



IE2062 [2023/JUL]- Web Security

Web Security BB Assignment

## **Report 08 - Social Deal**

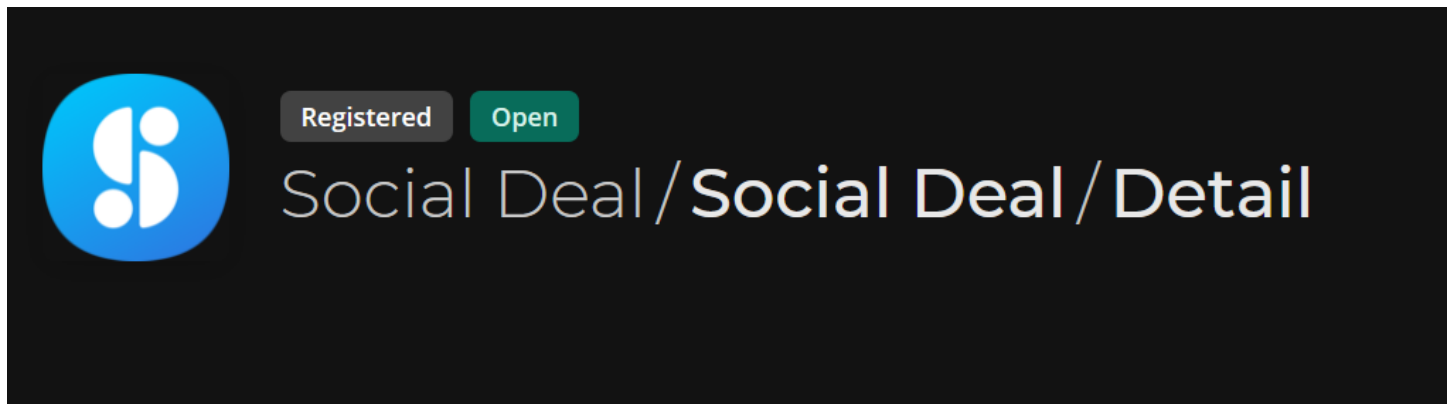
Lecturer in charge – Ms. Chethana Liyanapathirana

IT21826368 – Nanayakkara Y.D.T.D

# Contents

1. Social Deal/Social Deal/Detail .....	3
1.1. Overview .....	3
1.2. Scope .....	4
1.3. Out of Scope .....	4
1.4. Selected Domains .....	5
2. Information Gathering .....	6
2.1. Using Amass .....	6
2.2. Using Knockpy .....	8
2.3. Using Dmitry .....	9
3. Scanning Vulnerability .....	11
3.1. Using Rapid Scan .....	11
3.2. Using Nikto .....	12
3.3. Using Nmap .....	13
3. Vulnerability description .....	14
4. Affected components .....	14
5. Impact assessment .....	15
6. Steps to reproduce .....	15
7. Proof of concept (if applicable) .....	15
8. Proposed mitigation or fix .....	15
9. Summary .....	15

## 1. Social Deal/Social Deal/Detail



### 1.1.Overview

Description

Social Deal is THE online platform for consumers to buy the best deals in their region. With these deals they can discover restaurants/hotels/beauty/zoo and many other retailers for the best price. Social Deal is active in Netherlands, Belgium and Germany. The leading platform for social gathering for the best prices.

Relationship to bug bounty?

Our customers trust our brand. We want to be sure the data is protected to keep our brand value high.

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	€	40	75	300	525	1,125

View changes

## 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 access 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

www.socialdeal.nl 	Tier 2	URL
---	--------	-----

URL : [www.socialdeal.nl](http://www.socialdeal.nl) used in the report.

## 2. Information Gathering

### 2.1. Using Amass

```
(user@user)-[~]ools Kali Docs Kali Forums Kali NetHunter Exploit-DB Goo
$ 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
bbblink.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
```

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

[illegible]



## 2.3.Using Dmitry

```
(user@user)-[~] Tools - Kali Docs - Kali Forums - Kali NetHunter - Exploit-DB - Google Hacking DB
$ 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:          For registration information,
remarks:          you can consult the following sources:
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:          AFRINIC (Africa)
remarks:          http://www.afrinic.net/ whois.afrinic.net
remarks:          APNIC (Asia Pacific)
remarks:          http://www.apnic.net/ whois.apnic.net
remarks:          ARIN (Northern America)
remarks:          http://www.arin.net/ whois.arin.net
remarks:          LACNIC (Latin America and the Carribean)
remarks:          http://www.lacnic.net/ whois.lacnic.net
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

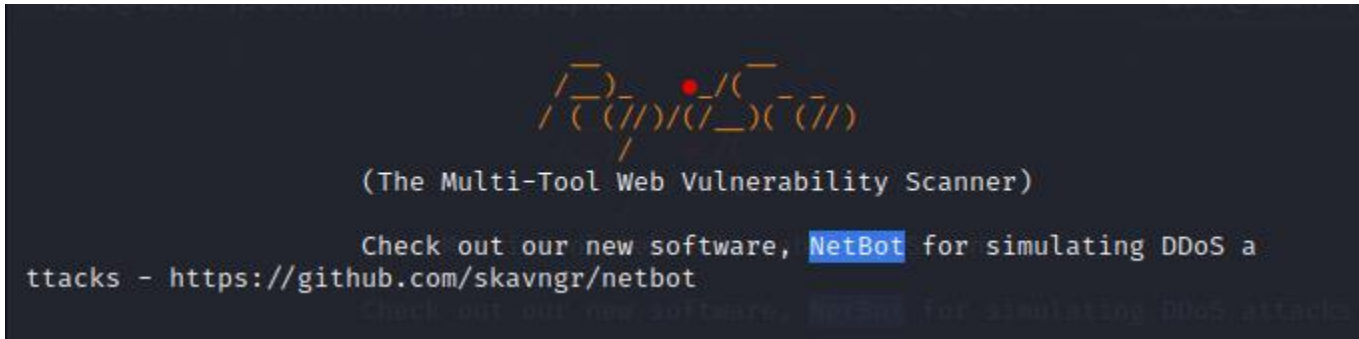
Port	State
25/tcp	open
80/tcp	open

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

```
Vulnerability Threat Level
Medium Found Subdomains with Amass
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 attacker 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 attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

```
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 attacker 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 attackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

- X-XSS protection is not present

```
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 (missing headers). However, older browsers are strongly recommended to be upgraded.
```

- Secure Client Initiated Renegotiation is supported

```
Vulnerability Threat Level
Medium Secure Client Initiated Renegotiation is supported.
Vulnerability Definition
Vulnerability 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 processed 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.
```

- No web application firewall detected.

```
Vulnerability Threat Level
Medium No Web Application Firewall Detected
Vulnerability Definition
Without a Web Application Firewall, an attacker may try to inject various attack patterns either manually or using automated scanners. An automated scanner may send hundreds of attack vectors and patterns to validate an attack, then are also chances for the application to get DoS or (Denial of Service)
Vulnerability Remediation
Web Application Firewalls offer great protection against common web attacks like XSS, SQLi, etc. They also provide an additional line of defense to your security infrastructure. This resource contains information on web application firewalls that could suit your application. https://www.gartner.com/reviews/market/web-application-firewall
```

```
[ Report Generation Phase Initiated. ]
Complete Vulnerability Report for socialdeal.nl named rs.vul.socialdeal.nl.2
Total Number of Vulnerability Checks      : 80
Total Number of Vulnerability Checks Skipped: 24
Total Number of Vulnerabilities Detected   : 8
Total Time Elapsed for the Scan            : 1h 6m 36s
```

## 3.2.Using Nikto

```
(user@user)-[~]
$ sudo nikto -h socialdeal.nl
- Nikto v2.5.0

+ Multiple IPs found: 54.77.0.91, 34.250.151.142
+ Target IP: 54.77.0.91
+ Target Hostname: socialdeal.nl
+ Target Port: 80
+ Start Time: 2023-10-31 14:16:49 (GMT-7)

+ Server: awselb/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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/missing-content-type-header/
+ Root page / redirects to: https://socialdeal.nl:443/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7975 requests: 12 error(s) and 2 item(s) reported on remote host
+ End Time: 2023-10-31 14:48:50 (GMT-7) (1921 seconds)

+ 1 host(s) tested
```

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

### 3.3.Using Nmap

```
(user@user)-[~]
$ sudo nmap -sS 23.192.44.0
[sudo] password for user:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 14:14 PDT
Nmap scan report for a23-192-44-0.deploy.static.akamaitechnologies.com (23.192.44.0)
Host is up (0.0036s latency).
All 1000 scanned ports on a23-192-44-0.deploy.static.akamaitechnologies.com (23.192.44.0) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 18.06 seconds

(user@user)-[~]
$ sudo nmap -sS 18.164.0.0
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 14:15 PDT
Nmap scan report for server-18-164-0-0.lim50.r.cloudfront.net (18.164.0.0)
Host is up (0.0064s latency).
All 1000 scanned ports on server-18-164-0-0.lim50.r.cloudfront.net (18.164.0.0) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 24.29 seconds

(user@user)-[~]
$ sudo nmap -sS 172.67.0.0
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 14:15 PDT
Nmap scan report for 172.67.0.0
Host is up (0.016s latency).
Not shown: 996 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

Nmap done: 1 IP address (1 host up) scanned in 5.01 seconds

(user@user)-[~]
$
```

- 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.