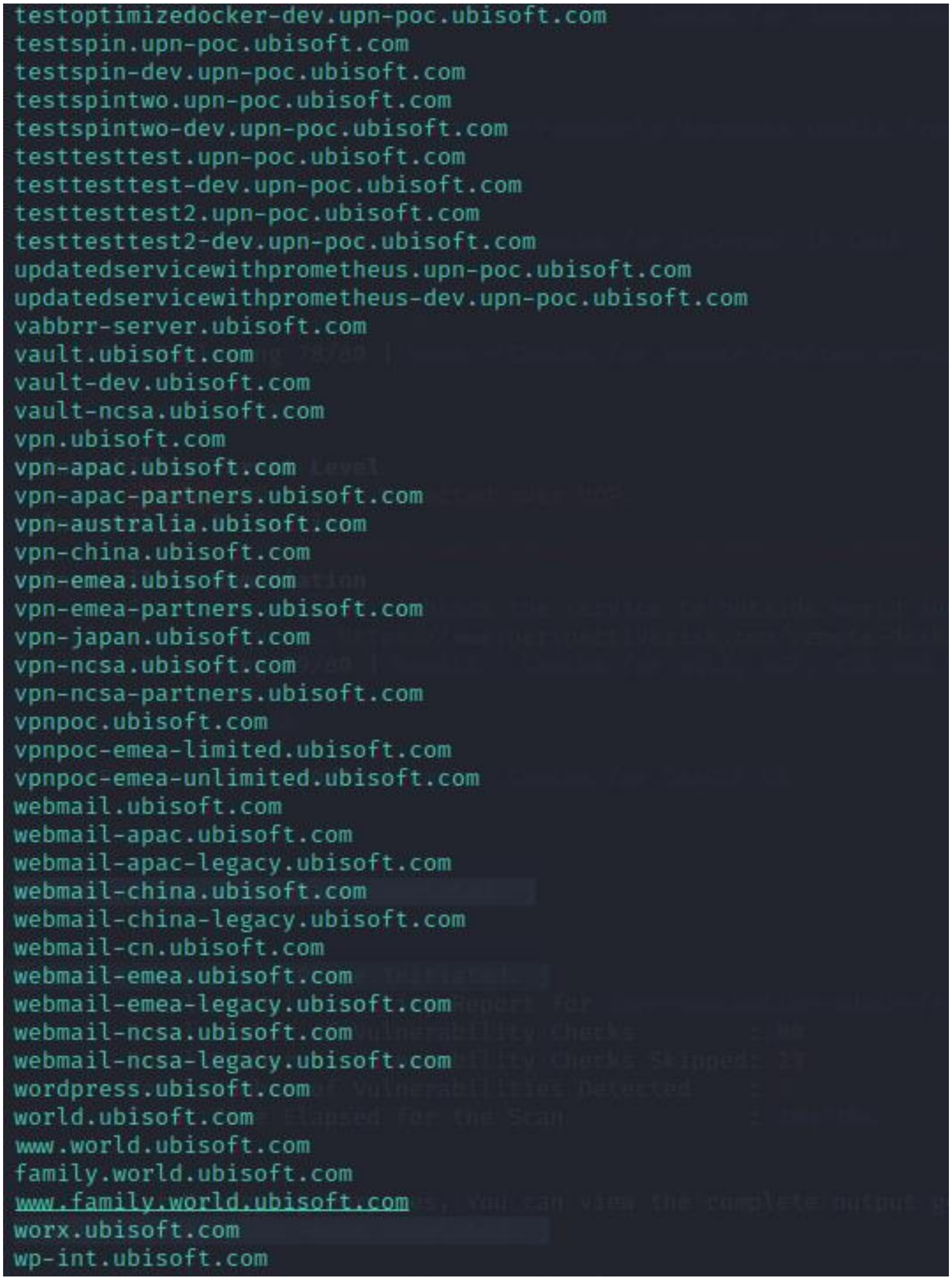


```
role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.108 (DEX
TER)


Gathered Inic-whois information for ubisoft.com
─────────────────────────────────
   Domain Name: UBISOFT.COM
   Registry Domain ID: 1202713_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.gandi.net
   Registrar URL: http://www.gandi.net
   Updated Date: 2023-10-17T21:26:10Z
   Creation Date: 1995-04-27T04:00:00Z
   Registry Expiry Date: 2033-04-28T04:00:00Z
   Registrar: Gandi SAS
   Registrar IANA ID: 81
   Registrar Abuse Contact Email: abuse@support.gandi.net
   Registrar Abuse Contact Phone: +33.170377661
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
```

1.2.Using sublist3r

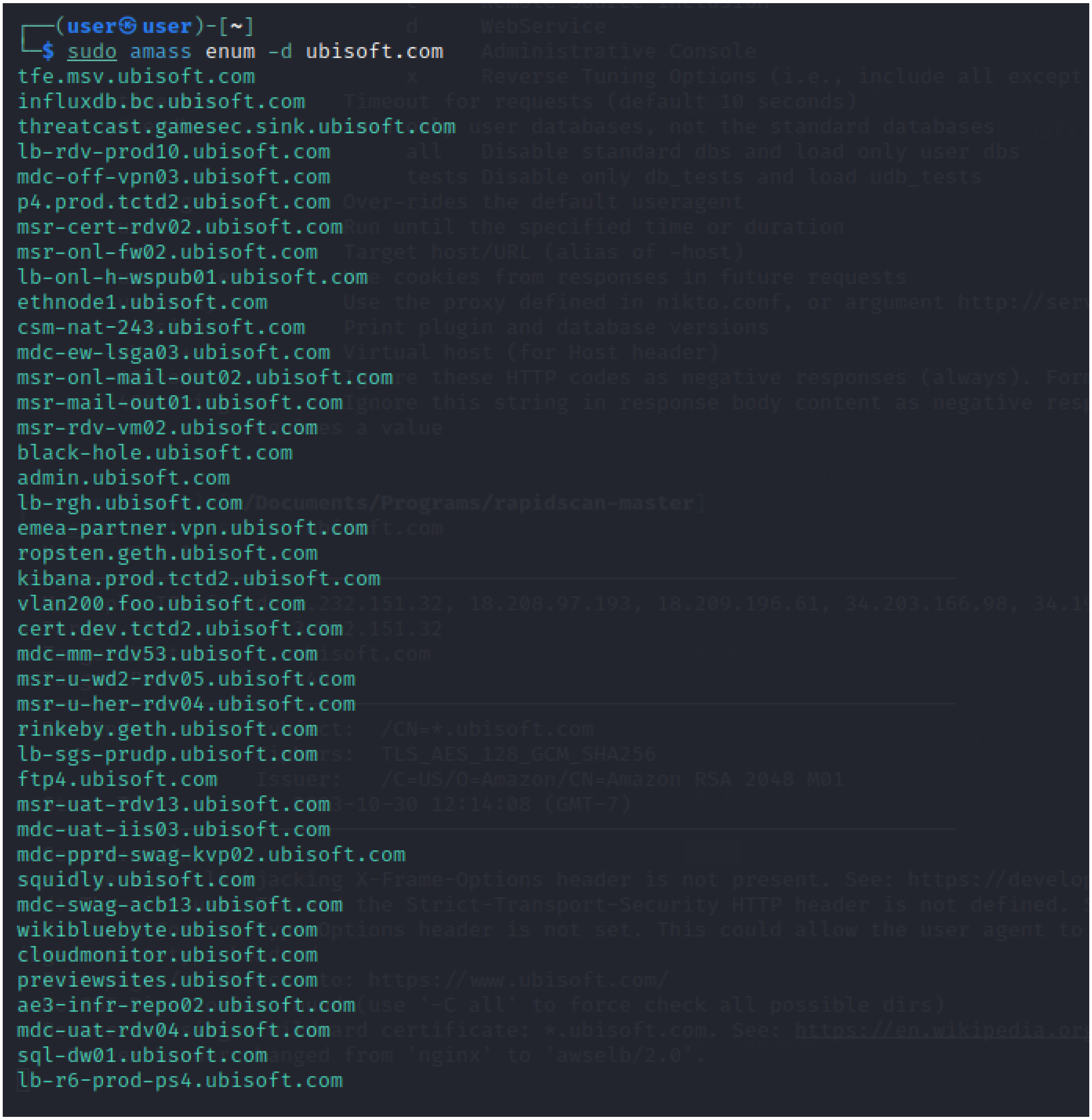


```
┌──(user㉿user)-[~]
└─$ sudo sublist3r -d ubisoft.com
[sudo] password for user:

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

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for ubisoft.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: 733
www.ubisoft.com
AnaplanSync.ubisoft.com
ac4nx.ubisoft.com
www.ac4nx.ubisoft.com
account.ubisoft.com
acinitiates.ubisoft.com
databin.dev.aether.ubisoft.com
databiniap.dev.aether.ubisoft.com
meshdemo.dev.aether.ubisoft.com
meshdemoiap.dev.aether.ubisoft.com
akin-search.ubisoft.com
apacmail.ubisoft.com
apex-gameserver-logs.ubisoft.com
www.apex-gameserver-logs.ubisoft.com
art.ubisoft.com
www.art.ubisoft.com
asp-emea.ubisoft.com
www.asp-emea.ubisoft.com
```



```
testoptimizedocker-dev.upn-poc.ubisoft.com
testspin.upn-poc.ubisoft.com
testspin-dev.upn-poc.ubisoft.com
testspintwo.upn-poc.ubisoft.com
testspintwo-dev.upn-poc.ubisoft.com
testtesttest.upn-poc.ubisoft.com
testtesttest-dev.upn-poc.ubisoft.com
testtesttest2.upn-poc.ubisoft.com
testtesttest2-dev.upn-poc.ubisoft.com
updatedservicewithprometheus.upn-poc.ubisoft.com
updatedservicewithprometheus-dev.upn-poc.ubisoft.com
vabbrr-server.ubisoft.com
vault.ubisoft.com
vault-dev.ubisoft.com
vault-ncsa.ubisoft.com
vpn.ubisoft.com
vpn-apac.ubisoft.com
vpn-apac-partners.ubisoft.com
vpn-australia.ubisoft.com
vpn-china.ubisoft.com
vpn-emea.ubisoft.com
vpn-emea-partners.ubisoft.com
vpn-japan.ubisoft.com
vpn-ncsa.ubisoft.com
vpn-ncsa-partners.ubisoft.com
vpnpoc.ubisoft.com
vpnpoc-emea-limited.ubisoft.com
vpnpoc-emea-unlimited.ubisoft.com
webmail.ubisoft.com
webmail-apac.ubisoft.com
webmail-apac-legacy.ubisoft.com
webmail-china.ubisoft.com
webmail-china-legacy.ubisoft.com
webmail-cn.ubisoft.com
webmail-emea.ubisoft.com
webmail-emea-legacy.ubisoft.com
webmail-ncsa.ubisoft.com
webmail-ncsa-legacy.ubisoft.com
wordpress.ubisoft.com
world.ubisoft.com
www.world.ubisoft.com
family.world.ubisoft.com
www.family.world.ubisoft.com
worx.ubisoft.com
wp-int.ubisoft.com
```

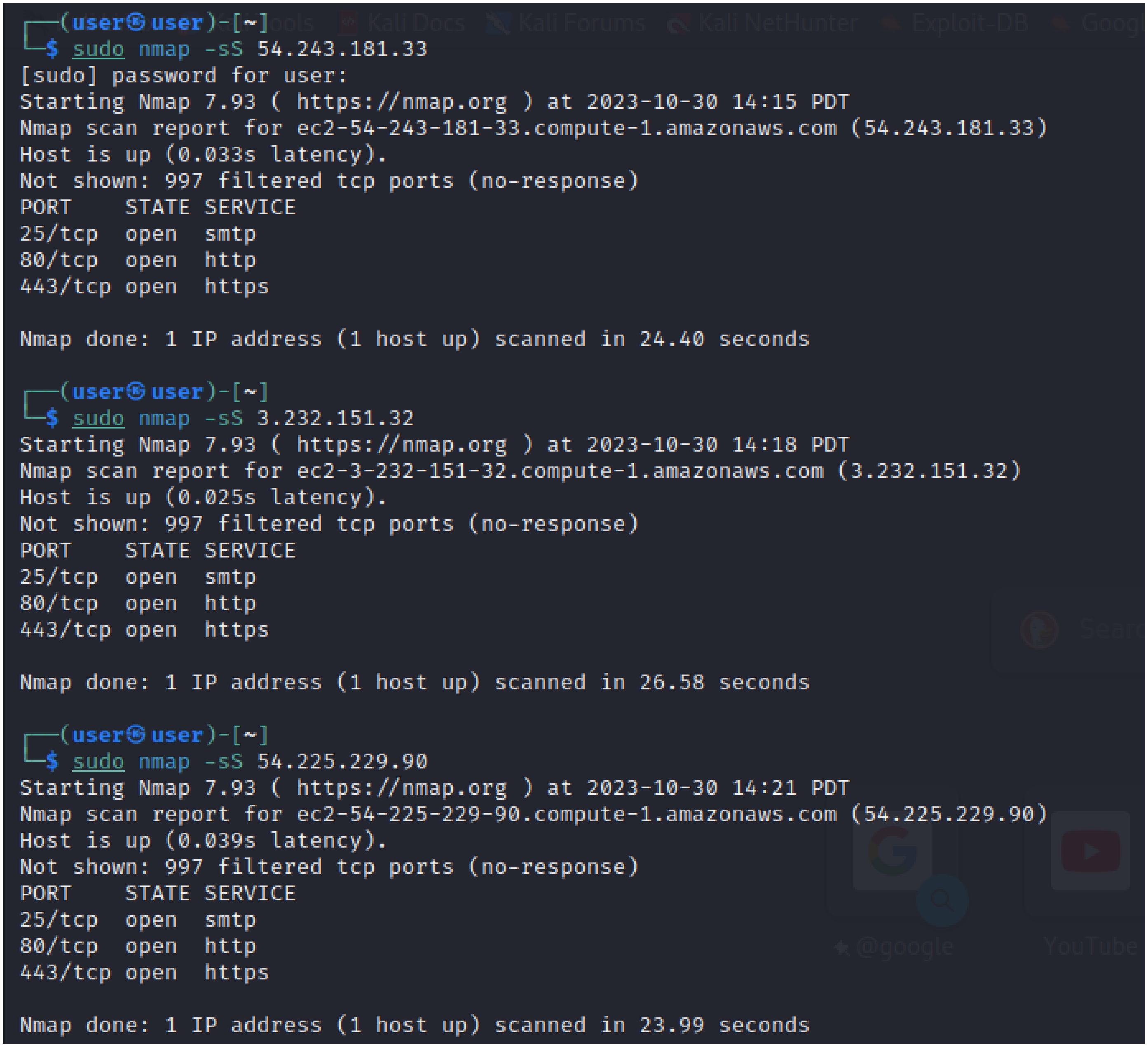
1.3. Using Amass



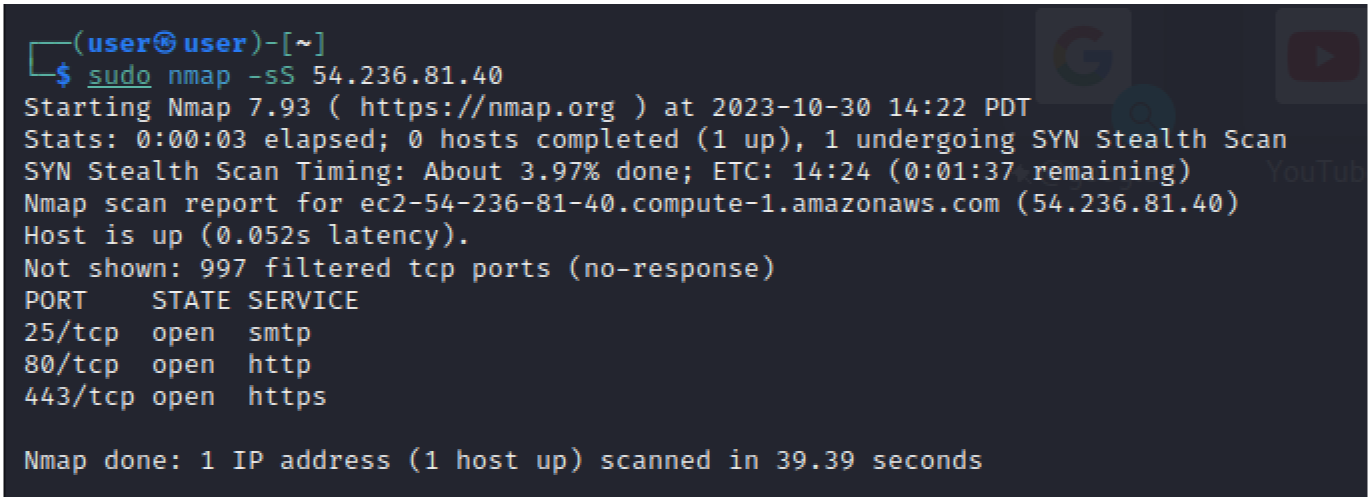
```
┌──(user㉿user)-[~]
└─$ sudo amass enum -d ubisoft.com
tfe.msv.ubisoft.com
influxdb.bc.ubisoft.com
threatcast.gamesec.sink.ubisoft.com
lb-rdv-prod10.ubisoft.com
mdc-off-vpn03.ubisoft.com
p4.prod.tctd2.ubisoft.com
msr-cert-rdv02.ubisoft.com
msr-onl-fw02.ubisoft.com
lb-onl-h-wspub01.ubisoft.com
ethnode1.ubisoft.com
csm-nat-243.ubisoft.com
mdc-ew-lsga03.ubisoft.com
msr-onl-mail-out02.ubisoft.com
msr-mail-out01.ubisoft.com
msr-rdv-vm02.ubisoft.com
black-hole.ubisoft.com
admin.ubisoft.com
lb-rgh.ubisoft.com
emea-partner.vpn.ubisoft.com
ropsten.geth.ubisoft.com
kibana.prod.tctd2.ubisoft.com
vlan200.foo.ubisoft.com
cert.dev.tctd2.ubisoft.com
mdc-mm-rdv53.ubisoft.com
msr-u-wd2-rdv05.ubisoft.com
msr-u-her-rdv04.ubisoft.com
rinkeby.geth.ubisoft.com
lb-sgs-prudp.ubisoft.com
ftp4.ubisoft.com
msr-uat-rdv13.ubisoft.com
mdc-uat-iis03.ubisoft.com
mdc-pprd-swag-kvp02.ubisoft.com
squidly.ubisoft.com
mdc-swag-acb13.ubisoft.com
wikibluebyte.ubisoft.com
cloudmonitor.ubisoft.com
previewsites.ubisoft.com
ae3-infr-repo02.ubisoft.com
mdc-uat-rdv04.ubisoft.com
sql-dw01.ubisoft.com
lb-r6-prod-ps4.ubisoft.com
```

3. Scanning Vulnerability

3.1.Using Nmap



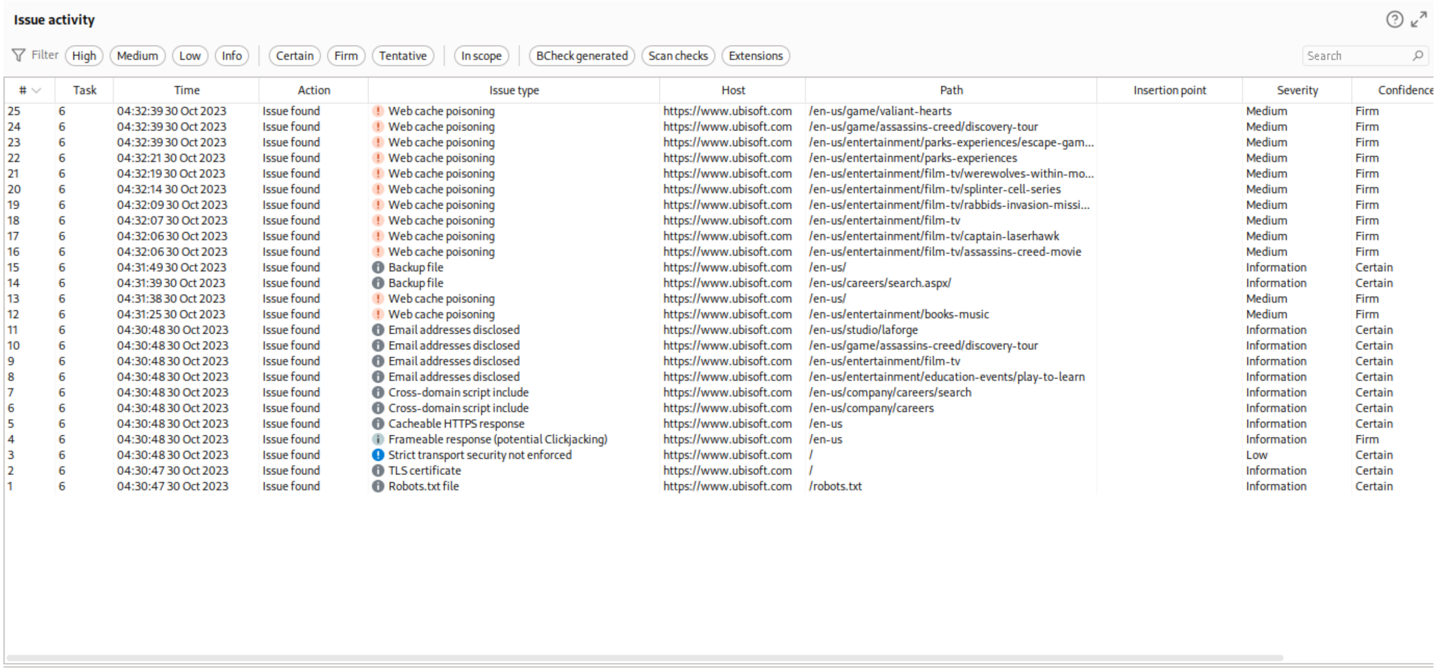
```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 54.243.181.33
[sudo] password for user:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 14:15 PDT
Nmap scan report for ec2-54-243-181-33.compute-1.amazonaws.com (54.243.181.33)
Host is up (0.033s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 24.40 seconds

┌──(user㉿user)-[~]
└─$ sudo nmap -sS 3.232.151.32
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 14:18 PDT
Nmap scan report for ec2-3-232-151-32.compute-1.amazonaws.com (3.232.151.32)
Host is up (0.025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 26.58 seconds

┌──(user㉿user)-[~]
└─$ sudo nmap -sS 54.225.229.90
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 14:21 PDT
Nmap scan report for ec2-54-225-229-90.compute-1.amazonaws.com (54.225.229.90)
Host is up (0.039s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 23.99 seconds
```



```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 54.236.81.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 14:22 PDT
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.97% done; ETC: 14:24 (0:01:37 remaining)
Nmap scan report for ec2-54-236-81-40.compute-1.amazonaws.com (54.236.81.40)
Host is up (0.052s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 39.39 seconds
```

3.2.Burp suite

- Using burp suite to scan the vulnerabilities.

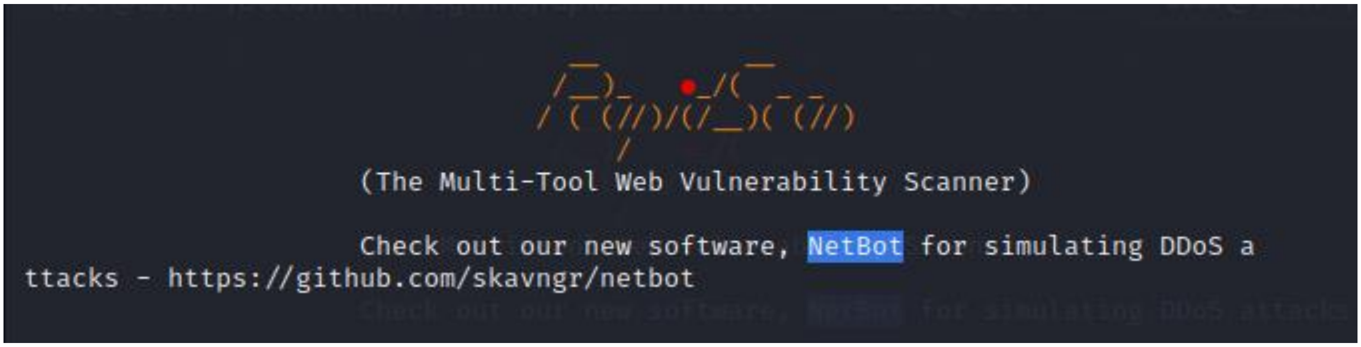


Issue activity

#	Task	Time	Action	Issue type	Host	Path	Insertion point	Severity	Confidence
25	6	04:32:39 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/game/valiant-hearts		Medium	Firm
24	6	04:32:39 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/game/assassins-creed/discovery-tour		Medium	Firm
23	6	04:32:39 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/parks-experiences/escape-gam...		Medium	Firm
22	6	04:32:21 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/parks-experiences		Medium	Firm
21	6	04:32:19 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/werewolves-within-mo...		Medium	Firm
20	6	04:32:14 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/splinter-cell-series		Medium	Firm
19	6	04:32:09 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/rabbids-invasion-missi...		Medium	Firm
18	6	04:32:07 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv		Medium	Firm
17	6	04:32:06 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/captain-laserhawk		Medium	Firm
16	6	04:32:06 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/film-tv/assassins-creed-movie		Medium	Firm
15	6	04:31:49 30 Oct 2023	Issue found	ℹ Backup file	https://www.ubisoft.com	/en-us/		Information	Certain
14	6	04:31:39 30 Oct 2023	Issue found	ℹ Backup file	https://www.ubisoft.com	/en-us/careers/search.aspx/		Information	Certain
13	6	04:31:38 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/		Medium	Firm
12	6	04:31:25 30 Oct 2023	Issue found	! Web cache poisoning	https://www.ubisoft.com	/en-us/entertainment/books-music		Medium	Firm
11	6	04:30:48 30 Oct 2023	Issue found	ℹ Email addresses disclosed	https://www.ubisoft.com	/en-us/studio/laforge		Information	Certain
10	6	04:30:48 30 Oct 2023	Issue found	ℹ Email addresses disclosed	https://www.ubisoft.com	/en-us/game/assassins-creed/discovery-tour		Information	Certain
9	6	04:30:48 30 Oct 2023	Issue found	ℹ Email addresses disclosed	https://www.ubisoft.com	/en-us/entertainment/film-tv		Information	Certain
8	6	04:30:48 30 Oct 2023	Issue found	ℹ Email addresses disclosed	https://www.ubisoft.com	/en-us/entertainment/education-events/play-to-learn		Information	Certain
7	6	04:30:48 30 Oct 2023	Issue found	ℹ Cross-domain script include	https://www.ubisoft.com	/en-us/company/careers/search		Information	Certain
6	6	04:30:48 30 Oct 2023	Issue found	ℹ Cross-domain script include	https://www.ubisoft.com	/en-us/company/careers		Information	Certain
5	6	04:30:48 30 Oct 2023	Issue found	ℹ Cacheable HTTPS response	https://www.ubisoft.com	/en-us		Information	Certain
4	6	04:30:48 30 Oct 2023	Issue found	ℹ Frameable response (potential Clickjacking)	https://www.ubisoft.com	/en-us		Information	Firm
3	6	04:30:48 30 Oct 2023	Issue found	! Strict transport security not enforced	https://www.ubisoft.com	/		Low	Certain
2	6	04:30:47 30 Oct 2023	Issue found	ℹ TLS certificate	https://www.ubisoft.com	/		Information	Certain
1	6	04:30:47 30 Oct 2023	Issue found	ℹ Robots.txt file	https://www.ubisoft.com	/robots.txt		Information	Certain

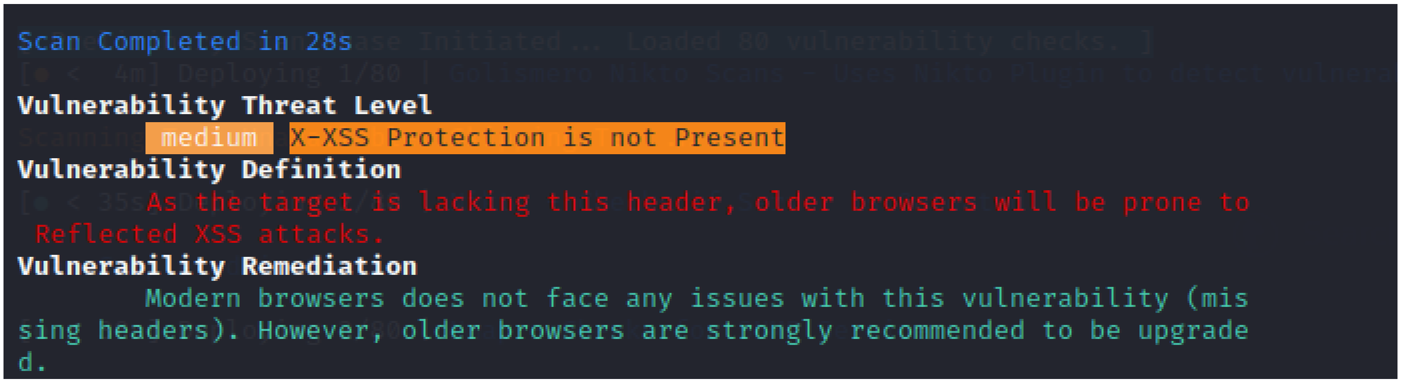
- Web Cache Poisoning
- Email address disclosed.
- Cross domain script included.

3.3.Using RapidScan



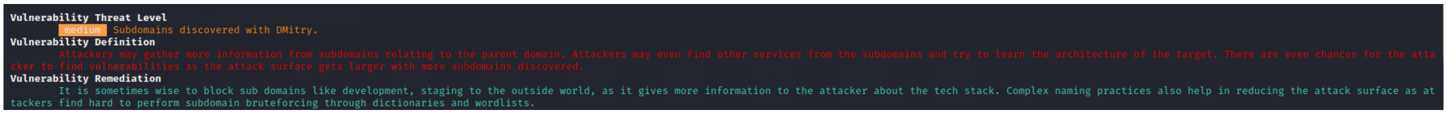
```
(The Multi-Tool Web Vulnerability Scanner)

                     Check out our new software, NetBot for simulating DDoS a
ttacks - https://github.com/skavngr/netbot
```

- X-XSS Protection is not Present.



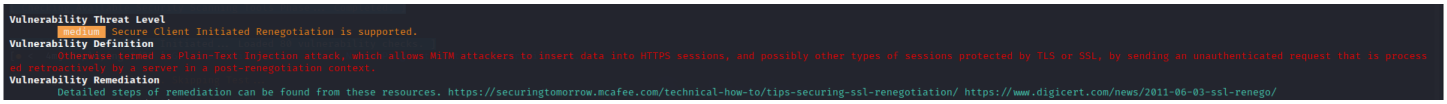
```
Scan Completed in 28s
Vulnerability Threat Level
         medium   X-XSS Protection is not Present
Vulnerability Definition
         As the target is lacking this header, older browsers will be prone to
 Reflected XSS attacks.
Vulnerability Remediation
         Modern browsers does not face any issues with this vulnerability (mis
sing headers). However, older browsers are strongly recommended to be upgrade
d.
```

- Subdomains discovered with Dmitry.



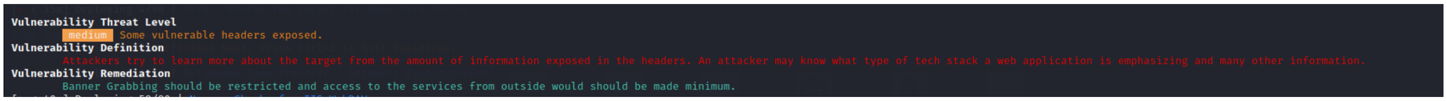
```
Vulnerability Threat Level
        medium  Subdomains discovered with DMitry.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances for the atta
cker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface as at
tackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

- Secure Client Initiated Renegotiation is supported.



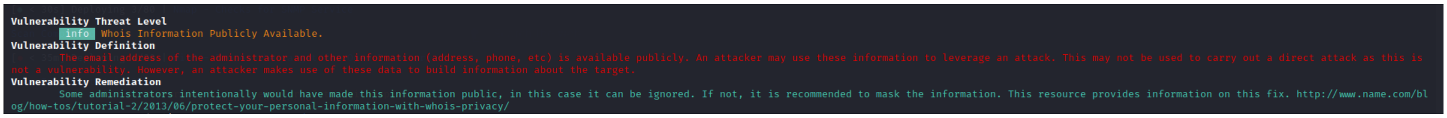
```
Vulnerability Threat Level
        medium  Secure Client Initiated Renegotiation is supported.
Vulnerability Definition
        Otherwise termed as Plain-Text Injection attack, which allows MiTM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is process
ed retroactively by a server in a post-renegotiation context.
Vulnerability Remediation
        Detailed steps of remediation can be found from these resources. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/
```

- Some vulnerable headers exposed.

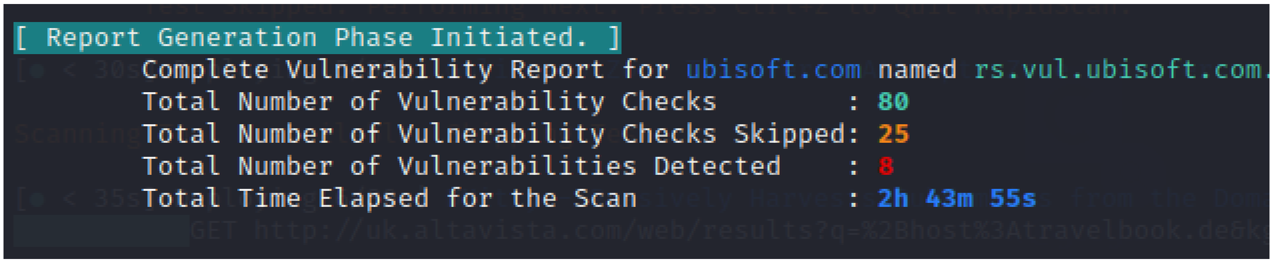


```
Vulnerability Threat Level
        medium  Some vulnerable headers exposed.
Vulnerability Definition
        Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.
Vulnerability Remediation
        Banner Grabbing should be restricted and access to the services from outside would should be made minimum.
```

- WHOIS Information Publicly Available.



```
Vulnerability Threat Level
        info  Whois Information Publicly Available.
Vulnerability Definition
        The email address of the administrator and other information (address, phone, etc) is available publicly. An attacker may use these information to leverage an attack. This may not be used to carry out a direct attack as this is
not a vulnerability. However, an attacker makes use of these data to build information about the target.
Vulnerability Remediation
        Some administrators intentionally would have made this information public, in this case it can be ignored. If not, it is recommended to mask the information. This resource provides information on this fix. http://www.name.com/bl
og/how-tos/tutorial-2/2013/06/protect-your-personal-information-with-whois-privacy/
```



```
[ Report Generation Phase Initiated. ]
               Complete Vulnerability Report for ubisoft.com named rs.vul.ubisoft.com.
               Total Number of Vulnerability Checks         : 80
               Total Number of Vulnerability Checks Skipped: 25
               Total Number of Vulnerabilities Detected     : 8
               Total Time Elapsed for the Scan              : 2h 43m 55s
```

4. Vulnerability description

- Web Cache Poisoning: A vulnerability that can lead to the contamination of cached web content, allowing attackers to serve malicious content to users.
- X-XSS Protection is not Present: The absence of an XSS protection header in a web application, potentially making it susceptible to cross-site scripting attacks.
- Subdomains Discovered with Dmitry: Discovery of subdomains using the Dmitry tool, potentially expanding the attack surface, and exposing sensitive information.
- Secure Client Initiated Renegotiation Supported: The presence of secure client-initiated renegotiation in a communication protocol, which can have security implications.
- Some Vulnerable Headers Exposed: Certain headers are exposed, which could potentially be exploited or provide information for further attacks.
- WHOIS Information Publicly Available: Publicly accessible WHOIS information, potentially exposing sensitive domain registration details.

5. Affected components.

- Web application, susceptible to web cache poisoning.
- Web application or website without an XSS protection header.
- Domain and its subdomains discovered using Dmitry.
- Systems supporting secure client-initiated renegotiation.
- The exposed headers and the services using them.
- Domain registration information exposed via WHOIS.

6. Impact assessment.

- Web Cache Poisoning: Potential for serving malicious content to users.
- X-XSS Protection is not Present: Risk of cross-site scripting attacks, leading to data theft or unauthorized actions.
- Subdomains Discovered: Expanded attack surface, potential for subdomain-related vulnerabilities.
- Secure Client Initiated Renegotiation: Security implications may lead to unauthorized access or data interception.
- Vulnerable Headers Exposed: Risk of header-based attacks or information exposure.
- WHOIS Information Publicly Available: Potential exposure of sensitive domain registration information.

7. Steps to reproduce.

- None.

8. Proof of concept (if applicable).

- None

9. Proposed mitigation or fix.

- Web Cache Poisoning: Implement proper input validation and content security policies to prevent cache poisoning.
- X-XSS Protection: Add XSS protection headers and implement input validation and output encoding.
- Subdomains: Carefully manage and secure discovered subdomains to prevent information exposure.
- Secure Client Initiated Renegotiation: Ensure secure communication configurations.
- Vulnerable Headers: Review and secure headers, implement security best practices.
- WHOIS Information: Consider privacy protection options for domain registration data.

10. Summary.

- Various vulnerabilities have been identified, including the risk of web cache poisoning, absence of XSS protection, expanded attack surface with discovered subdomains, secure client-initiated renegotiation, vulnerable headers, and public availability of domain registration information. Mitigation measures and thorough security assessments are necessary to protect the affected components and ensure system security.