IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

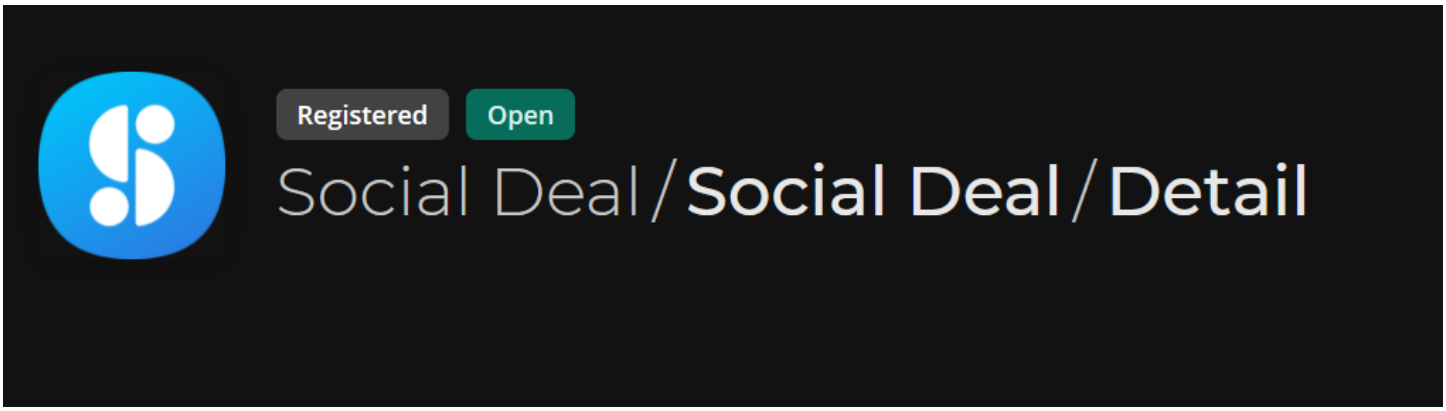
Report 08 - Social Deal

Lecturer in charge – Ms. Chethana Liyanapathirana

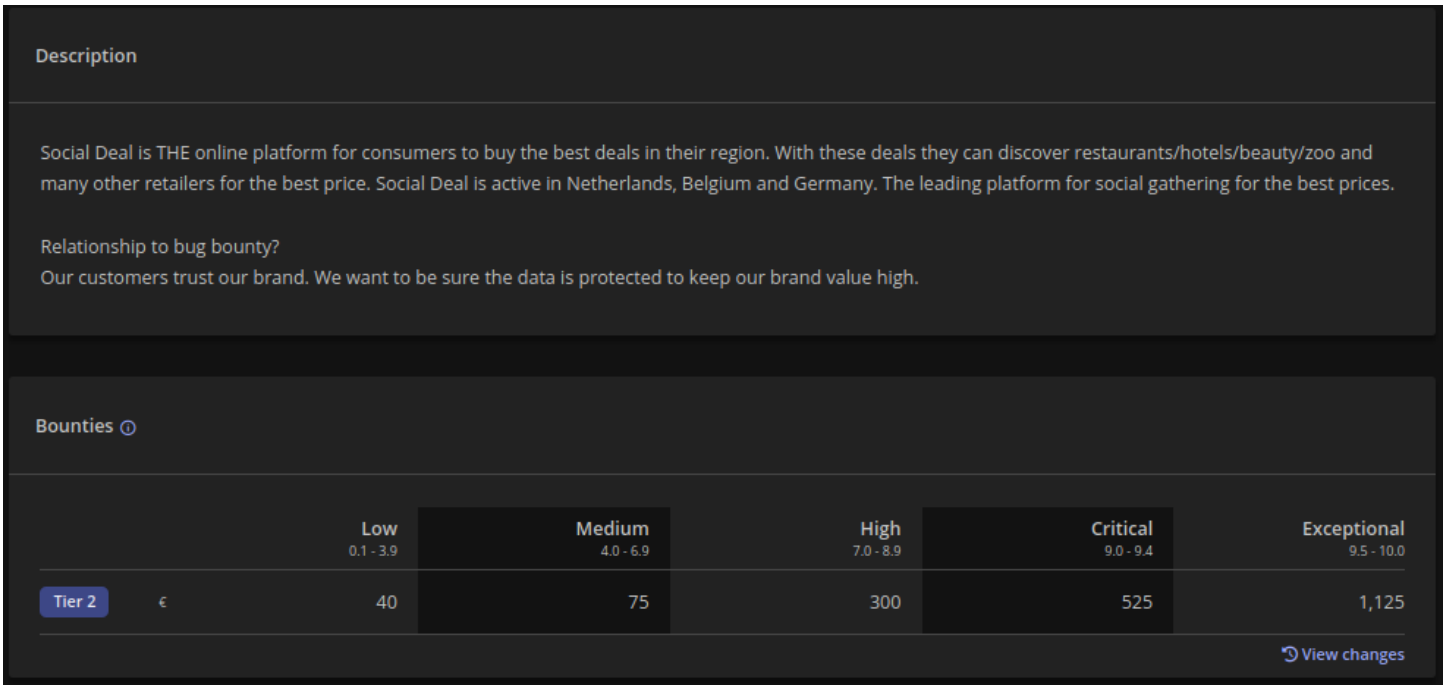
IT21826368 – Nanayakkara Y.D.T.D

Contents

1. Social Deal/Social Deal/Detail



1.1.Overview



1.2.Scope

In scope

Introduction

We are happy to announce our program! We've done our best to clean up our known issues and now would like to request your help to spot the ones we missed!

Our worst-case scenarios are:

Full acces to our servers and database.

Any useful infrastructure information:

We run on multiple AWS ASG's running EC2 with Linux and PHP (7.4/8.1).
Every project/domain has it's own ASG. But most have DB access, or use one or more internal API's to get the correct data.
Our main database is MariaDB (latest version).
We also have some projects running in NuxtJS. (Tier 2/3)

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

Known Issues (date last updated: 28-2-2023)

- Iframe possible (click jacking)

Domains

- Any domain that is not listed in the Domains section, is out of scope for this program

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

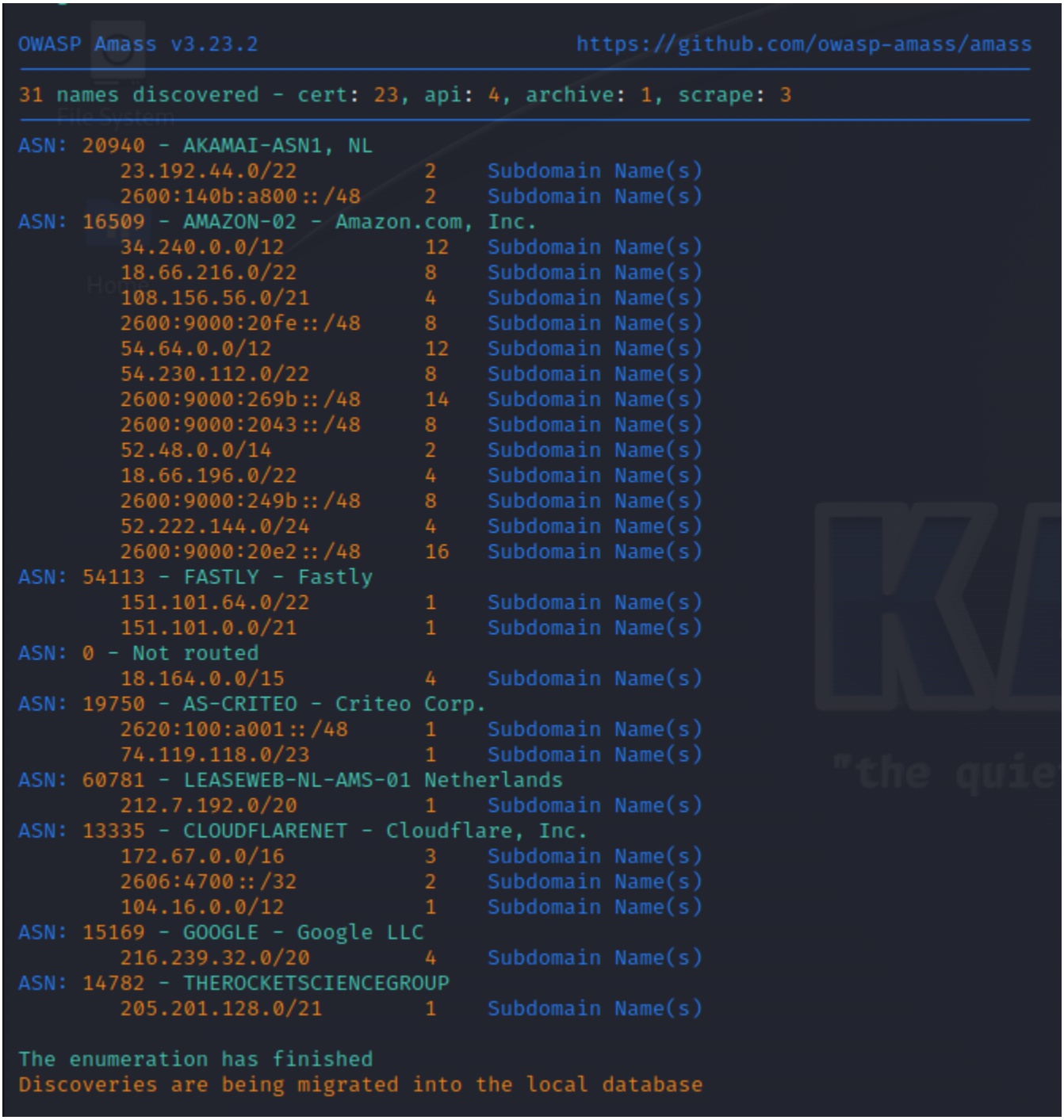
1.4. Selected Domains

URL : www.socialdeal.nl used in the report.

2. Information Gathering

2.1.Using Amass

```
┌──(user㉿user)-[~]
└─$ sudo amass enum -d socialdeal.nl
[sudo] password for user:
mail.socialdeal.nl
stage.socialdeal.nl
goto.socialdeal.nl
socialdeal.nl
gtm.socialdeal.nl
open.mail.socialdeal.nl
email.socialdeal.nl
email.mail.socialdeal.nl
content.socialdeal.nl
excellent.socialdeal.nl
open.socialdeal.nl
werk.socialdeal.nl
game.socialdeal.nl
www.socialdeal.nl
bblink.socialdeal.nl
crm.socialdeal.nl
socialdeal.socialdeal.nl
web-media.socialdeal.nl
media.socialdeal.nl
test2.socialdeal.nl
movies.socialdeal.nl
test-dev.socialdeal.nl
b3.socialdeal.nl
dcsqim.socialdeal.nl
web1.socialdeal.nl
development.socialdeal.nl
tracking.socialdeal.nl
richresults.socialdeal.nl
kerstpakket.socialdeal.nl
v2.socialdeal.nl
images.socialdeal.nl
```


OWASP Amass v3.23.2 https://github.com/owasp-amass/amass
31 names discovered - cert: 23, api: 4, archive: 1, scrape: 3
ASN: 20940 - AKAMAI-ASN1, NL
23.192.44.0/22 2 Subdomain Name(s)
2600:140b:a800::/48 2 Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
34.240.0.0/12 12 Subdomain Name(s)
18.66.216.0/22 8 Subdomain Name(s)
108.156.56.0/21 4 Subdomain Name(s)
2600:9000:20fe::/48 8 Subdomain Name(s)
54.64.0.0/12 12 Subdomain Name(s)
54.230.112.0/22 8 Subdomain Name(s)
2600:9000:269b::/48 14 Subdomain Name(s)
2600:9000:2043::/48 8 Subdomain Name(s)
52.48.0.0/14 2 Subdomain Name(s)
18.66.196.0/22 4 Subdomain Name(s)
2600:9000:249b::/48 8 Subdomain Name(s)
52.222.144.0/24 4 Subdomain Name(s)
2600:9000:20e2::/48 16 Subdomain Name(s)
ASN: 54113 - FASTLY - Fastly
151.101.64.0/22 1 Subdomain Name(s)
151.101.0.0/21 1 Subdomain Name(s)
ASN: 0 - Not routed
18.164.0.0/15 4 Subdomain Name(s)
ASN: 19750 - AS-CRITEO - Criteo Corp.
2620:100:a001::/48 1 Subdomain Name(s)
74.119.118.0/23 1 Subdomain Name(s)
ASN: 60781 - LEASEWEB-NL-AMS-01 Netherlands
212.7.192.0/20 1 Subdomain Name(s)
ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
172.67.0.0/16 3 Subdomain Name(s)
2606:4700::/32 2 Subdomain Name(s)
104.16.0.0/12 1 Subdomain Name(s)
ASN: 15169 - GOOGLE - Google LLC
216.239.32.0/20 4 Subdomain Name(s)
ASN: 14782 - THEROCKETSCIENCEGROUP
205.201.128.0/21 1 Subdomain Name(s)
The enumeration has finished
Discoveries are being migrated into the local database

2.2.Using Knockpy

```
┌──(user㉿user)-[~]
└─$ sudo knockpy socialdeal.nl
[sudo] password for user:

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

local: 10757 | remote: 60

Wordlist: 10817 | Target: socialdeal.nl | Ip: 54.77.0.91

16:14:18

Ip address      Code  Subdomain                    Server                         Real hostname
54.77.0.91      200   12.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   1000.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   11.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   1.socialdeal.nl              Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   080.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   111.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   163.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   01.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   02.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   03.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   15.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   10.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   09.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   101.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   125.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   18.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   0.socialdeal.nl              Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   129.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   123.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   120.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   1rer.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   1c.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   2.socialdeal.nl              Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   20.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   200.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   2005.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   2006.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
```

```
54.77.0.91      200   voci.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vod1.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vod2.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vod101.socialdeal.nl         Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vodka.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vodafone.socialdeal.nl       Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vmscanus.socialdeal.nl       Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vod102.socialdeal.nl         Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vod5.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   voeux.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vps02.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vps15.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vps2.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vps14.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vps1.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vps11.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vps12.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vps10.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vps13.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vp.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vpdn.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   voyeur.socialdeal.nl         Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vpgk.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vpn02.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vpn1.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vpn2.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vpn4.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vpn0.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vpn01.socialdeal.nl          Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   vpn.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vpn3.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   vpn5.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91            websrv.socialdeal.nl                                        public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142        websrv1.socialdeal.nl                                       public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142        websvn.socialdeal.nl                                        public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   www.socialdeal.nl            Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   yp.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   yoyo.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
34.250.151.142  200   ys.socialdeal.nl             Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com
54.77.0.91      200   ysu1.socialdeal.nl           Apache                         public-production-default-1472906072.eu-west-1.elb.amazonaws.com

17:15:29

Ip address: 28 | Subdomain: 4990 | elapsed time: 01:01:10
```

2.3.Using Dmitry

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

HostIP:54.77.0.91
HostName:socialdeal.nl

Gathered Inet-whois information for 54.77.0.91
---------------------------------

inetnum:        54.39.0.0 - 56.255.255.255
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:        2019-01-07T10:45:51Z
last-modified:  2019-01-07T10:45:51Z
source:         RIPE

role:           Internet Assigned Numbers Authority
```

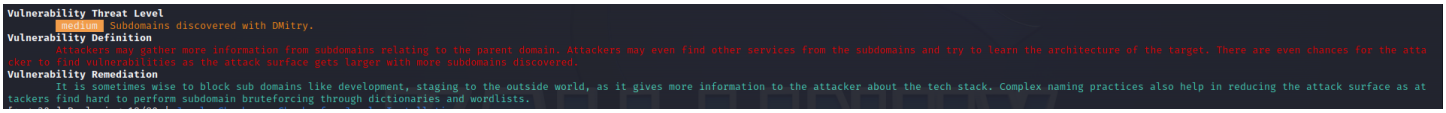
```
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z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

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



Gathered Inic-whois information for socialdeal.nl
---------------------------------

Gathered Netcraft information for socialdeal.nl
---------------------------------

Retrieving Netcraft.com information for socialdeal.nl
Netcraft.com Information gathered

Gathered Subdomain information for socialdeal.nl
---------------------------------
Searching Google.com:80 ...
HostName:www.socialdeal.nl
HostIP:54.77.0.91
HostName:welcome.socialdeal.nl
HostIP:54.77.0.91
HostName:partner.socialdeal.nl
HostIP:34.250.151.142
HostName:excellent.socialdeal.nl
HostIP:34.246.28.232
HostName:werk.socialdeal.nl
HostIP:104.21.65.152
HostName:partners.socialdeal.nl
HostIP:34.250.151.142
HostName:x3ewww.socialdeal.nl
HostIP:54.77.0.91
Searching Altavista.com:80 ...
Found 7 possible subdomain(s) for host socialdeal.nl, Searched 0 pages containing 0 results

Gathered E-Mail information for socialdeal.nl
---------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
```

```
Found 0 E-Mail(s) for host socialdeal.nl, Searched 0 pages containing 0 results

Gathered TCP Port information for 54.77.0.91
---------------------------------

 Port           State

25/tcp          open
80/tcp          open

Portscan Finished: Scanned 150 ports, 2 ports were in state closed


All scans completed, exiting
```

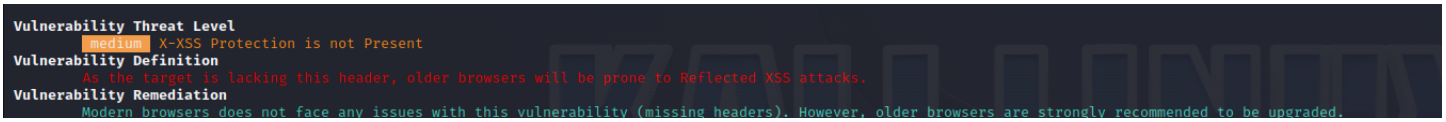
3. Scanning Vulnerability

3.1.Using Rapid Scan

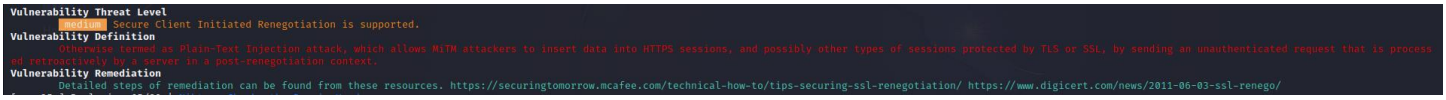
- Found Subdomains with Amass and Dmitry



- X-XSS protection is not present

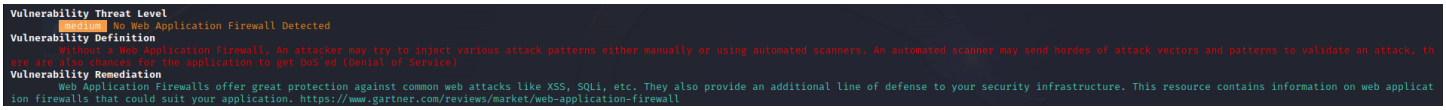


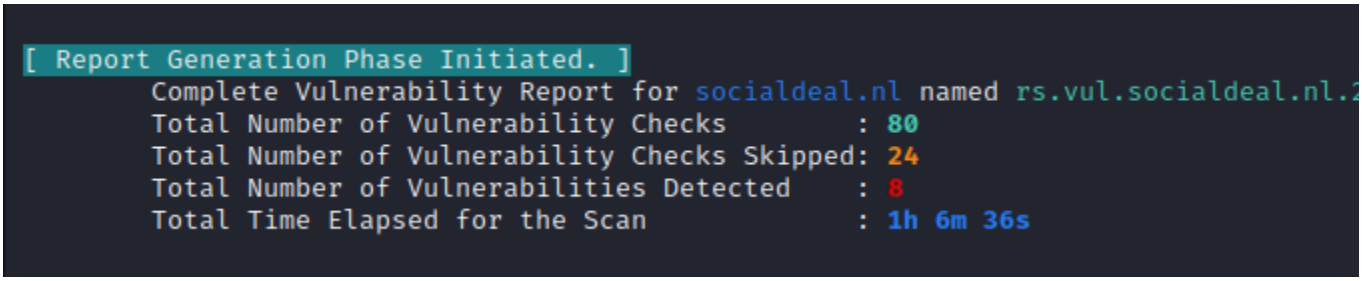
- Secure Client Initiated Renegotiation is supported



- Some Vulnerable headers exposed.

- No web application firewall detected.

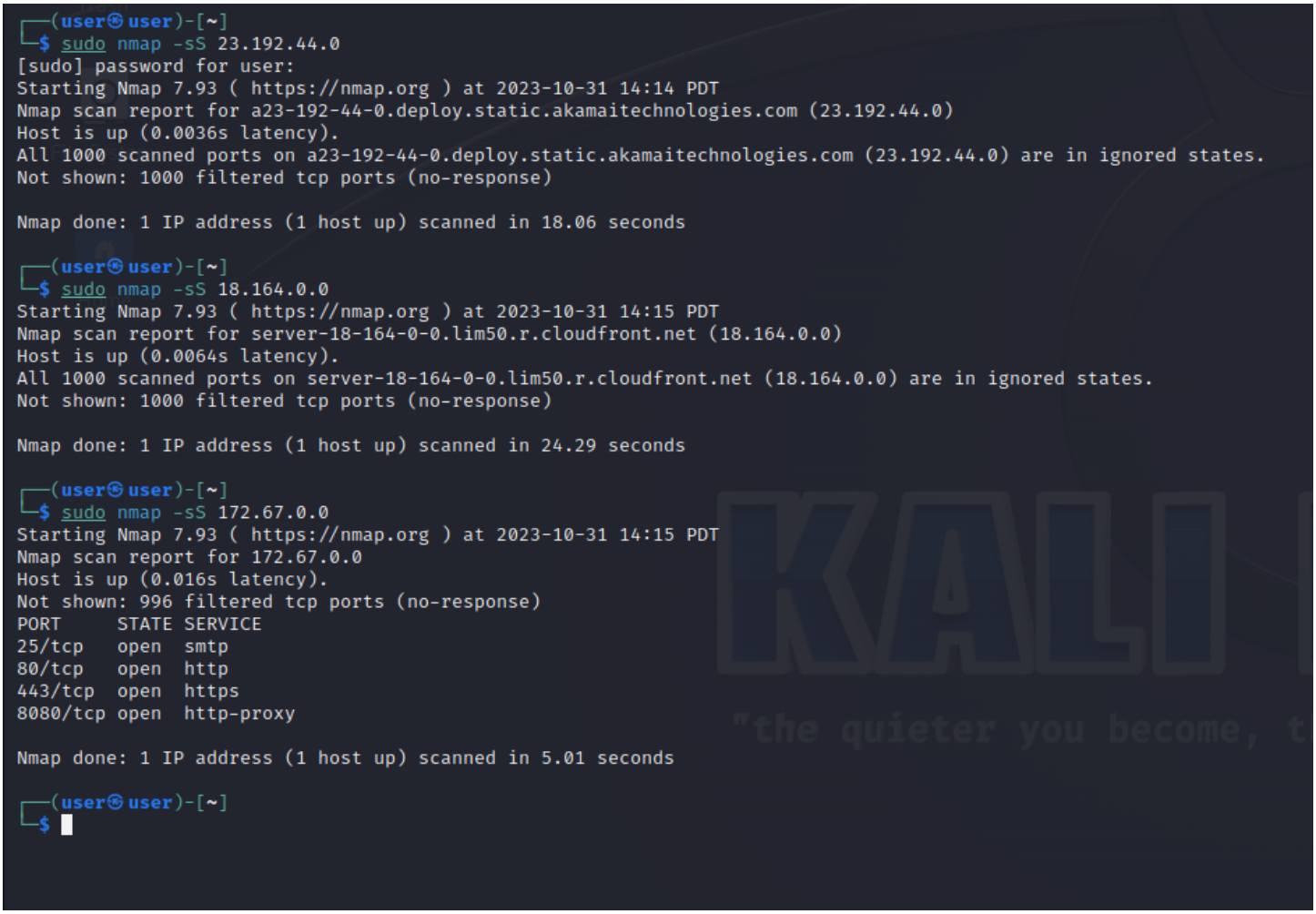




3.2.Using Nikto

- The anti-click-jacking X-Frame Options is not present.
- X content- type- options header not preset

3.3.Using Nmap



- We can see 4 ports are open as the result.

3. Vulnerability description

- **Anti-Clickjacking X-Frame Options Not Present**:
  - The absence of the "X-Frame-Options" header leaves the website potentially vulnerable to clickjacking attacks, where attackers can frame the website within malicious contexts.
  -
- **X-Content-Type-Options Header Not Present**:
  - The missing "X-Content-Type-Options" header can expose the website to content type sniffing attacks, allowing browsers to interpret responses in unintended ways.
  -
- **X-XSS Protection Not Present**:
  - The lack of "X-XSS-Protection" header indicates a vulnerability to cross-site scripting (XSS) attacks, where malicious scripts can be injected into web pages.
  -
- **Secure Client-Initiated Renegotiation Supported**:
  - The support for Secure Client-Initiated Renegotiation may introduce security risks if not configured correctly, potentially facilitating man-in-the-middle attacks.
  -
- **Some Vulnerable Headers Exposed**:
  - Vulnerable headers are exposed, suggesting that certain HTTP headers may be misconfigured or insecure.
  -
- **No Web Application Firewall Detected**:
  - The absence of a web application firewall (WAF) means that the website lacks an additional layer of protection against common web application attacks.

4. Affected components.

- **Anti-Clickjacking X-Frame Options Not Present**:
  - Affects the entire website as it pertains to security headers.
- **X-Content-Type-Options Header Not Present**:
  - Impacts HTTP responses, affecting how browsers interpret content types.
- **X-XSS Protection Not Present**:
  - Affects the entire website, potentially exposing user data to XSS attacks.
- **Secure Client-Initiated Renegotiation Supported**:
  - Impacts the server's SSL/TLS configuration and security.
- **Some Vulnerable Headers Exposed**:
  - Affects the security and integrity of the HTTP headers.
- **No Web Application Firewall Detected**:
  - Impacts the website's security against common web application attacks.

5. Impact assessment.

- **Anti-Clickjacking X-Frame Options Not Present**:
  - Moderate risk: Potential clickjacking attacks can compromise user security.
  -
- **X-Content-Type-Options Header Not Present**:
  - Low to moderate risk: Content type sniffing attacks can have security implications.
  -
- **X-XSS Protection Not Present**:
  - Moderate risk: The absence of XSS protection headers increases the risk of successful XSS attacks, compromising user data.
  -
- **Secure Client-Initiated Renegotiation Supported**:
  - Moderate risk: If not properly configured, it could lead to SSL/TLS vulnerabilities.
  -
- **Some Vulnerable Headers Exposed**:
  - Low to moderate risk: Misconfigured or vulnerable headers could expose security weaknesses.
  -
- **No Web Application Firewall Detected**:
  - Moderate risk: The absence of a WAF may leave the website vulnerable to web application attacks.

6. Steps to reproduce.

- None

7. Proof of concept (if applicable)

- None

8. Proposed mitigation or fix

- implementing missing headers.
- configuring Secure Client-Initiated Renegotiation securely.
- Identifying, mitigating, and securing HTTP response headers that are misconfigured or have vulnerabilities.
- considering the adoption of a WAF.

9. Summary

- The assessment has revealed a range of security vulnerabilities and configuration issues, including missing security headers, the absence of XSS protection, support for Secure Client-Initiated Renegotiation, exposed vulnerable headers, and the lack of a web application firewall. Addressing these findings is critical to enhance the overall security and resilience of the target system.