

Sri Lanka Institute of Information Technology



BUG BOUNTY REPORT - 1

Web Security – IE2062

IT22362780

Jayaweera N.S

Report Details

Report # - 01

Domain - <https://truecaller.com>

Platform -hackerone.com

Scans performed - Recon-ng scan
Nmap scan
Metasploit testing
Nslookup
Wafw00f scan
Gobuster scan
Wapplyzer scan
Zap scan
Dotdotpwn scan
Sqlmap scan
Text injection testing
XSS injection testing
Command injection testing

Recon scan

The recon-ng will be used to find all the sub domains in the target.

```
(kali@kali)~$ recon-ng
[*] Version check disabled.

Download Truecaller

Sponsored by ...

BLACK HILLS
www.blackhillsinfosec.com

PRACTISEC
www.practisec.com

[bb1]@kali: [recon-ng v5.1.2; Tim Tones (@lanmaster53)]

[*] No modules enabled/installed.
[recon-ng][default] > workspaces create bb1
[recon-ng][bb1] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][bb1] > modules load hackertarget
```

Installing the module” hackertarget”.

```
[*] No modules enabled/installed.

[recon-ng][default] > workspaces create bb1
[recon-ng][bb1] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...

[recon-ng][bb1] > modules load hackertarget
[recon-ng][bb1][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][bb1][hackertarget] > options set SOURCE truecaller.com
SOURCE ⇒ truecaller.com
[recon-ng][bb1][hackertarget] > run
```

Set the source to truecaller.com

```
[*] Country: None
[*] Host: truecaller.com
[*] Ip_Address: 65.2.43.23
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: account-asia-south1.truecaller.com
[*] Ip_Address: 35.190.118.8
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: account-noneu.truecaller.com
[*] Ip_Address: 35.190.118.8
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ads.truecaller.com
[*] Ip_Address: 192.121.90.120
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

100 sub domains are found.

```
[*] Country: None
[*] Host: www.truecaller.com
[*] Ip_Address: 199.36.158.100
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
SUMMARY
[*] 100 total (100 new) hosts found.
[recon-ng][bb1][hackertarget] >
```

Nmap scan

Using nmap scan all the open ports in the target can be identified.

```
(kali@kali)~$ nmap -sS -T4 truecaller.com
You requested a scan type which requires root privileges.
QUITTING!

(kali@kali)~$ sudo nmap -sS -T4 truecaller.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-10 01:44 EDT
Nmap scan report for truecaller.com (65.2.43.23)
Host is up (0.014s latency).
Other addresses for truecaller.com (not scanned): 13.232.183.173
rDNS record for 65.2.43.23: ec2-65-2-43-23.ap-south-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

No unusual ports are open.

But Smtip port 25 is vulnerable when it's opened, because it lacks authentication and encryption.

Let's see if we can establish a connection on port 25.

```
(kali@kali)~$ nmap truecaller.com --script=smtp* -p 25
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-10 01:52 EDT
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 55.56% done; ETC: 01:53 (0:00:19 remaining)
Nmap scan report for truecaller.com (65.2.43.23)
Host is up (0.050s latency).
Other addresses for truecaller.com (not scanned): 13.232.183.173
rDNS record for 65.2.43.23: ec2-65-2-43-23.ap-south-1.compute.amazonaws.com

PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-enum-users: it uses cookies
|_ Couldn't establish connection on port 25
|_smtp-commands: Couldn't establish connection on port 25
|_smtp-open-relay: Couldn't establish connection on port 25

Nmap done: 1 IP address (1 host up) scanned in 35.77 seconds
```

Connection cannot be established therefore a vulnerability cannot be identified.

Metasploit scan

[illegible]

Search for the smtp.

```

#--=--=--=
#--=--= 2204 exploits - 1189 auxiliary - 484 post
#--=--= 951 payloads - 43 encoders - 11 nops
#--=--= 2 evasion

```

Metasploit tip: Search can apply complex filters such as search cve:2000 type:exploit, see all the filters with help search

Metasploit Documentation: <https://docs.metasploit.com/>

info > search -help

Matching Modules

Download Table

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/000/apache_james_user	2015-10-01	normal	Yes	Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
1	auxiliary/server/capture/000		normal	No	Authentication Capture: 000
2	auxiliary/wcmw/000/gawazi_on_login_foat		normal	No	Carlo Gawazi Energy Meters - Login Brute Force, Extract Info and Den
Platform Database					
3	exploit/linux/000/clsaw_miller_blackhole	2007-06-26	excellent	No	CLAW Miller Blackhole-Node Remote Code Execution
4	exploit/windows/browser/remoteclient_mail_active	2010-05-10	great	No	CommuniCrypt Mail 3.36 000 ActiveX Stack Buffer Overflow
5	exploit/linux/000/exim_gethostbyname_buf	2015-01-27	great	Yes	Exim GHOST (glibc gethostbyname) buffer overflow
6	exploit/linux/000/exim4_insecure_coot	2013-02-02	excellent	No	Exim and Dovecot Insecure Configuration Command Injection
7	exploit/linux/000/exim4_string_format	2018-12-07	excellent	No	Exim4 string format function heap buffer overflow
8	auxiliary/c/000/000/emailer	2017-01-26	normal	Yes	Generic Eximilr (000)
9	exploit/linux/000/000/exim4	2017-01-26	excellent	No	Exim4 000 Command Injection
10	exploit/windows/http/mosman_worldclient_firmware	2003-12-20	great	Yes	Mosman WorldClient Firmware.cgi Stack Buffer Overflow
11	exploit/windows/000/msbl_0at_exchange2000_exchange	2003-10-15	good	Yes	MSB-004 Exchange 2000 EXCH50 Heap Overflow
12	exploit/windows/x64/mw6_011_cpi	2004-06-13	average	No	MS04-011 Microsoft Private Communications Transport Overflow
13	auxiliary/linux/windows/000/mw6_010_exchange	2004-11-12	normal	No	MS04-010 Exchange MS04PROF Heap Overflow

Use the module “fuzzer” to fuzz the smtp service. And for username enumeration use the “smtp_enum”

```

Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/postup_userflow1

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(15auxiliary/scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):



| Name      | Current Setting                                               | Required | Description                                                                                                                                                                     |
|-----------|---------------------------------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS    |                                                               | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT     | 25                                                            | yes      | The target port (TCP)                                                                                                                                                           |
| THREADS   | 1                                                             | yes      | The number of concurrent threads (max one per host)                                                                                                                             |
| UNIXONLY  | true                                                          | yes      | Skip Microsoft bannered servers when testing unix users                                                                                                                         |
| USER_FILE | /usr/share/metasploit-framework/data/wordlists/unix_users.txt | yes      | The file that contains a list of probable users accounts.                                                                                                                       |



View the full module info with the info, or info -i command.

msf6 auxiliary(15auxiliary/scanner/smtp/smtp_enum) > set RHOSTS 65.2.43.23
RHOSTS => 65.2.43.23
msf6 auxiliary(15auxiliary/scanner/smtp/smtp_enum) > run
[*] Unknown command: RUN
msf6 auxiliary(15auxiliary/scanner/smtp/smtp_enum) > run

[*] 65.2.43.23:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```



```
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > set RHOSTS truecaller.com
RHOSTS => truecaller.com
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > run

[-] 65.2.43.23:25 - The connection with (65.2.43.23:25) timed out.
[*] 65.2.43.23:25 - Fuzzing with iteration 1

[*] 65.2.43.23:25 - Could not connect to the service:
[*] truecaller.com:25 - Scanned 1 of 2 hosts (50% complete)
[*] truecaller.com:25 - Scanned 1 of 2 hosts (50% complete)
[*] truecaller.com:25 - Scanned 1 of 2 hosts (50% complete)
[*] truecaller.com:25 - Scanned 1 of 2 hosts (50% complete)
[*] truecaller.com:25 - Scanned 1 of 2 hosts (50% complete)
[-] 13.232.183.173:25 - The connection with (13.232.183.173:25) timed out.
[*] 13.232.183.173:25 - Fuzzing with iteration 1

[*] 13.232.183.173:25 - Could not connect to the service:
[*] truecaller.com:25 - Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > █
```

Fuzzing failed due to connection time out indicating inability to enumerate the service.

Nslookup

With the use of the command below, the ip address of the web applications can be found.

```
(kali@kali)-[~]  
$ nslookup truecaller.com  
Server:         192.168.1.1  
Address:        192.168.1.1#53  
  
Non-authoritative answer:  
Name:   truecaller.com  
Address: 65.2.43.23  
Name:   truecaller.com  
Address: 13.232.183.173
```


Wafw00f scan

Used to identify the type of WAF that is used to protect the web application.

No WAF detected from the above scan.

Gobuster scan

The gobuster scan helps to find hidden Directories, URLs, Sub-Domains, and S3 Buckets seamlessly.

```
[kali@kali:~]$ gobuster dir -u https://www.truecaller.com -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehleiner (@firefart)

[*] Url: https://www.truecaller.com
[*] Method: GET
[*] Threads: 10
[*] Wordlist: /usr/share/wordlists/dirb/common.txt
[*] Negative Status codes: 404
[*] User Agent: gobuster/3.6
[*] Timeout: 10s

Starting gobuster in directory enumeration mode

/ (Status: 201) [Size: 123] => https://play.google.com/store/apps/details?id=com.truecaller&referrer=utm_source%3Dgoogle&ad=com.truecaller
/about (Status: 200) [Size: 171143]
/About (Status: 200) [Size: 192417]
/Blog (Status: 200) [Size: 334387]
/blog (Status: 200) [Size: 334413]
/careers (Status: 200) [Size: 156012]
/contact (Status: 201) [Size: 70] => https://corporate.truecaller.com/newsroom/media-contact
/cookies (Status: 201) [Size: 29] => /cookie-policy
/directory (Status: 200) [Size: 137800]
/Download (Status: 200) [Size: 177105]
/download (Status: 200) [Size: 197009]
/es (Status: 201) [Size: 21] => /es-es
/features (Status: 200) [Size: 199079]
/id (Status: 201) [Size: 21] => /id-id
/i (Status: 201) [Size: 94] => https://itunes.apple.com/app/apple-store/id441245870?mt=8&referrer=utm_source%3Dgoogle&ad=com.truecaller
```

```
Starting gobuster in directory enumeration mode

/ (Status: 201) [Size: 123] => https://play.google.com/store/apps/details?id=com.truecaller&referrer=utm_source%3Dgoogle&ad=com.truecaller
/about (Status: 200) [Size: 171143]
/About (Status: 200) [Size: 192417]
/Blog (Status: 200) [Size: 334387]
/blog (Status: 200) [Size: 334413]
/careers (Status: 200) [Size: 156012]
/contact (Status: 201) [Size: 70] => https://corporate.truecaller.com/newsroom/media-contact
/cookies (Status: 201) [Size: 29] => /cookie-policy
/directory (Status: 200) [Size: 137800]
/Download (Status: 200) [Size: 177105]
/download (Status: 200) [Size: 197009]
/es (Status: 201) [Size: 21] => /es-es
/features (Status: 200) [Size: 199079]
/id (Status: 201) [Size: 21] => /id-id
/i (Status: 201) [Size: 94] => https://itunes.apple.com/app/apple-store/id441245870?mt=8&referrer=utm_source%3Dgoogle&ad=com.truecaller
/index (Status: 201) [Size: 16] => /
/index.html (Status: 201) [Size: 16] => /
/messaging (Status: 200) [Size: 183907]
/promius (Status: 200) [Size: 164678]
/preview (Status: 200) [Size: 109571]
/privacy-policy (Status: 200) [Size: 164327]
/privacy (Status: 201) [Size: 36] => /privacy-policy-contact
/robots.txt (Status: 200) [Size: 247]
/safety (Status: 200) [Size: 189311]
/sitemap.xml (Status: 200) [Size: 18988]
/support (Status: 201) [Size: 50] => https://support.truecaller.com/support/home
/us (Status: 201) [Size: 167] => /
/x (Status: 201) [Size: 24] => /download

Progress: 4610 / 4615 (99.88%)
Finished
```

Sqlmap scan

With the use of this scan, we can identify whether a sql injection can be done or not.

```
(kali@kali:~)$ sqlmap -u https://support.truecaller.com/support/search?term=lalala
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] ending @ 04:00:39 /2024-04-18/
```

```
I V
[04/00:32] [INFO] testing 'Generic UNION query (NULL) - 1 to 38 columns'
[04/00:34] [WARNING] GET parameter 'term' does not seem to be injectable
[04/00:39] [CRITICAL] All tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. Please retry with the switch '--test-only' (along with --technique=02) as this case looks like a perfect candidate (low textual content along with inability of comparison engine to detect at least one dynamic parameter). If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[04/00:39] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 87 times
[04/00:39] [WARNING] your sqlmap version is outdated
```

The above results prove that there is no injection vulnerability in the above web application.

Dotdotpwn scan

Dotdotpwn is a directory traversal checker.

```
[===== TARGET INFORMATION =====]
[+] Hostname: truecaller.com
[+] Protocol: http
[+] Port: 80

[===== TRAVERSAL ENGINE =====]
[+] Creating Traversal patterns (mix of dots and slashes)
[+] Multiplying 6 times the traversal patterns (-d switch)
[+] Creating the Special Traversal patterns
[+] Translating (back)slashes in the filenames
[+] Adapting the filenames according to the OS type detected (unix)
[+] Including Special suffixes
[+] Traversal Engine DONE ! - Total traversal tests created: 11028

[===== TESTING RESULTS =====]
[+] Ready to launch 3.33 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)

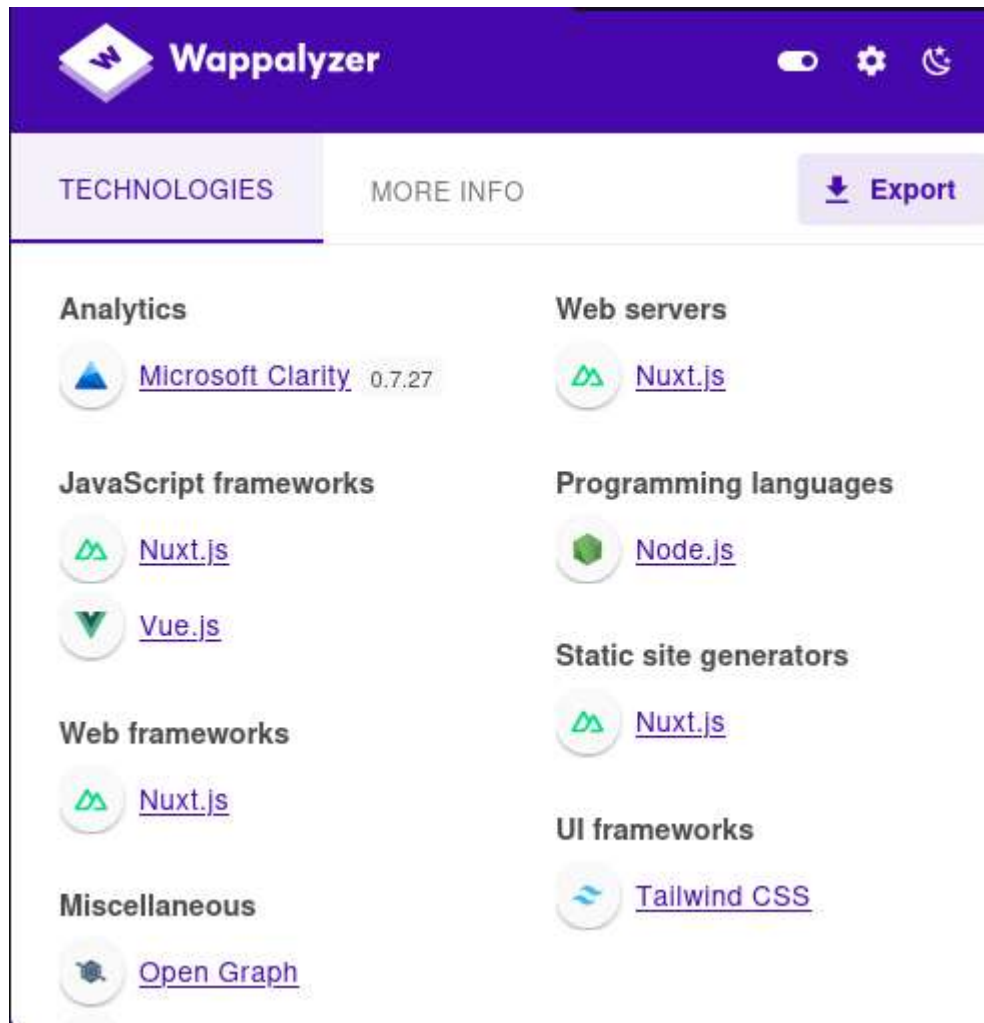
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../..etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../..etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://truecaller.com:80/../../../../etc/issue
```

The scan results returned status codes within the range 400 (400-499). It shows a client error.

Therefore, we can conclude that the tested destinations are not vulnerable to a directory traversal.

Manual scanning -using Wapplyzer

The Wapplyzer is used to identify the technologies used in the web application.



No unusual/vulnerable versions are found.

Zap scan

With the use of the “active scan”, some potential vulnerabilities can be found.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (14.3%)	1 (14.3%)
	Medium	0 (0.0%)	1 (14.3%)	0 (0.0%)	2 (28.6%)	3 (42.9%)
	Low	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (28.6%)	1 (14.3%)	3 (42.9%)
	Total	0 (0.0%)	1 (14.3%)	2 (28.6%)	4 (57.1%)	7 (100%)

Risk=Medium, Confidence=Low (2)

<http://truecaller.com> (2)

Absence of Anti-CSRF Tokens (1)

► GET <http://truecaller.com>

Hidden File Found (1)

► GET <http://truecaller.com/.hg>

Risk=High, Confidence=Low (1)

<http://truecaller.com> (1)

Cloud Metadata Potentially Exposed (1)

► GET <http://truecaller.com/latest/meta-data/>

Risk=Medium, Confidence=High (1)

<http://truecaller.com> (1)

Content Security Policy (CSP) Header Not Set (1)

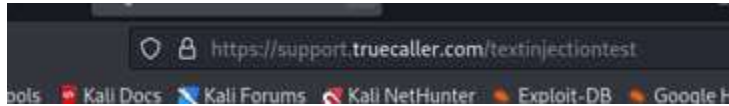
► GET <http://truecaller.com>

According to the above results the following can be found:

- Absence of anti-CSRF tokens.
- One hidden file found.
- Cloud meta data are potentially exposed.
- Content security policy (CSP) header not set.

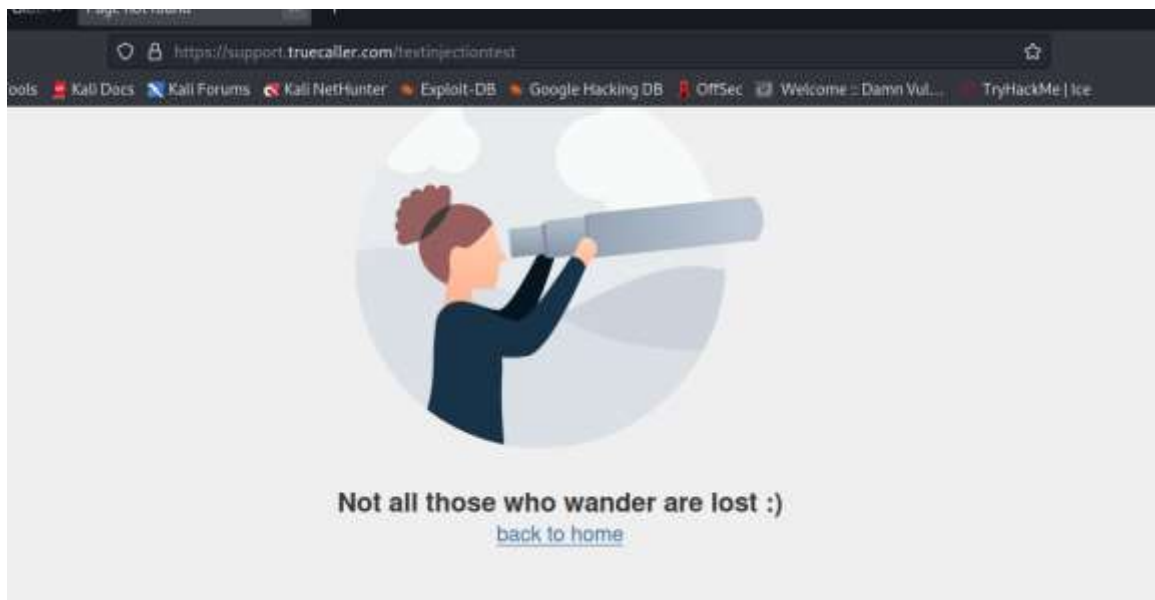
Text injection

An arbitrary string value is appended to the URL to see whether the web application is vulnerable towards a text injection.



If the entered text is reflected on the error response of the web page, there is a possibility to inject malicious content.

If not, the web application is safe.

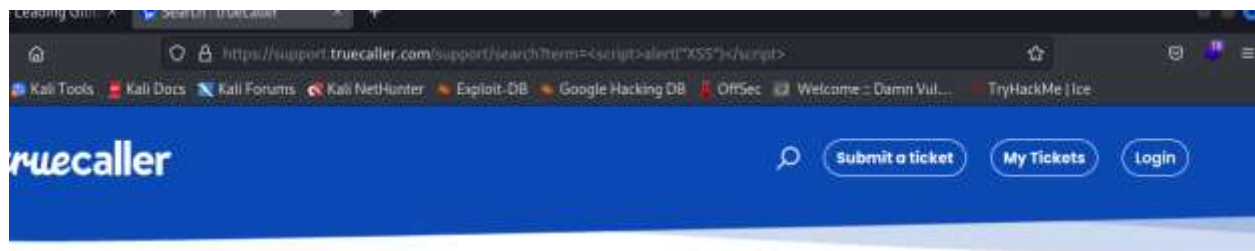


There is no possibility for a text injection.

XSS injection testing

This scan checks whether the web application is vulnerable to XSS injection.

There is a search function, and we can pass the parameters to the url and checked against xss injection.

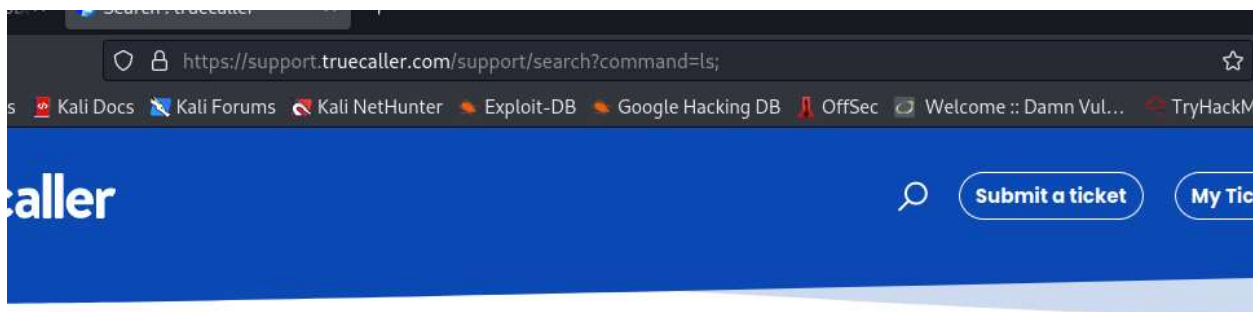
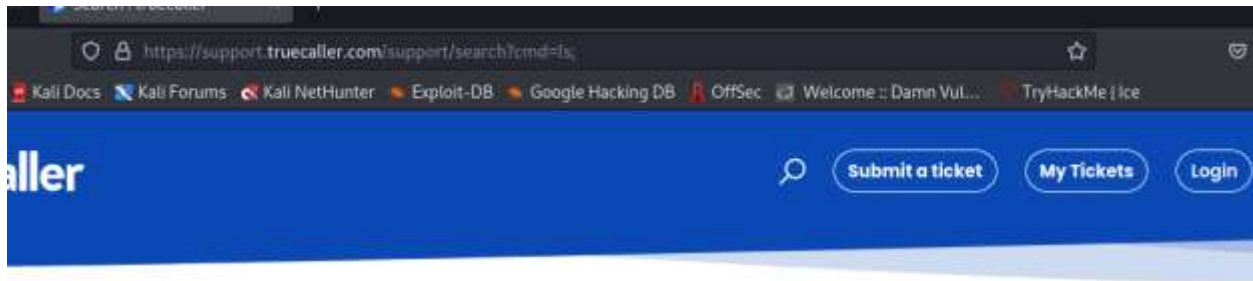


It is safe from reflective xss.

Command injection testing

The query that is used for searching is used against this vulnerability.

The “ls” command is appended to the url.



No command injection vulnerability can be found.