IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

Report 10 – Intigriti.com

Lecturer in charge – Ms. Chethana Liyanapathirana

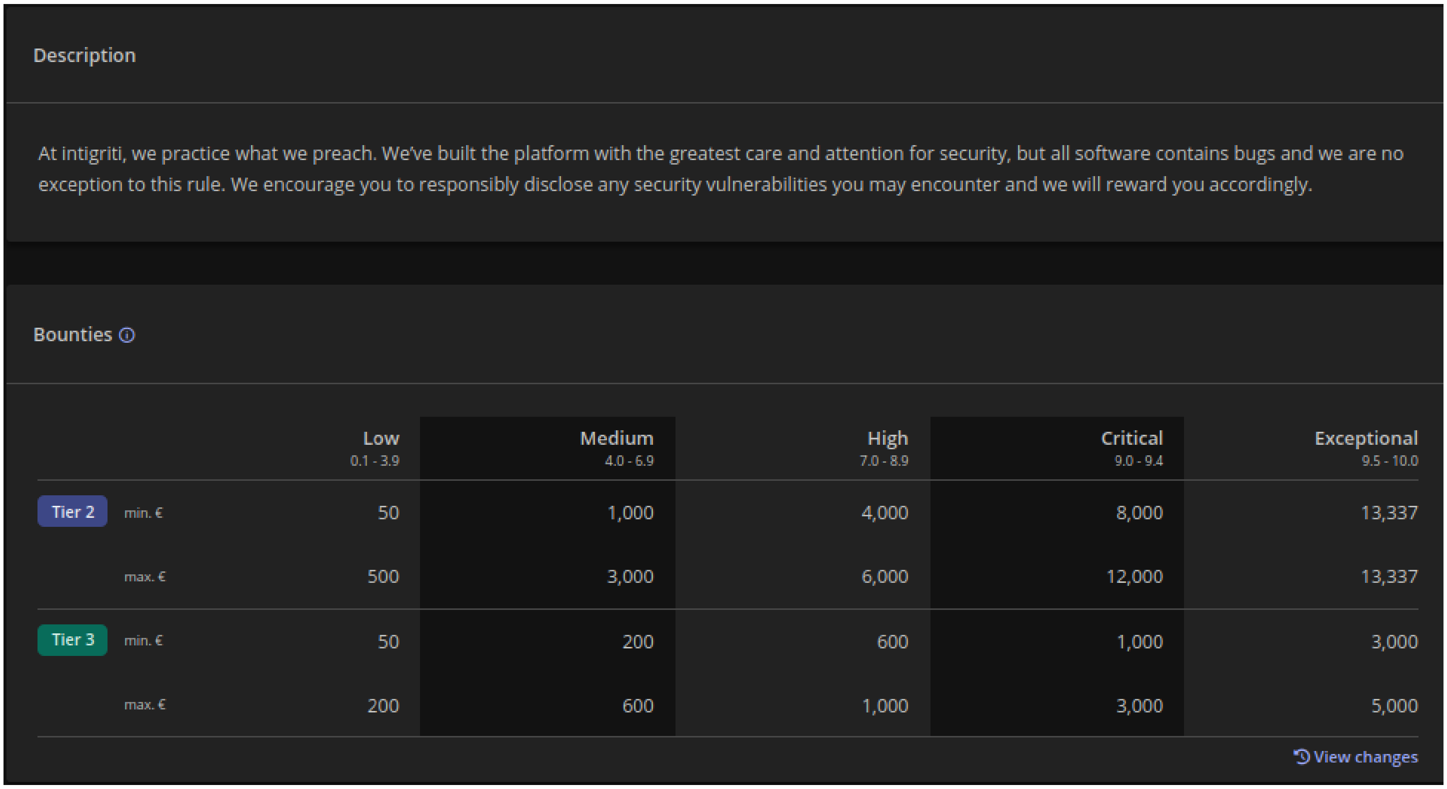
IT21826368 – Nanayakkara Y.D.T.D

Contents

1. intigriti/intigriti/Detail

intigriti / intigriti / Detail

1.1.Overview



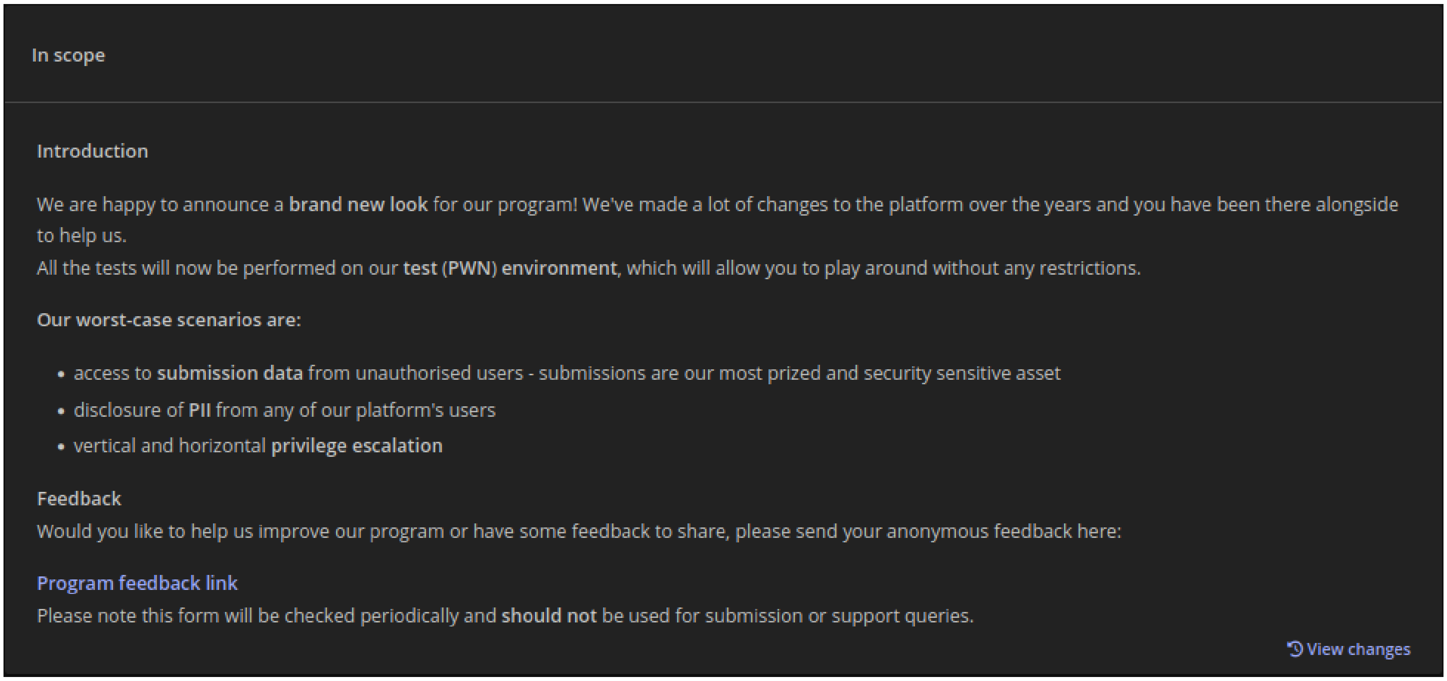
Description

At intigriti, we practice what we preach. We've built the platform with the greatest care and attention for security, but all software contains bugs and we are no exception to this rule. We encourage you to responsibly disclose any security vulnerabilities you may encounter and we will reward you accordingly.

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	min. €	50	1,000	4,000	8,000	13,337
	max. €	500	3,000	6,000	12,000	13,337
Tier 3	min. €	50	200	600	1,000	3,000
	max. €	200	600	1,000	3,000	5,000

1.2.Scope



In scope

Introduction

We are happy to announce a **brand new look** for our program! We've made a lot of changes to the platform over the years and you have been there alongside to help us.
All the tests will now be performed on our **test (PWN) environment**, which will allow you to play around without any restrictions.

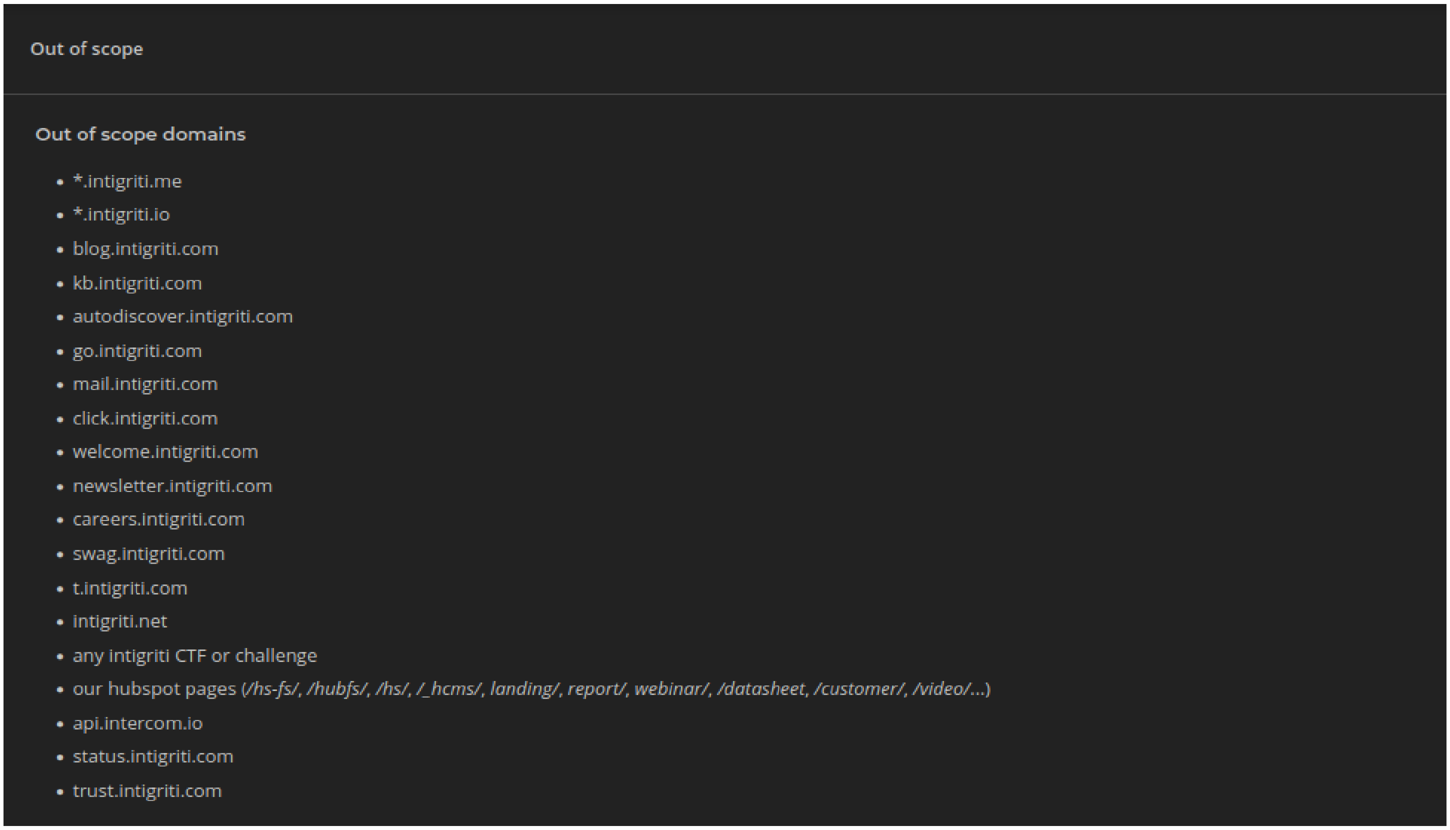
Our worst-case scenarios are:

- access to **submission data** from unauthorised users - submissions are our most prized and security sensitive asset
- disclosure of **PII** from any of our platform's users
- vertical and horizontal **privilege escalation**

Feedback
Would you like to help us improve our program or have some feedback to share, please send your anonymous feedback here:

Program feedback link
Please note this form will be checked periodically and **should not** be used for submission or support queries.

1.3.Out of Scope

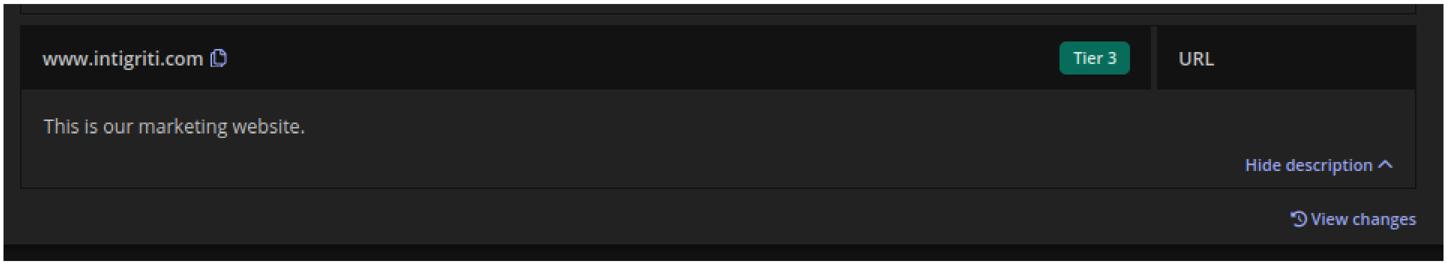


Out of scope

Out of scope domains

- *.intigriti.me
- *.intigriti.io
- blog.intigriti.com
- kb.intigriti.com
- autodiscover.intigriti.com
- go.intigriti.com
- mail.intigriti.com
- click.intigriti.com
- welcome.intigriti.com
- newsletter.intigriti.com
- careers.intigriti.com
- swag.intigriti.com
- t.intigriti.com
- intigriti.net
- any intigriti CTF or challenge
- our hubspot pages *(/hs-fs/, /hubfs/, /hs/, /_hcms/, landing/, report/, webinar/, /datasheet, /customer/, /video/...)*
- api.intercom.io
- status.intigriti.com
- trust.intigriti.com

1.4. Selected Domains


www.intigriti.com

Tier 3

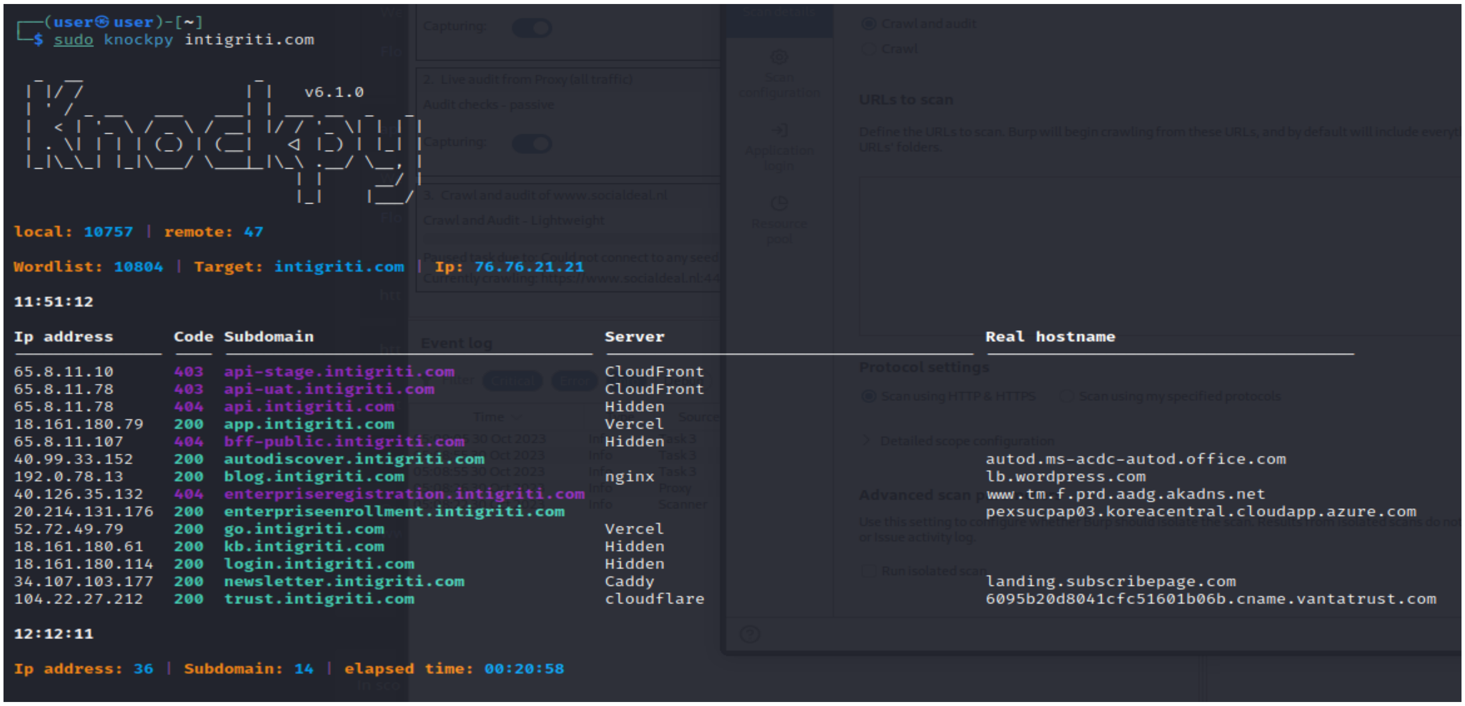
URL

This is our marketing website.

This is the URL www.intigriti.com used in the report.

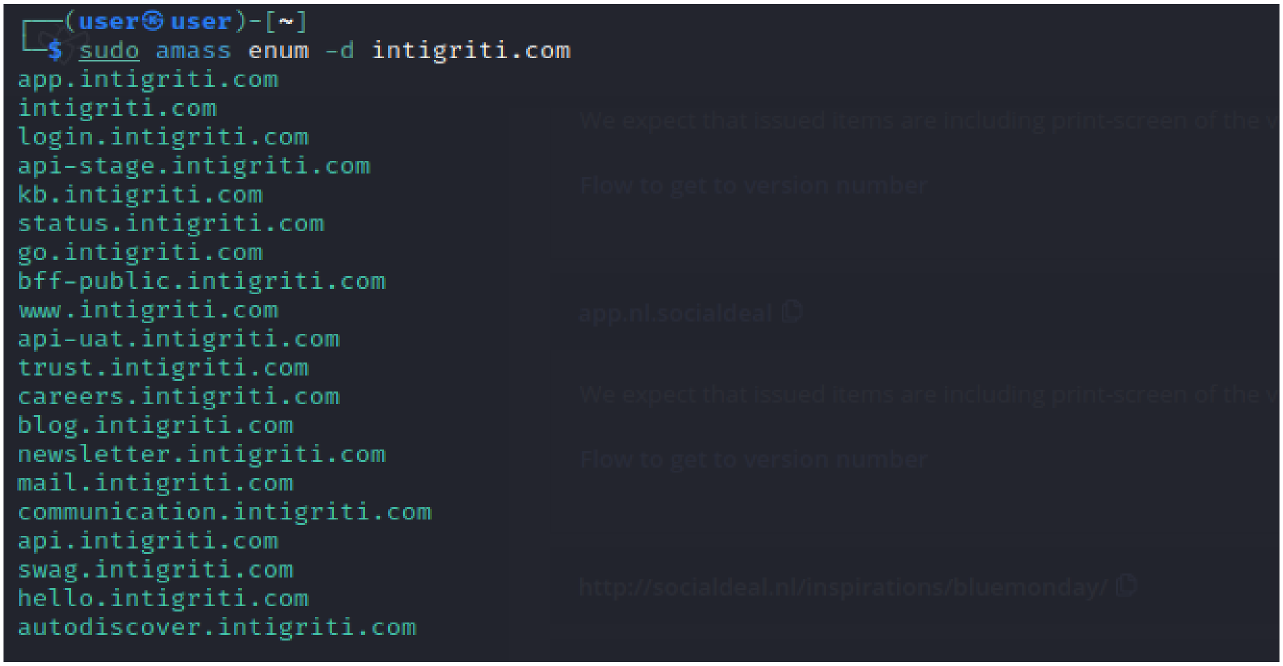
2. Information Gathering

2.1. Using Knockpy to scan the URL.

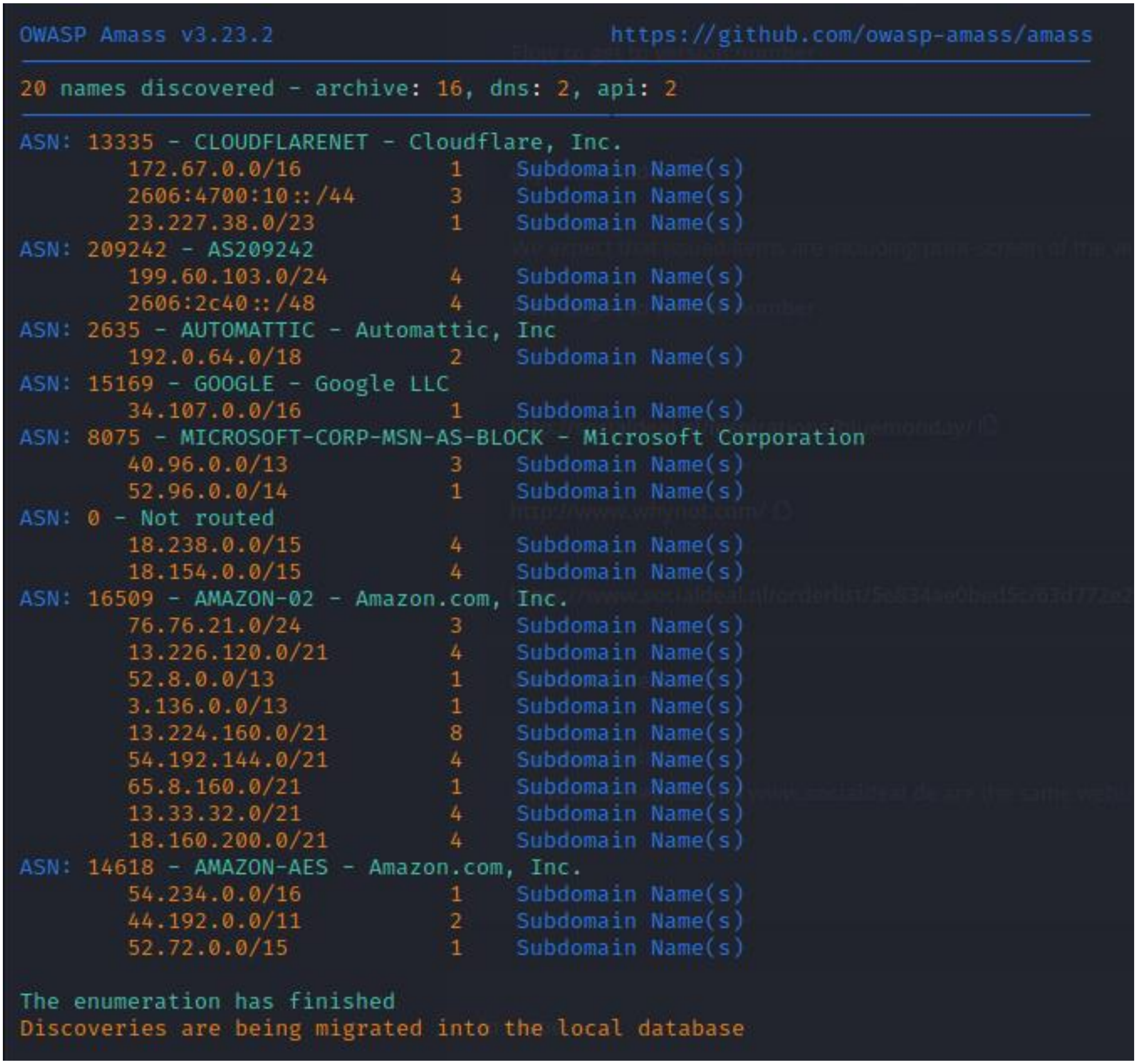


```
┌──(user㉿user)-[~]
└─$ sudo knockpy intigriti.com

  _  __                 _
 | |/ /                | |   v6.1.0
 | ' / _ __   ___   ___| | ___ __  _   _
 |  < | '_ \ / _ \ / __| |/ / '_ \| | | |
 | . \| | | | (_) | (__|   <| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/

local: 10757 | remote: 47

Wordlist: 10804 | Target: intigriti.com | Ip: 76.76.21.21

11:51:12

Ip address      Code Subdomain                            Server                             Real hostname
_______________ ____ ____________________________________ _________________________________  ____________________________
65.8.11.10      403  api-stage.intigriti.com              CloudFront
65.8.11.78      403  api-uat.intigriti.com                CloudFront
65.8.11.78      404  api.intigriti.com                    Hidden
18.161.180.79   200  app.intigriti.com                    Vercel
65.8.11.107     404  bff-public.intigriti.com             Hidden
40.99.33.152    200  autodiscover.intigriti.com                                                autod.ms-acdc-autod.office.com
192.0.78.13     200  blog.intigriti.com                   nginx                                lb.wordpress.com
40.126.35.132   404  enterpriseregistration.intigriti.com                                      www.tm.f.prd.aadg.akadns.net
20.214.131.176  200  enterpriseenrollment.intigriti.com                                        pexsucpap03.koreacentral.cloudapp.azure.com
52.72.49.79     200  go.intigriti.com                     Vercel
18.161.180.61   200  kb.intigriti.com                     Hidden
18.161.180.114  200  login.intigriti.com                  Hidden
34.107.103.177  200  newsletter.intigriti.com             Caddy                                landing.subscribepage.com
104.22.27.212   200  trust.intigriti.com                  cloudflare                           6095b20d8041cfc51601b06b.cname.vantatrust.com

12:12:11

Ip address: 36 | Subdomain: 14 | elapsed time: 00:20:58
```

2.2. Using Amass



```
┌──(user㉿user)-[~]
└─$ sudo amass enum -d intigriti.com
app.intigriti.com
intigriti.com
login.intigriti.com
api-stage.intigriti.com
kb.intigriti.com
status.intigriti.com
go.intigriti.com
bff-public.intigriti.com
www.intigriti.com
api-uat.intigriti.com
trust.intigriti.com
careers.intigriti.com
blog.intigriti.com
newsletter.intigriti.com
mail.intigriti.com
communication.intigriti.com
api.intigriti.com
swag.intigriti.com
hello.intigriti.com
autodiscover.intigriti.com
```

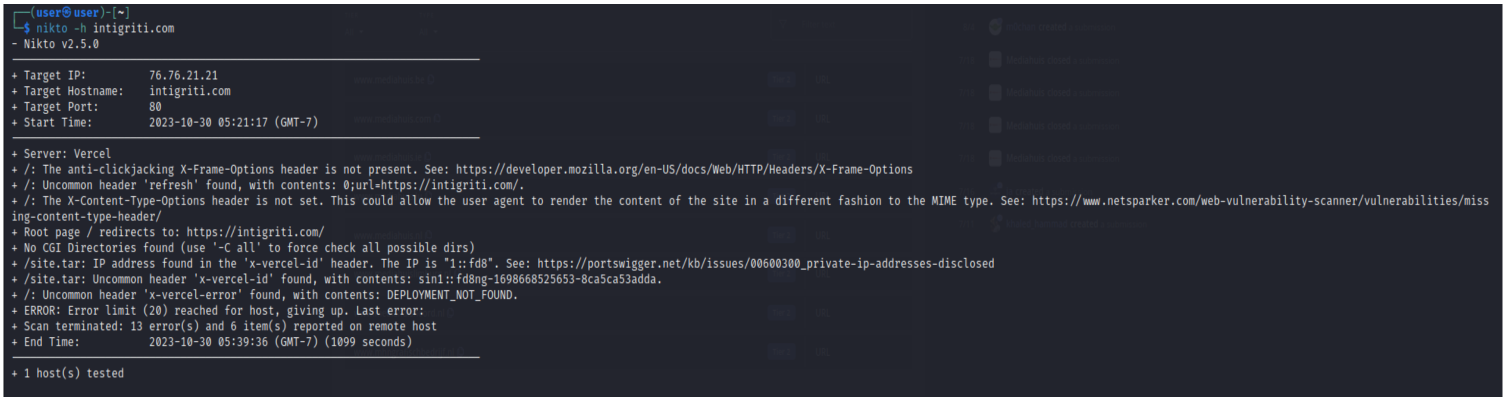


```
OWASP Amass v3.23.2                          https://github.com/owasp-amass/amass
--------------------------------------------------------------------------------
20 names discovered - archive: 16, dns: 2, api: 2
--------------------------------------------------------------------------------
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
        172.67.0.0/16           1    Subdomain Name(s)
        2606:4700:10::/44       3    Subdomain Name(s)
        23.227.38.0/23          1    Subdomain Name(s)
ASN: 209242 - AS209242
        199.60.103.0/24         4    Subdomain Name(s)
        2606:2c40::/48          4    Subdomain Name(s)
ASN: 2635 - AUTOMATTIC - Automattic, Inc
        192.0.64.0/18           2    Subdomain Name(s)
ASN: 15169 - GOOGLE - Google LLC
        34.107.0.0/16           1    Subdomain Name(s)
ASN: 8075 - MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation
        40.96.0.0/13            3    Subdomain Name(s)
        52.96.0.0/14            1    Subdomain Name(s)
ASN: 0 - Not routed
        18.238.0.0/15           4    Subdomain Name(s)
        18.154.0.0/15           4    Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        76.76.21.0/24           3    Subdomain Name(s)
        13.226.120.0/21         4    Subdomain Name(s)
        52.8.0.0/13             1    Subdomain Name(s)
        3.136.0.0/13            1    Subdomain Name(s)
        13.224.160.0/21         8    Subdomain Name(s)
        54.192.144.0/21         4    Subdomain Name(s)
        65.8.160.0/21           1    Subdomain Name(s)
        13.33.32.0/21           4    Subdomain Name(s)
        18.160.200.0/21         4    Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc.
        54.234.0.0/16           1    Subdomain Name(s)
        44.192.0.0/11           2    Subdomain Name(s)
        52.72.0.0/15            1    Subdomain Name(s)

The enumeration has finished
Discoveries are being migrated into the local database
```

- From the result we can perform a Nmap scan

3. Scanning Vulnerability

3.1. Using Nikto to Scan



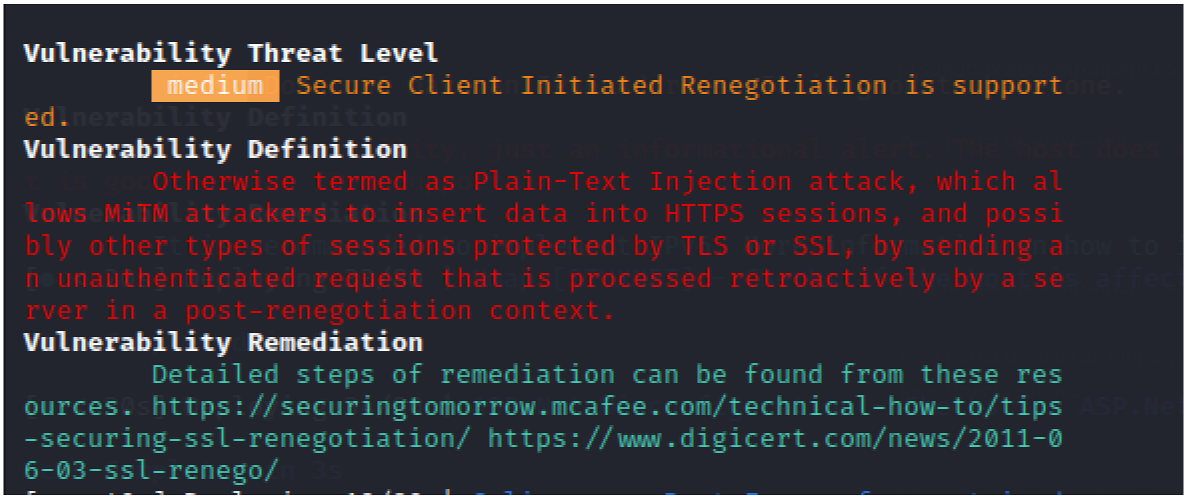
```
┌──(user㉿user)-[~]
└─$ nikto -h intigriti.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          76.76.21.21
+ Target Hostname:    intigriti.com
+ Target Port:        80
+ Start Time:         2023-10-30 05:21:17 (GMT-7)
---------------------------------------------------------------------------
+ Server: Vercel
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'refresh' found, with contents: 0;url=https://intigriti.com/.
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ Root page / redirects to: https://intigriti.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /site.tar: IP address found in the 'x-vercel-id' header. The IP is "1::fd8". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /site.tar: Uncommon header 'x-vercel-id' found, with contents: sin1::fd8ng-1698668525653-8ca5ca53adda.
+ /: Uncommon header 'x-vercel-error' found, with contents: DEPLOYMENT_NOT_FOUND.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 13 error(s) and 6 item(s) reported on remote host
+ End Time:           2023-10-30 05:39:36 (GMT-7) (1099 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Anti clickjack x-frame options header is not present.
- Uncommon header ‘refresher’ found with the contents: 0; URL = https://intigriti.com/

3.2. Using Rapid Scan

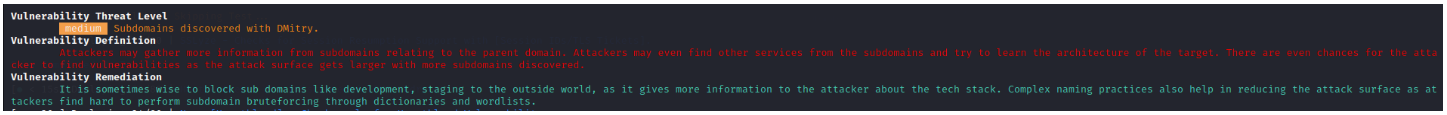
```
                                   (The Multi-Tool Web Vulnerability Scanner)

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

- Secure Client Initiated Renegotiation is supported.



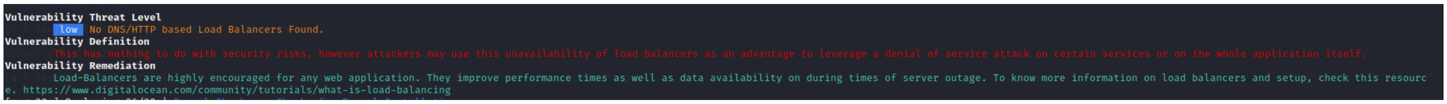
```
Vulnerability Threat Level
        medium  Secure Client Initiated Renegotiation is support
ed.
Vulnerability Definition
        Otherwise termed as Plain-Text Injection attack, which al
lows MiTM attackers to insert data into HTTPS sessions, and possi
bly other types of sessions protected by TLS or SSL, by sending a
n unauthenticated request that is processed retroactively by a se
rver in a post-renegotiation context.
Vulnerability Remediation
        Detailed steps of remediation can be found from these res
ources. https://securingtomorrow.mcafee.com/technical-how-to/tips
-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-0
6-03-ssl-renego/
```

- Subdomains Discovered with Dmitry



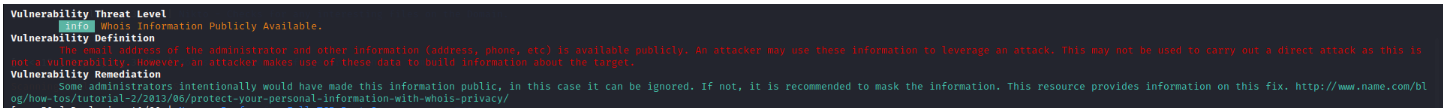
```
Vulnerability Threat Level
        medium  Subdomains discovered with DMitry.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. 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.
```

- No DNS/HTTP based load balancers found.



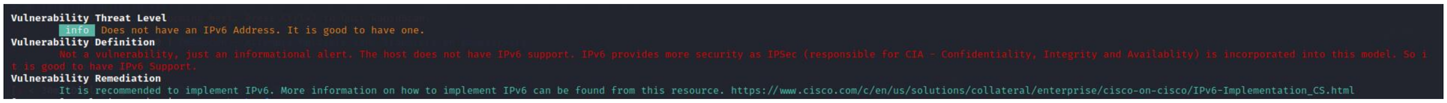
```
Vulnerability Threat Level
        low  No DNS/HTTP based Load Balancers Found.
Vulnerability Definition
        This has nothing to do with security risks, however attackers may use this unavailability of load balancers as an advantage to leverage a denial of service attack on certain services or on the whole application itself.
Vulnerability Remediation
        Load-Balancers are highly encouraged for any web application. They improve performance times as well as data availability on during times of server outage. To know more information on load balancers and setup, check this resourc
e. https://www.digitalocean.com/community/tutorials/what-is-load-balancing
```

- Whois Information Publicly Available



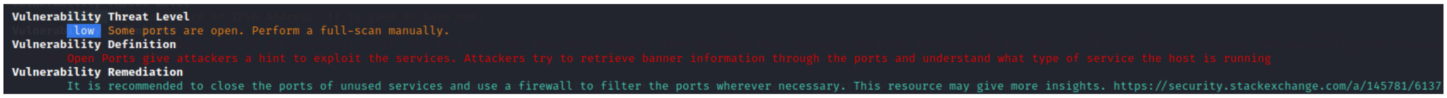
```
Vulnerability Threat Level
        info  Whois Information Publicly Available.
Vulnerability Definition
        The email address of the administrator and other information (address, phone, etc) is available publicly. An attacker may use these information to leverage an attack. This may not be used 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/
```

- Does not have an IPV6 address.



```
Vulnerability Threat Level
        info  Does not have an IPv6 Address. It is good to have one.
Vulnerability Definition
        Not a vulnerability, just an informational alert. The host does not have IPv6 support. IPv6 provides more security as IPSec (responsible for CIA - Confidentiality, Integrity and Availablity) is incorporated into this model. So i
t is good to have IPv6 Support.
Vulnerability Remediation
        It is recommended to implement IPv6. More information on how to implement IPv6 can be found from this resource. https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implementation_CS.html
```

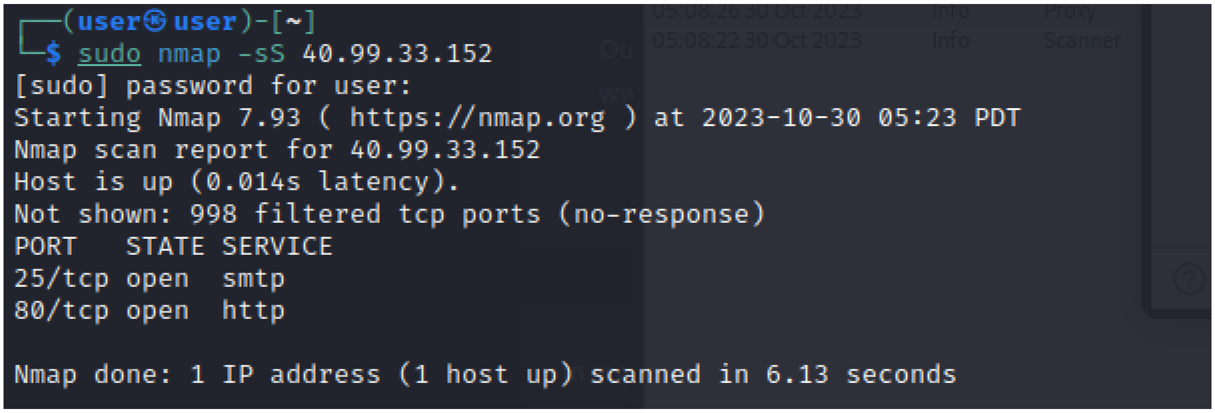
- Some Ports are open



```
Vulnerability Threat Level
        low  Some ports are open. Perform a full-scan manually.
Vulnerability Definition
        Open Ports give attackers a hint to exploit the services. Attackers try to retrieve banner information through the ports and understand what type of service the host is running
Vulnerability Remediation
        It is recommended to close the ports of unused services and use a firewall to filter the ports wherever necessary. This resource may give more insights. https://security.stackexchange.com/a/145781/6137
```

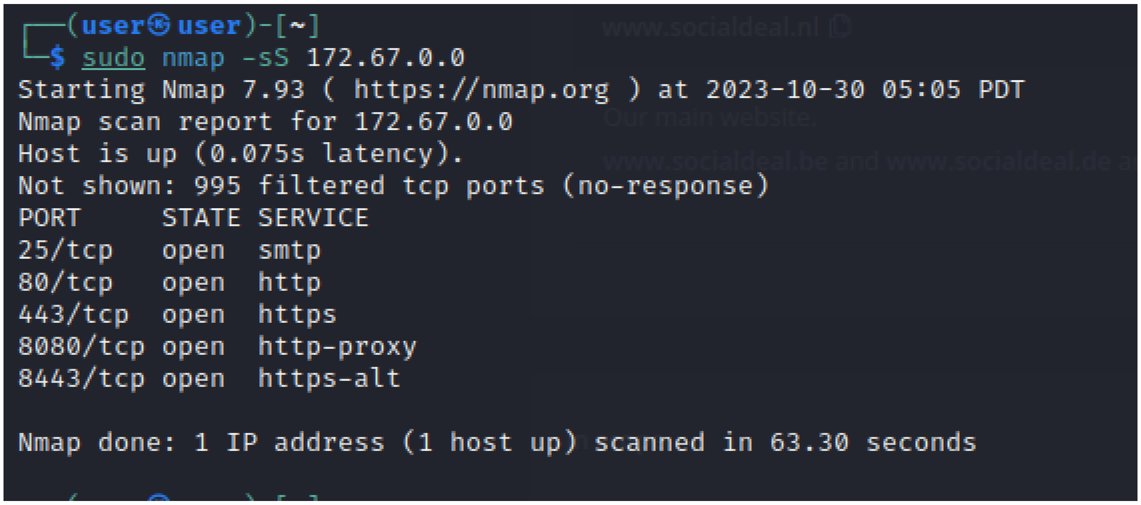
3.3.Using Nmap to scan ports.

- Let’s scan 40.99.33.152 port which belongs to autodiscover.intigriti.com.



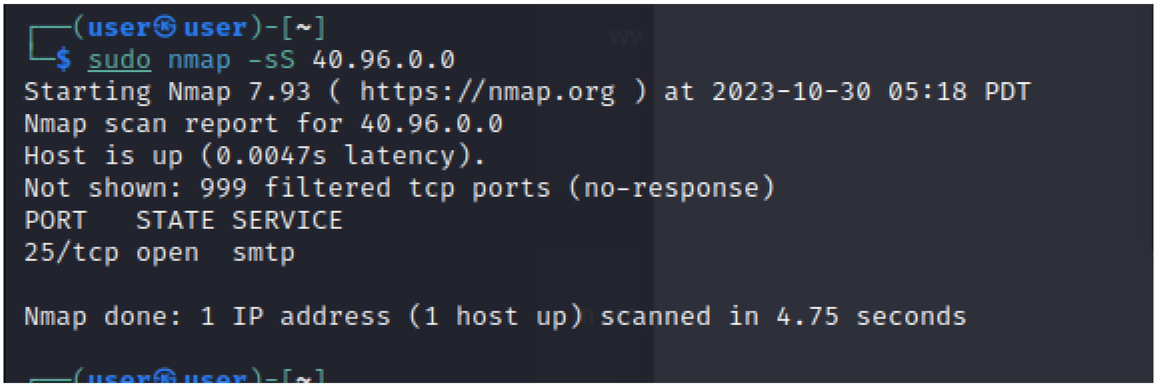
```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 40.99.33.152
[sudo] password for user:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 05:23 PDT
Nmap scan report for 40.99.33.152
Host is up (0.014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
25/tcp open  smtp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 6.13 seconds
```

- Let’s scan 172.67.0.0 port by Cloudflare. Inc



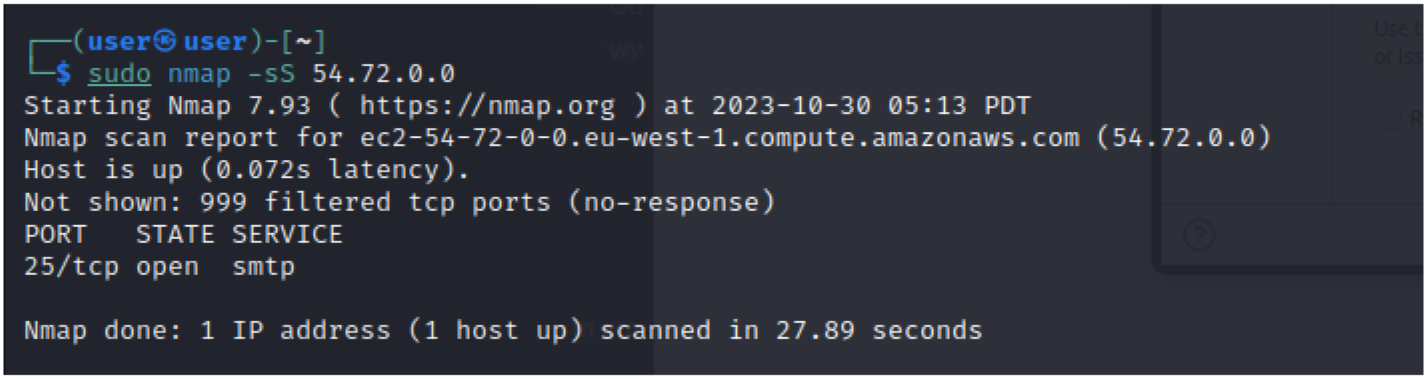
```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 172.67.0.0
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 05:05 PDT
Nmap scan report for 172.67.0.0
Host is up (0.075s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 63.30 seconds
```

- Let’s scan 40.96.0.0 port by Microsoft.



```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 40.96.0.0
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 05:18 PDT
Nmap scan report for 40.96.0.0
Host is up (0.0047s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
25/tcp open  smtp

Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds

┌──(user㉿user)-[~]
```

- Let’s scan 54.72.0.0 port by Amazon.



```
┌──(user㉿user)-[~]
└─$ sudo nmap -sS 54.72.0.0
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 05:13 PDT
Nmap scan report for ec2-54-72-0-0.eu-west-1.compute.amazonaws.com (54.72.0.0)
Host is up (0.072s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
25/tcp open  smtp

Nmap done: 1 IP address (1 host up) scanned in 27.89 seconds
```

4. Vulnerability description

- **Anti Clickjack X-Frame Options Header**:
    - This vulnerability arises from the absence of the "X-Frame-Options" header. It is a security feature that prevents clickjacking attacks by denying a web page from being displayed in iframe.
    - Without this header, attackers could potentially frame your website in a malicious context and trick users into taking unintended actions.
    -
- **Uncommon Header 'Refresher'**:
    - The presence of an unusual HTTP header named 'refresher' with the value '0; URL = https://intigriti.com' suggests an atypical server configuration.
    -
- **Secure Client-Initiated Renegotiation**:
    - Secure Client-Initiated Renegotiation is a security concern related to SSL/TLS renegotiation. It allows a client to request a renegotiation of the security parameters during an ongoing SSL/TLS session.
    - This feature, when supported, can introduce vulnerabilities if not configured correctly. Attackers could potentially abuse this to launch man-in-the-middle attacks.
    -
- **No DNS/HTTP-based Load Balancers**:
    - The absence of DNS or HTTP-based load balancers means that the website might not have a mechanism to distribute incoming traffic across multiple servers for redundancy and load balancing.
    - This could affect the website's availability and scalability, making it vulnerable to traffic spikes or server failures.
    -
- **Publicly Available WHOIS Information**:
    - Publicly available WHOIS information exposes domain registration details, such as the registrant's name, contact information, and domain creation/update dates.
    - This information can be leveraged for social engineering, spam, or other malicious activities.
    -
- **Lack of IPV6 Address**:
    - The absence of an IPv6 address means the website may not be compatible with the next-generation Internet Protocol, IPv6.
    - As IPv6 adoption increases, not having an IPv6 address could limit the website's reach and functionality.
    -
- **Open Ports**:
    - Open ports indicate that specific network services or applications are accessible from the internet.
    - The presence of open ports requires a thorough review and potential hardening to ensure only necessary services are exposed, and proper access controls are in place.

5. Affected components.

- The entire website may be affected.
- HTTP response headers
- Secure Client-Initiated Renegotiation affects the server's SSL/TLS implementation.
- Lack of load balancers affects the website's availability and scalability.
- Public WHOIS information exposes domain registration details.
- IPV6 address absence affects network infrastructure.

6. Impact assessment

- The absence of the Anti-Clickjack X-Frame Options Header poses a moderate risk of clickjacking attacks.
- Uncommon headers may indicate security or configuration issues.
- Secure Client-Initiated Renegotiation support can introduce potential security vulnerabilities.
- Lack of load balancers may impact availability during traffic spikes.
- Public WHOIS information exposes domain registrant details, potentially for malicious purposes.
- The lack of an IPV6 address may limit future network compatibility.
- Open ports may be potential entry points for attackers.

7. Steps to reproduce.

- None

8. Proof of concept (if applicable)

- None

9. Proposed mitigation or fix

- Implement the Anti Clickjack X-Frame Options Header with appropriate settings to prevent clickjacking.
- Review and remove any unusual headers like 'refresher.'
- Evaluate the necessity of Secure Client-Initiated Renegotiation and disable if not required.
- Consider implementing DNS or HTTP-based load balancers for redundancy.
- Review and potentially restrict public access to WHOIS information.
- Assess the need for IPV6 support and consider implementing it if required.
- Review and secure open ports, closing unnecessary services and applying access controls.

10. Summary

Finally, the security assessment has uncovered several vulnerabilities and configuration issues within the target system. The absence of the Anti-Clickjack X-Frame Options Header poses a moderate risk, potentially leaving the website susceptible to clickjacking attacks. An unusual HTTP header named 'refresher' suggests possible misconfigurations or unusual behavior that warrants further investigation. The support for Secure Client-Initiated Renegotiation introduces potential security risks if not correctly configured. Additionally, the absence of DNS or HTTP-based load balancers may affect the website's availability and scalability. The exposure of WHOIS information raises privacy and security concerns. Above discovered Vulnerabilities are not much of a found and they are in the out-of-scope section.