

# Sri Lanka Institute of Information Technology



Specialized in Cyber Security

Year 2, Semester 2

IE2062 – Web Security

Bug Bounty – Report 08

Student ID No.	Name
IT23136106	D.M.M. Pasindu Supushmika

# Table of Contents

- 01. [Website Overview](#)
- 02. [Step 01: Gather Information](#)
  - a. [Subdomain Discovery](#)
    - i. [Sublist3r](#)
    - ii. [Subfinder](#)
  - b. [Live Subdomains](#)
  - c. [IP Discovery](#)
  - d. [Open Ports](#)
  - e. [Used Technologies](#)
- 03. [Step 02: Scanning and Vulnerability Identification](#)
  - a. [Identify Potential Vulnerabilities](#)
  - b. [Content Security Policy \(CSP\) Header Not Set](#)
- 04. [Step 03: Exploitation and Validation](#)
- 05. [Step 04: Mitigation / Fix](#)

1. Website Overview

[Truecaller - Leading Global Caller ID & Call Blocking App](#)  
HackerOne Link: [Truecaller](#) | [Bug Bounty Program Policy](#) | [HackerOne](#)

Security page

Program guidelines

Scope

Hacktivity

Thanks

Updates

Collaborators

Program highlights

Platform StandardsFully compliant with Platform Standards. Managed by HackerOneCollaboration EnabledIncludes Retesting

2 days, 23 hoursAverage time to first response

1 week, 1 dayAverage time to triage

1 month, 1 weekAverage time to bounty

1 month, 2 weeksAverage time from submission to bounty

3 months, 2 daysAverage time to resolution

Rewards summaryLast updated on December 4, 2024. View changes

Each severity lists the 90-day average bounty and the percentage of total resolved reports, if applicable.

LowAvg. bounty n/a42.86% submissions

MediumAvg. bounty \$48045.24% submissions

HighAvg. bounty n/a11.90% submissions

CriticalAvg. bounty n/a0% submissions

Truecaller

[https://www.truecaller.com](#)  
@truecaller

The World's Best Caller ID and Spam Blocking App  
Bug Bounty Program launched in Mar 2024

Response efficiency: 76%

Submit report

Rewards

Severity	Rewards
Low	\$100-\$250
Medium	\$250-\$750
High	\$1,350-\$3,000

truecaller

Android app

iPhone app

Premium

Community

Business

Scam Alert

EN

Sign in

Download

The World's Best Caller ID and Spam Blocking App

Try Truecaller for Free

Google Play4.5

App Store4.5

+94 Search phone number...

NEW!

Truecaller finally works on iPhone!

Identify partners

Lina PerssonTruecaller Caller ID

Activate WindowsGo to Settings to activate Windows.

## Step 01: Gather Information.

### a. Sub-domain Discovery

#### i. Sublist3r: [sublist3r truecaller results.txt](#)

**Tool** : Sublist3r

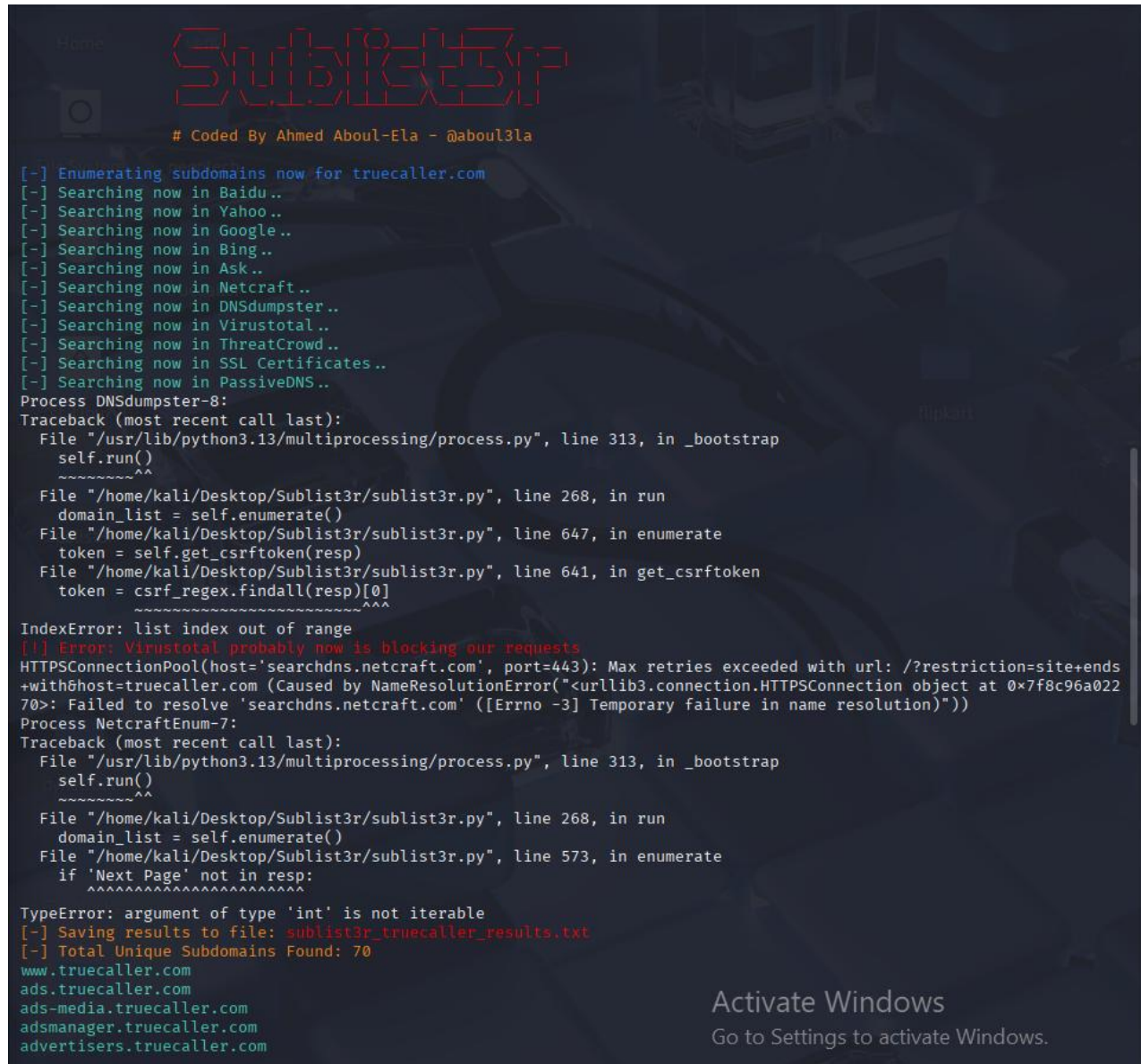
**Code** : python3 sublist3r.py -d truecaller.com -o sublist3r\_truecaller\_results.txt

**Explanation:**

*python3 sublist3r.py* - Run the script using python

*-d truecaller.com* - Target domain

*-o sublist3r\_truecaller\_results.txt* – Output file where the result is saved



```

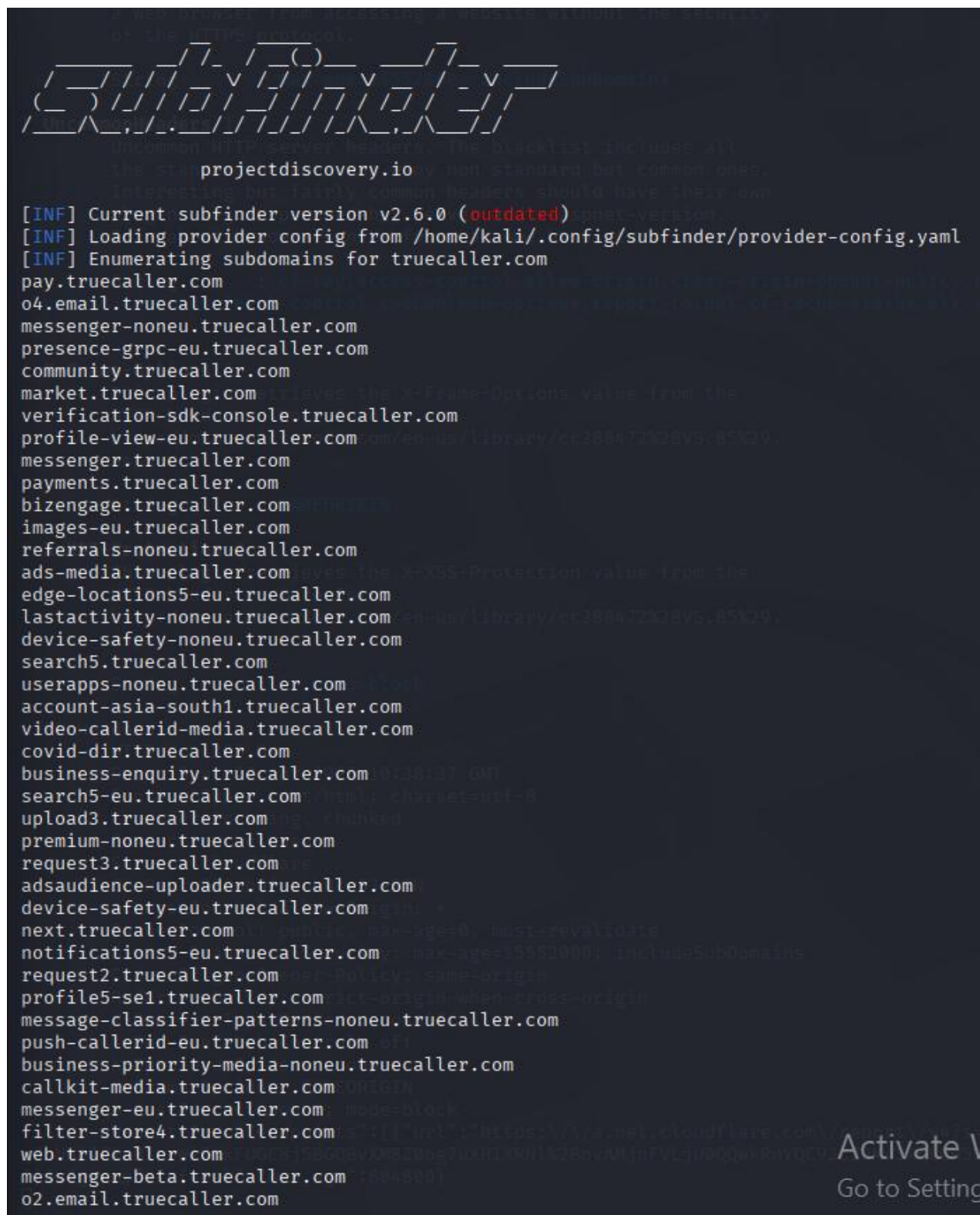
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for truecaller.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..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~^
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrf_token(resp)
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 641, in get_csrf_token
    token = csrf_regex.findall(resp)[0]
    ~~~~~^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
HTTPSConnectionPool(host='searchdns.netcraft.com', port=443): Max retries exceeded with url: /?restriction=site+ends+with&host=truecaller.com (Caused by NameResolutionError("<urllib3.connection.HTTPSConnection object at 0x7f8c96a02270>: Failed to resolve 'searchdns.netcraft.com' ([Errno -3] Temporary failure in name resolution)"))
Process NetcraftEnum-7:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~^
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 573, in enumerate
    if 'Next Page' not in resp:
    ~~~~~^
TypeError: argument of type 'int' is not iterable
[-] Saving results to file: sublist3r_truecaller_results.txt
[-] Total Unique Subdomains Found: 70
www.truecaller.com
ads.truecaller.com
ads-media.truecaller.com
adsmanager.truecaller.com
advertisers.truecaller.com

Activate Windows
Go to Settings to activate Windows.
```

www.truecaller.com  
ads.truecaller.com  
ads-media.truecaller.com  
adsmanager.truecaller.com  
advertisers.truecaller.com  
app.truecaller.com  
bb.truecaller.com  
beta.truecaller.com  
bizengage.truecaller.com  
blog.truecaller.com  
www.blog.truecaller.com  
business.truecaller.com  
business-enquiry.truecaller.com  
business-support.truecaller.com  
callkit-media.truecaller.com  
careers.truecaller.com  
chat.truecaller.com  
cloud-telephony-v2-noneu.truecaller.com  
community.truecaller.com  
img.content.truecaller.com  
corporate.truecaller.com  
covid-dir.truecaller.com  
dev.truecaller.com  
developer.truecaller.com  
docs.truecaller.com  
images-override-eu.truecaller.com  
jira-test.truecaller.com  
landing.truecaller.com  
landlines.truecaller.com  
leads.truecaller.com  
leads-test.truecaller.com  
loans.truecaller.com  
market.truecaller.com  
messenger.truecaller.com  
messenger-alpha.truecaller.com  
messenger-beta.truecaller.com  
next.truecaller.com  
offers.truecaller.com  
payments.truecaller.com  
premium.truecaller.com  
priority.truecaller.com  
privacy.truecaller.com  
promo-pay.truecaller.com  
sdk-console-noneu.truecaller.com  
static-images-eu.truecaller.com  
static-topspammers-eu.truecaller.com  
stores-web-noneu.truecaller.com  
support.truecaller.com  
tc-images-override-eu.truecaller.com  
tcbrandsolutions.truecaller.com  
tcbrandsolutions.truecaller.com  
techblog.truecaller.com  
terms.truecaller.com  
topspammers-noneu-storage.truecaller.com  
delivery.updates.truecaller.com  
userapps-tmp.truecaller.com  
veri.truecaller.com  
verification-sdk-console.truecaller.com



ii. Subfindre: [subfinder result truecaller.txt](#)**Tool** : Subfinder**Code** : subfinder -d truecaller.com -o subfinder\_result.txt**Explanation:***subfinder* - run subfinder too*-d truecaller.com* - Mention the target website*-o subfinder\_result.txt* – Mention the output file


```

subfinder
projectdiscovery.io
[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for truecaller.com
pay.truecaller.com
o4.email.truecaller.com
messenger-noneu.truecaller.com
presence-grpc-eu.truecaller.com
community.truecaller.com
market.truecaller.com
verification-sdk-console.truecaller.com
profile-view-eu.truecaller.com
messenger.truecaller.com
payments.truecaller.com
bizengage.truecaller.com
images-eu.truecaller.com
referrals-noneu.truecaller.com
ads-media.truecaller.com
edge-locations5-eu.truecaller.com
lastactivity-noneu.truecaller.com
device-safety-noneu.truecaller.com
search5.truecaller.com
userapps-noneu.truecaller.com
account-asia-south1.truecaller.com
video-callerid-media.truecaller.com
covid-dir.truecaller.com
business-enquiry.truecaller.com
search5-eu.truecaller.com
upload3.truecaller.com
premium-noneu.truecaller.com
request3.truecaller.com
adsaudience-uploader.truecaller.com
device-safety-eu.truecaller.com
next.truecaller.com
notifications5-eu.truecaller.com
request2.truecaller.com
profile5-se1.truecaller.com
message-classifier-patterns-noneu.truecaller.com
push-callerid-eu.truecaller.com
business-priority-media-noneu.truecaller.com
callkit-media.truecaller.com
messenger-eu.truecaller.com
filter-store4.truecaller.com
web.truecaller.com
messenger-beta.truecaller.com
o2.email.truecaller.com

```

pay.truecaller.com

o4.email.truecaller.com

messenger-noneu.truecaller.com

presence-grpc-eu.truecaller.com  
community.truecaller.com  
market.truecaller.com  
verification-sdk-console.truecaller.com  
profile-view-eu.truecaller.com  
messenger.truecaller.com  
payments.truecaller.com  
bizengage.truecaller.com  
images-eu.truecaller.com  
referrals-noneu.truecaller.com  
ads-media.truecaller.com  
edge-locations5-eu.truecaller.com  
lastactivity-noneu.truecaller.com  
device-safety-noneu.truecaller.com  
search5.truecaller.com  
userapps-noneu.truecaller.com  
account-asia-south1.truecaller.com  
video-callerid-media.truecaller.com  
covid-dir.truecaller.com  
business-enquiry.truecaller.com  
search5-eu.truecaller.com  
upload3.truecaller.com  
premium-noneu.truecaller.com  
request3.truecaller.com  
adsaudience-uploader.truecaller.com  
device-safety-eu.truecaller.com  
next.truecaller.com  
notifications5-eu.truecaller.com  
request2.truecaller.com  
profile5-se1.truecaller.com  
message-classifier-patterns-noneu.truecaller.com  
push-callerid-eu.truecaller.com  
business-priority-media-noneu.truecaller.com  
callkit-media.truecaller.com  
messenger-eu.truecaller.com  
filter-store4.truecaller.com  
web.truecaller.com  
messenger-beta.truecaller.com  
o2.email.truecaller.com  
search5-noneu.truecaller.com  
survey-eu.truecaller.com  
messenger-alpha.truecaller.com  
topspammers-noneu-storage.truecaller.com  
support.truecaller.com  
advertisers.truecaller.com  
contact-lists-eu.truecaller.com  
outline.truecaller.com  
business-support.truecaller.com  
request.truecaller.com  
premium.truecaller.com  
verify-reg1.truecaller.com  
promo-pay.truecaller.com  
company-profile-noneu.truecaller.com  
static-images-eu.truecaller.com  
ads-config-engine-noneu.truecaller.com  
comments-noneu.truecaller.com  
pixel-noneu.truecaller.com  
delivery.updates.truecaller.com

## b. Live Subdomain Discovery

**Tool** : [http://livesub\\_results.txt](http://livesub_results.txt)

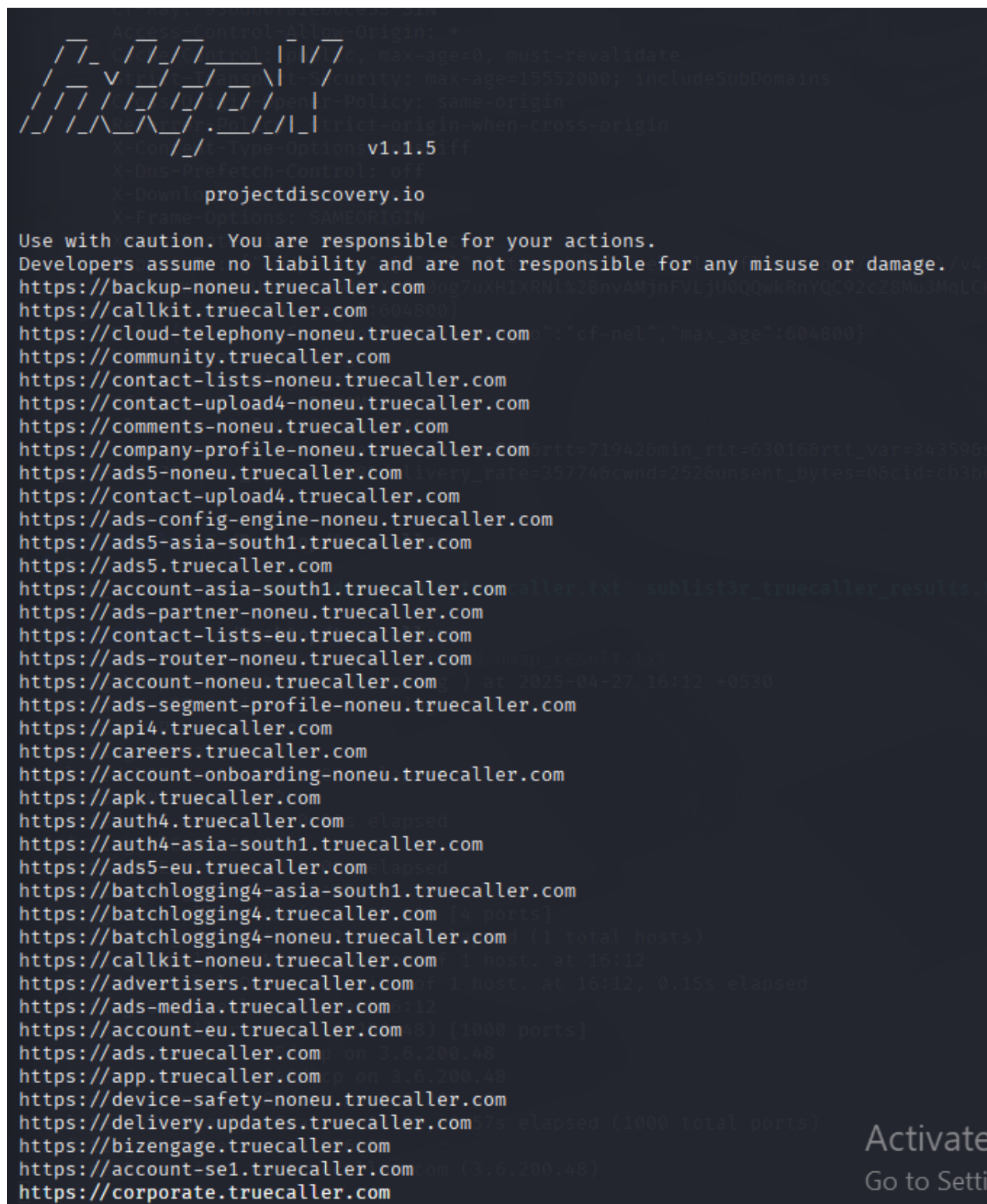
**Code** : `httpx-toolkit -l subfinder_result_truecaller.txt -o livesub_results.txt`

**Explanation:**

`httpx-toolkit` - run the httpx tool

`-l subfinder_result_truecaller.txt` – mention the file containing input

`-o livesub_results.txt` – mention the file which should write the output



```

Access-Control-Allow-Origin: *
max-age=0, must-revalidate
Security: max-age=15552000; includeSubDomains
Policy: same-origin
strict-origin-when-cross-origin
v1.1.5
X-Content-Type-Options: no-sniff
X-Dns-Prefetch-Control: off
X-Down: projectdiscovery.io
X-Frame-Options: SAMEORIGIN

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
https://backup-noneu.truecaller.com
https://callkit.truecaller.com
https://cloud-telephony-noneu.truecaller.com
https://community.truecaller.com
https://contact-lists-noneu.truecaller.com
https://contact-upload4-noneu.truecaller.com
https://comments-noneu.truecaller.com
https://company-profile-noneu.truecaller.com
https://ads5-noneu.truecaller.com
https://contact-upload4.truecaller.com
https://ads-config-engine-noneu.truecaller.com
https://ads5-asia-south1.truecaller.com
https://ads5.truecaller.com
https://account-asia-south1.truecaller.com
https://ads-partner-noneu.truecaller.com
https://contact-lists-eu.truecaller.com
https://ads-router-noneu.truecaller.com
https://account-noneu.truecaller.com
https://ads-segment-profile-noneu.truecaller.com
https://api4.truecaller.com
https://careers.truecaller.com
https://account-onboarding-noneu.truecaller.com
https://apk.truecaller.com
https://auth4.truecaller.com
https://auth4-asia-south1.truecaller.com
https://ads5-eu.truecaller.com
https://batchlogging4-asia-south1.truecaller.com
https://batchlogging4.truecaller.com
https://batchlogging4-noneu.truecaller.com
https://callkit-noneu.truecaller.com
https://advertisers.truecaller.com
https://ads-media.truecaller.com
https://account-eu.truecaller.com
https://ads.truecaller.com
https://app.truecaller.com
https://device-safety-noneu.truecaller.com
https://delivery.updates.truecaller.com
https://bizengage.truecaller.com
https://account-se1.truecaller.com
https://corporate.truecaller.com

```

<https://backup-noneu.truecaller.com>

<https://callkit.truecaller.com>

<https://cloud-telephony-noneu.truecaller.com>



<https://community.truecaller.com>  
<https://contact-lists-noneu.truecaller.com>  
<https://contact-upload4-noneu.truecaller.com>  
<https://comments-noneu.truecaller.com>  
<https://company-profile-noneu.truecaller.com>  
<https://ads5-noneu.truecaller.com>  
<https://contact-upload4.truecaller.com>  
<https://ads-config-engine-noneu.truecaller.com>  
<https://ads5-asia-south1.truecaller.com>  
<https://ads5.truecaller.com>  
<https://account-asia-south1.truecaller.com>  
<https://ads-partner-noneu.truecaller.com>  
<https://contact-lists-eu.truecaller.com>  
<https://ads-router-noneu.truecaller.com>  
<https://account-noneu.truecaller.com>  
<https://ads-segment-profile-noneu.truecaller.com>  
<https://api4.truecaller.com>  
<https://careers.truecaller.com>  
<https://account-onboarding-noneu.truecaller.com>  
<https://apk.truecaller.com>  
<https://auth4.truecaller.com>  
<https://auth4-asia-south1.truecaller.com>  
<https://ads5-eu.truecaller.com>  
<https://batchlogging4-asia-south1.truecaller.com>  
<https://batchlogging4.truecaller.com>  
<https://batchlogging4-noneu.truecaller.com>  
<https://callkit-noneu.truecaller.com>  
<https://advertisers.truecaller.com>  
<https://ads-media.truecaller.com>  
<https://account-eu.truecaller.com>  
<https://ads.truecaller.com>  
<https://app.truecaller.com>  
<https://device-safety-noneu.truecaller.com>  
<https://delivery.updates.truecaller.com>  
<https://bizengage.truecaller.com>  
<https://account-se1.truecaller.com>  
<https://corporate.truecaller.com>  
<https://batchlogging4-eu.truecaller.com>  
<https://callkit-eu.truecaller.com>  
<https://edge-locations5-noneu.truecaller.com>  
<https://edge-locations5.truecaller.com>  
<https://blog.truecaller.com>  
<https://enterprise-userfeedback-noneu.truecaller.com>  
<https://feature-flags-noneu.truecaller.com>  
<https://device-safety-eu.truecaller.com>  
<https://filter-store4-noneu.truecaller.com>  
<https://filter-store4.truecaller.com>  
<https://insights-categorizer-noneu.truecaller.com>  
<https://images-noneu.truecaller.com>  
<https://lastactivity-noneu.truecaller.com>  
<https://edge-locations5-eu.truecaller.com>  
<https://link-reports-noneu.truecaller.com>  
<https://leadgen.truecaller.com>  
<https://message-classifier-patterns-noneu.truecaller.com>  
<https://developer.truecaller.com>  
<https://messenger-noneu.truecaller.com>  
<https://messenger-previews-noneu.truecaller.com>

### c. IP Discovery

**Tool:** nslookup: [nslookup\\_result.txt](#)

**Code:** since we have a file with subdomains, to find IP addresses using “nslookup” we need to make a loop until all the IPs of all the subdomains are found.

```
while read sub; do
    echo "Looking up: $sub" >> nslookup_result.txt
    nslookup "$sub" | awk '/^Name:|^Address:/' >> nslookup_result.txt
    echo "-----" >> nslookup_result.txt
done < livesub_results.txt
```

#### Explanation:

*While read sub; do* - start of the loop

*Echo “Looking up: \$sub” >> nslookup\_result.txt* - print message “Looking up: subdomain” into the file “nslookup\_result.txt”

*nslookup “\$sub” | awk ‘/^Name:|^Address:/' >> nslookup\_result.txt* - run the nslookup command

*echo “-----” >> nslookup\_result.txt* - separate one subdomain details from another

*done < livesub\_results.txt* - End the loop and continue until the lines in the livesub\_results.txt

```
(kali@kali)~[~/Desktop/truecaller]
$ ./nslookup_script.sh

(kali@kali)~[~/Desktop/truecaller]
$ cat nslookup_result.txt
Looking up: https://backup-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://callkit.truecaller.com
Address:      192.168.0.1#53

Looking up: https://cloud-telephony-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://community.truecaller.com
Address:      192.168.0.1#53

Looking up: https://contact-lists-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://contact-upload4-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://comments-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://company-profile-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://ads5-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://contact-upload4.truecaller.com
Address:      192.168.0.1#53

Looking up: https://ads-config-engine-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://ads5-asia-south1.truecaller.com
Address:      192.168.0.1#53

Looking up: https://ads5.truecaller.com
Address:      192.168.0.1#53

Looking up: https://account-asia-south1.truecaller.com
Address:      192.168.0.1#53

Looking up: https://ads-partner-noneu.truecaller.com
Address:      192.168.0.1#53

Looking up: https://contact-lists-eu.truecaller.com
Address:      192.168.0.1#53
```

**IP list:**

Looking up: <https://backup-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://callkit.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://cloud-telephony-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://community.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://contact-lists-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://contact-upload4-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://comments-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://company-profile-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://ads5-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://contact-upload4.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://ads-config-engine-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://ads5-asia-south1.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://ads5.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://account-asia-south1.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://ads-partner-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://contact-lists-eu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://ads-router-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://account-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

Looking up: <https://ads-segment-profile-noneu.truecaller.com>

Address: 192.168.0.1#53

-----

#### d. Open Ports

**Tool:** nmap: [nmap\\_result.txt](#)

**Code:** `nmap -sV -A -v -O truecaller.com -oN nmap_results.txt`

**Explanation:**

`nmap` - start the tool  
`-sV` - Service and version detection  
`-A` - OS detection, version detection, script scanning  
`-v` - increase verbosity level  
`-O` - Os detection  
`- truecaller.com` - target website  
`-oN nmap_results.txt` - result in an output text file

```
(kali@kali)~[~/Desktop/truecaller]
$ nmap -sV -A -v -O truecaller.com -oN nmap_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 16:12 +0530
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:12
Completed NSE at 16:12, 0.00s elapsed
Initiating NSE at 16:12
Completed NSE at 16:12, 0.00s elapsed
Initiating NSE at 16:12
Completed NSE at 16:12, 0.00s elapsed
Initiating Ping Scan at 16:12
Scanning truecaller.com (3.6.200.48) [4 ports]
Completed Ping Scan at 16:12, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:12
Completed Parallel DNS resolution of 1 host. at 16:12, 0.15s elapsed
Initiating SYN Stealth Scan at 16:12
Scanning truecaller.com (3.6.200.48) [1000 ports]
Discovered open port 25/tcp on 3.6.200.48
Discovered open port 443/tcp on 3.6.200.48
Discovered open port 80/tcp on 3.6.200.48
Completed SYN Stealth Scan at 16:12, 6.57s elapsed (1000 total ports)
Initiating Service scan at 16:12
Scanning 3 services on truecaller.com (3.6.200.48)
Completed Service scan at 16:13, 29.38s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against truecaller.com (3.6.200.48)
Retrying OS detection (try #2) against truecaller.com (3.6.200.48)
Initiating Traceroute at 16:13
Completed Traceroute at 16:13, 0.02s elapsed
Initiating Parallel DNS resolution of 1 host. at 16:13
Completed Parallel DNS resolution of 1 host. at 16:13, 0.04s elapsed
NSE: Script scanning 3.6.200.48.
Initiating NSE at 16:13
Completed NSE at 16:14, 33.14s elapsed
Initiating NSE at 16:14
Completed NSE at 16:14, 1.95s elapsed
Initiating NSE at 16:14
Completed NSE at 16:14, 0.01s elapsed
Nmap scan report for truecaller.com (3.6.200.48)
Host is up (0.0029s latency).
Other addresses for truecaller.com (not scanned): 3.6.216.71 2406:da00:a000::306:c830 2406:da00:a000::306:d847
rDNS record for 3.6.200.48: ec2-3-6-200-48.ap-south-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http   nginx
|_http-title: Did not follow redirect to https://www.truecaller.com/
|_http-methods:
|_ Supported Methods: GET
443/tcp   open  tcpwrapped
|_ssl-cert: Subject: commonName=truecaller.com
| Subject Alternative Name: DNS:truecaller.com
```

Activate Windows  
Go to Settings to activate Windows.



### e. Used Technologies

**Tool:** whatweb - [whatweb result.txt](#)

**Code:** whatweb -v truecaller.com > whatweb\_result.txt

**Explanation:**

*whatweb* - start whatweb tool

*-v* - verbose

*Truecaller.com* - target website

> *whatweb\_result.txt* - file with the output

```
(kali@kali)-[~/Desktop/truecaller]
$ whatweb -v truecaller.com --o whatweb_results.txt
WhatWeb report for http://truecaller.com
Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 3.6.200.48
Country : UNITED STATES, US

Summary : HTTPServer[nginx], nginx, RedirectLocation[https://www.truecaller.com/]

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

    String : nginx (from server string)

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

    String : https://www.truecaller.com/ (from location)

[ nginx ]
    Nginx (Engine-X) is a free, open-source, high-performance
    HTTP server and reverse proxy, as well as an IMAP/POP3
    proxy server.

    Website : http://nginx.net/

HTTP Headers:
HTTP/1.1 301 Moved Permanently
Content-Type: text/html
Date: Sun, 27 Apr 2025 10:38:32 GMT
Location: https://www.truecaller.com/
Server: nginx
Content-Length: 178
Connection: Close

WhatWeb report for https://www.truecaller.com/
Status : 200 OK
Title : Truecaller - Leading Global Caller ID & Call Blocking App
IP : 104.26.9.130
Country : UNITED STATES, US

Summary : HTML5, HTTPServer[cloudflare], Open-Graph-Protocol[website], PoweredBy[Apple's], Script[application/javascript,module,text/javascript], Strict-Transport-Security[max-age=15552000; includeSubDomains], UncommonHeaders[cf-ray,access-control-allow-origin,cross-origin-opener-policy,referrer-policy,x-content-type-options,x-dns-prefetch-control,x-download-options,report-to,nel,cf-cache-status,alt-svc,server-timing], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]

Detected Plugins:
[ HTML5 ]
    HTML version 5, detected by the doctype declaration
```

Activate Windows  
Go to Settings to activate Windows.

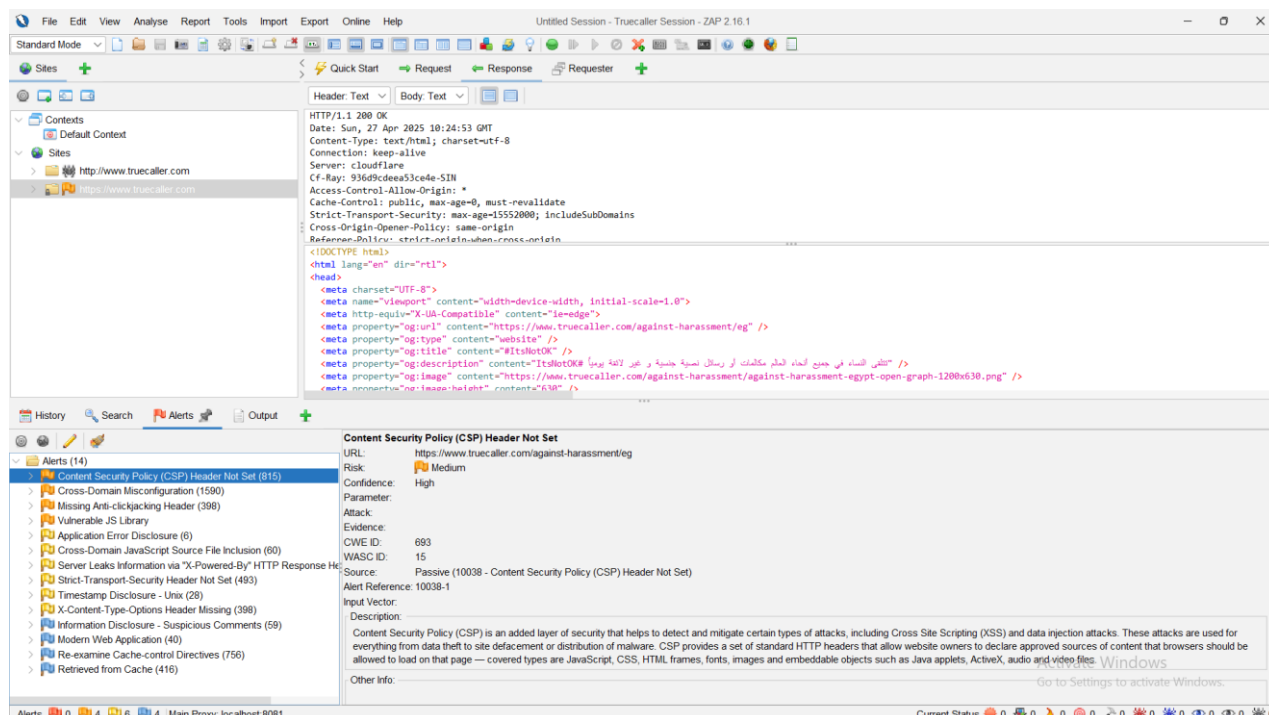


### 3. Step 02: Scanning and vulnerability identification

#### a. Identify Potential Vulnerabilities

**Tool** : OWASP ZAP

**Vulnerability** : Content Security Policy (CSP) Header Not Set



#### Content Security Policy (CSP) Header Not Set:

URL: <https://www.truecaller.com/against-harassment/eg>

Risk: Medium

Confidential: High

Parameter:

Attack:

Evidence:

CWE ID: 693

WASC ID: 15

Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)

Alert Reference: 10038-1

Input Vector:

- Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
- Other Info:
- Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
- Reference:
  - [https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\\_Content\\_Security\\_Policy](https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy)
  - [https://cheatsheetseries.owasp.org/cheatsheets/Content\\_Security\\_Policy\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html)
  - <https://www.w3.org/TR/CSP/>
  - <https://w3c.github.io/webappsec-csp/>
  - <https://web.dev/articles/csp>
  - <https://caniuse.com/#feat=contentsecuritypolicy>

- <https://content-security-policy.com/>
- Alert Tags:
  - OWASP\_2021\_A05: [https://owasp.org/Top10/A05\\_2021-Security\\_Misconfiguration/](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)
  - CWE-693: <https://cwe.mitre.org/data/definitions/693.html>
  - OWASP\_2017\_A06: [https://owasp.org/www-project-top-ten/2017/A6\\_2017-Security\\_Misconfiguration.html](https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html)

## b. Content Security Policy (CSP) Header Not Set

A **Content Security Policy (CSP)** is a security standard that helps prevent a variety of attacks such as Cross-Site Scripting (XSS), clickjacking, and data injection by controlling the sources from which content can be loaded on a web page. If the CSP header is not set, websites are much more vulnerable to these attacks because browsers will not enforce any restrictions on content loading behavior.

Cause of Content Security Policy (CSP) Header Not Set website:

- Lack of awareness or understanding about the importance of CSP
- Assuming that HTTPS alone is enough to secure web content
- Complex web applications making CSP rules difficult to implement
- Fear of breaking existing site functionality when enforcing a strict CSP
- Not using modern web development frameworks that support automatic CSP generation
- Ignoring browser security best practices during deployment

Propositions to Mitigation or Fix:

- Set a Strong CSP Header: Define a restrictive CSP using directives like default-src, script-src, img-src, etc.
- Use CSP Generators and Validators: Tools like Mozilla Observatory and CSP Evaluator can help create and validate policies
- Implement CSP in Reporting Mode First: Use Content-Security-Policy-Report-Only to monitor potential issues before enforcing
- Minimize Inline Scripts and Styles: Refactor the application to reduce or eliminate inline JavaScript and CSS
- Regularly Update CSP Policies: Adjust and tighten the policy over time as the website evolves
- Educate Developers and Security Teams: Make sure everyone understands the role and benefits of CSP in web security
- Combine with Other Headers: Use CSP alongside other security headers like X-Frame-Options, Strict-Transport-Security, and X-Content-Type-Options for layered protection

## 4. Step 03: Exploitation and Validation

### Request:

```
GET https://www.truecaller.com/against-harassment/eg HTTP/1.1
host: www.truecaller.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://www.truecaller.com/sitemap.xml
```

### Response:

```
HTTP/1.1 200 OK
Date: Sun, 27 Apr 2025 10:24:53 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Server: cloudflare
Cf-Ray: 936d9cdea53ce4e-SIN
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0, must-revalidate
Strict-Transport-Security: max-age=15552000; includeSubDomains
Cross-Origin-Opener-Policy: same-origin
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
X-Dns-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=0w8mQ6sFq10Fjq3m4etebd0vHmKu4pxbaapMMDeT08cBfg3KUUIf7R8zKc80pWxzQg5wisabNOsAEzjA0vcEGKoKjfnWcbQnKvZBvQRV8X6%2F7vUEfyr4E910eT6AScsCU0Zbm8%3D"}], "group":"cf-nel", "max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel", "max_age":604800}
Vary: Accept-Encoding

<!DOCTYPE html>
<html lang="en" dir="rtl">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <meta property="og:url" content="https://www.truecaller.com/against-harassment/eg" />
  <meta property="og:type" content="website" />
  <meta property="og:title" content="#ItsNotOK" />
  <meta property="og:description" content="تتلى النساء في جميع أنحاء العالم مكالمات أو رسائل نصية جنسية و غير لائقة بويماً #ItsNotOK" />
  <meta property="og:image" content="https://www.truecaller.com/against-harassment/against-harassment-egypt-open-graph-1200x630.png" />
  <meta property="og:image:height" content="630" />
  <meta property="og:image:width" content="1200" />
  <meta name="twitter:image" content="https://www.truecaller.com/against-harassment/against-harassment-egypt-open-graph-1200x1200.png">
  <meta name="description" content="تتلى النساء في جميع أنحاء العالم مكالمات أو رسائل نصية جنسية و غير لائقة بويماً #ItsNotOK" />
  <link rel="stylesheet" href="https://use.typekit.net/cak5zly.css">
  <link rel="stylesheet" href="/against-harassment/ah-styles-003.css">
  <title>#ItsNotOK</title>
  <script defer data-domain="truecaller.com" src="https://plausible.io/js/script.js"></script>
</script>
<script>
  document.documentElement.setAttribute("cf-window-internal-height", 0.01m);
</script>
```

## 5. Step 04: Mitigation / Fix

Immediate Mitigation Actions:

1. Implement a Basic CSP header to restrict content sources.

Long Term Prevention:

1. Use tools like [CSP Builder](#) to create policies.
2. Scan for CSP bypasses with *OWASP ZAP* or *Burp Suite*.