Sri Lanka Institute of Information Technology

BUG BOUNTY REPORT - 8

Web Security – IE2062

IT22362780

Jayaweera N.S

Report Details

Report #	- 08
Domain	- https://tripadvisor.com
Platform	-bugcrowd.com
Scans performed -	Recon-ng scan Nmap scan Wafw00f scan Dotdotpwn scan Nikto scan Sqlmap scan Manual scanning using Wapplyzer Text injection testing File upload vulnerability testing Command injection testing XSS injection testing Metasploit scan Nslookup

Nmap scan

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

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 tripadvisor.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 03:48 EDT
Nmap scan report for tripadvisor.com (151.101.66.28)
Host is up (0.015s latency).
Other addresses for tripadvisor.com (not scanned): 151.101.130.28 151.101.194.28 151.101.2.28
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 6.10 seconds
```

No unusual ports found.

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

In order to find whether it’s vulnerable let’s run a Metasploit scan.

Metasploit

```
msf6 > search smtp

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                  2015-10-01       normal     Yes    Apache James Serv
e
   1   auxiliary/server/capture/smtp                                          normal     No     Authentication Ca
   2   auxiliary/scanner/http/gavazzi_em_login_loot                           normal     No     Carlo Gavazzi Ene
mp Plant Database
   3   exploit/unix/smtp/clamav_milter_blackhole             2007-08-24       excellent  No     ClamAV Milter Bla
   4   exploit/windows/browser/communicrypt_mail_activex     2010-05-19       great      No     CommuniCrypt Mail
   5   exploit/linux/smtp/exim_gethostbyname_bof             2015-01-27       great      Yes    Exim GHOST (glibc
   6   exploit/linux/smtp/exim4_dovecot_exec                 2013-05-03       excellent  No     Exim and Dovecot
   7   exploit/unix/smtp/exim4_string_format                 2010-12-07       excellent  No     Exim4 string_form
   8   auxiliary/client/smtp/emailer                                          normal     No     Generic Emailer (
   9   exploit/linux/smtp/haraka                             2017-01-26       excellent  Yes    Haraka SMTP Comma
   10  exploit/windows/http/mdaemon_worldclient_form2raw     2003-12-29       great      Yes    MDaemon WorldClie
   11  exploit/windows/smtp/ms03_046_exchange2000_xexch50    2003-10-15       good       Yes    MS03-046 Exchange
   12  exploit/windows/ssl/ms04_011_pct                      2004-04-13       average    No     MS04-011 Microsof
   13  auxiliary/dos/windows/smtp/ms06_019_exchange          2004-11-12       normal     No     MS06-019 Exchange
   14  exploit/windows/smtp/mercury_cram_md5                 2007-08-18       great      No     Mercury Mail SMTP
   15  exploit/unix/smtp/morris_sendmail_debug               1988-11-02       average    Yes    Morris Worm sendm
```

search for smtp.

```
msf6 > use auxiliary/fuzzers/smtp/smtp_fuzzer
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > show options

Module options (auxiliary/fuzzers/smtp/smtp_fuzzer):

   Name          Current Setting     Required  Description
   ----          ---------------     --------  -----------
   CMD           EHLO                yes       Command to fuzzer (Accepted: EHLO, HELO, MAILFROM, RCPTTO, DATA, VRFY, EXPN)
   INTERACTIONS  100                 no        Number of interactions to run
   MAILFROM      sender@example.com  yes       FROM address of the e-mail
   MAILTO        target@example.com  yes       TO address of the e-mail
   RESPECTORDER  true                no        Respect order of commands
   RHOSTS                            yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metaspl
   RPORT         25                  yes       The target port (TCP)
   STARTLEN      100                 yes       Length of the string - start number
   THREADS       1                   yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
```

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

Set the RHOSTS to tripadvisor.com

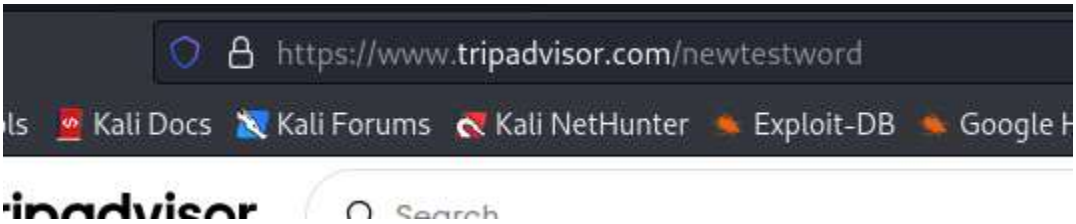
```
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > set RHOSTS tripadvisor.com
RHOSTS => tripadvisor.com
msf6 auxiliary(fuzzers/smtp/smtp_fuzzer) > run

[-] 151.101.130.28:25     - Connection reset by peer
[*] 151.101.130.28:25     - Fuzzing with iteration 1

[-] 151.101.130.28:25     - EOFError
[*] 151.101.130.28:25     - Fuzzing with iteration 2

[-] 151.101.130.28:25     - EOFError
[*] 151.101.130.28:25     - Fuzzing with iteration 3

[-] 151.101.130.28:25     - Connection reset by peer
[*] 151.101.130.28:25     - Fuzzing with iteration 4

[-] 151.101.130.28:25     - Connection reset by peer
[*] 151.101.130.28:25     - Fuzzing with iteration 5

[-] 151.101.130.28:25     - Connection reset by peer
[*] 151.101.130.28:25     - Fuzzing with iteration 6

[-] 151.101.130.28:25     - Connection reset by peer
[*] 151.101.130.28:25     - Fuzzing with iteration 7

[-] 151.101.130.28:25     - EOFError
[*] 151.101.130.28:25     - Fuzzing with iteration 8

[-] 151.101.130.28:25     - Connection reset by peer
[*] 151.101.130.28:25     - Fuzzing with iteration 9
```

```
[-] 151.101.66.28:25      - EOFError
[*] 151.101.66.28:25      - Fuzzing with iteration 97

[-] 151.101.66.28:25      - EOFError
[*] 151.101.66.28:25      - Fuzzing with iteration 98

[-] 151.101.66.28:25      - EOFError
[*] 151.101.66.28:25      - Fuzzing with iteration 99

[-] 151.101.66.28:25      - EOFError
[*] 151.101.66.28:25      - Fuzzing with iteration 100

[*] tripadvisor.com:25    - Scanned 4 of 4 hosts (100% complete)
[*] Auxiliary module execution completed
```

Fuzzing failed due to connection time out indicating inability to enumerate the service. fuzzing attempts blocked by server.

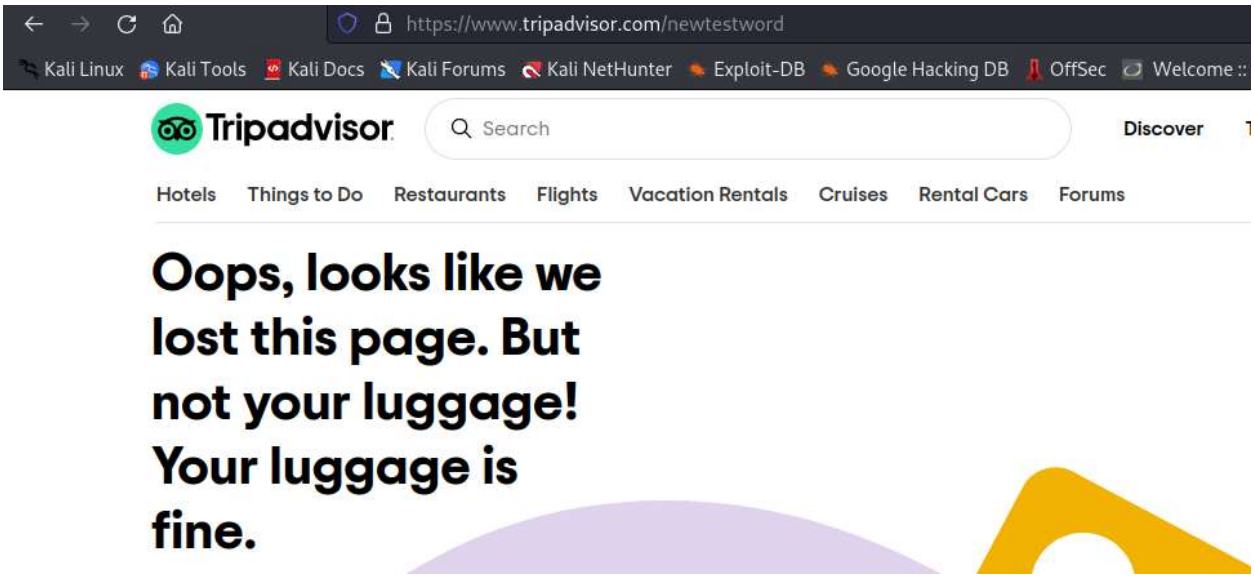
Text injection

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.



No text injection vulnerability can be found.

Wafw00f scan

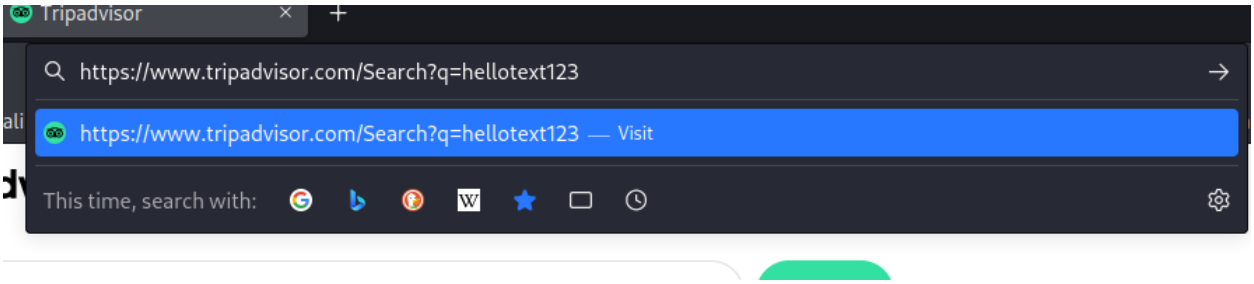
Used to identify the type of WAF that is used to protect the web application.

```
┌──(kali㉿kali)-[~]
└─$ wafw00f https://tripadvisor.com

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://tripadvisor.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

No WAF is used in this web application.

Sql map

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



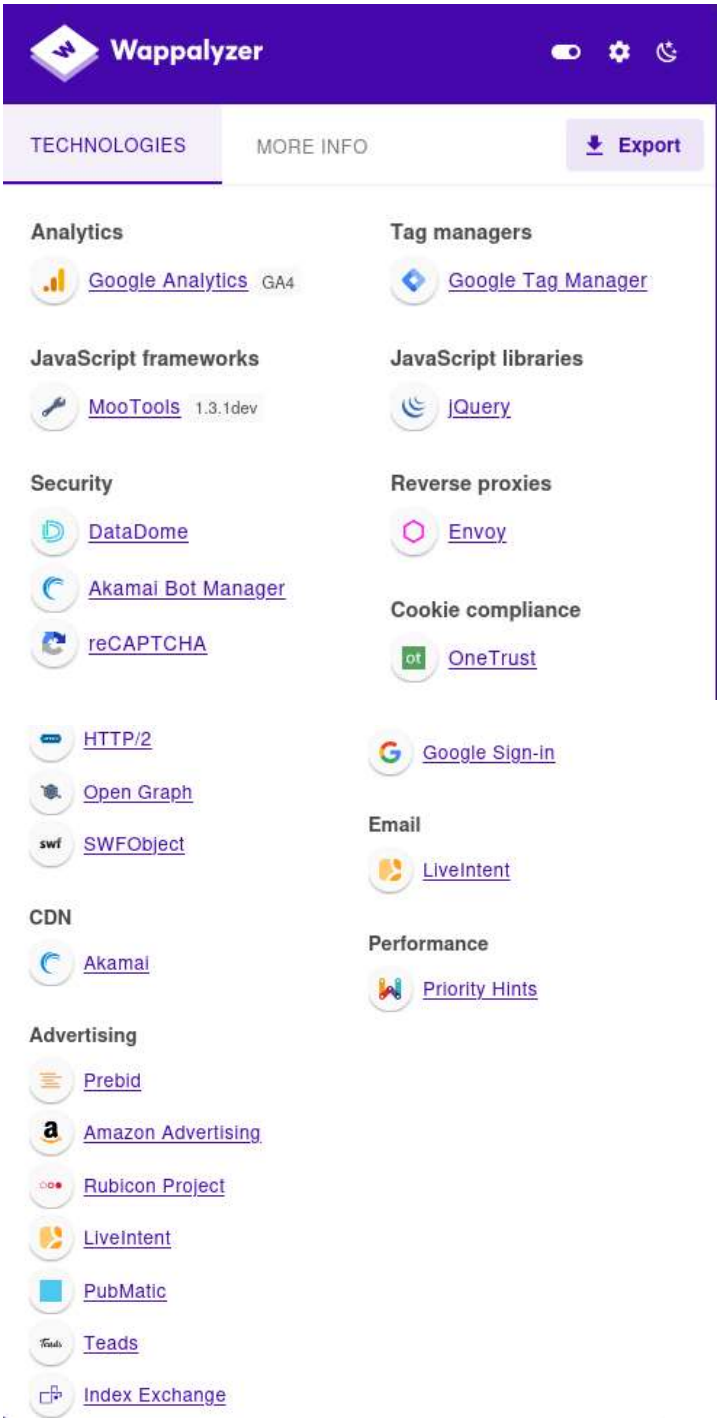

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u https://www.tripadvisor.com/Search?q=hellotext123
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
 state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by th

[*] starting @ 05:01:33 /2024-05-01/

[05:01:35] [INFO] testing connection to the target URL
[05:01:36] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of
you have not declared cookie(s), while server wants to set its own ('datadome=SAVKJteVonM...c59cPG~d5T;TAUnique=%1%en
Y/n] y
[05:01:41] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:01:44] [INFO] testing if the target URL content is stable
[05:01:45] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on
 parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
```

```
[05:02:53] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[05:02:53] [CRITICAL] considerable lagging has been detected in connection response
[05:02:57] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[05:03:15] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comm
[05:03:20] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[05:03:27] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[05:03:34] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[05:03:57] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one ot
] y
[05:04:09] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[05:04:19] [WARNING] GET parameter 'q' does not seem to be injectable
[05:04:19] [CRITICAL] all tested parameters do not appear to be injectable. Try to
ou can give it a go with the switch '--text-only' if the target page has a low perc
ere is some kind of protection mechanism involved (e.g. WAF) maybe you could try to
t'
[05:04:19] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 92 times
[05:04:19] [WARNING] your sqlmap version is outdated
```

There is no injection vulnerability in the above web application.

Wapplyzer

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



These are the technologies used.

Nslookup

```
┌──(kali㉿kali)-[~]
└─$ nslookup tripadvisor.com
Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
Name:   tripadvisor.com
Address: 151.101.66.28
Name:   tripadvisor.com
Address: 151.101.130.28
Name:   tripadvisor.com
Address: 151.101.194.28
Name:   tripadvisor.com
Address: 151.101.2.28
```

The ip address of the web application is found.

Recon ng

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

```
[1] Recon modules

[recon-ng][default] > workspaces create bb1
[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|pr

[recon-ng][bb1][hackertarget] > options set SOURCE tripadvisor.com
SOURCE => tripadvisor.com
[recon-ng][bb1][hackertarget] > run

TRIPADVISOR.COM
[*] Country: None
[*] Host: tripadvisor.com
[*] Ip_Address: 151.101.130.28
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] Country: None
[*] Host: hipchat01.drt01.corp.tripadvisor.com
[*] Ip_Address: 192.170.137.44
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: hipchat02.drt01.corp.tripadvisor.com
[*] Ip_Address: 192.170.137.43
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: jg01.drt01.corp.tripadvisor.com
[*] Ip_Address: 192.170.137.42
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: jg03.drt01.corp.tripadvisor.com
[*] Ip_Address: 192.170.137.42
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
SUMMARY
[*] 73 total (73 new) hosts found.
[recon-ng][bb1][hackertarget] >
```

73 total subdomains found.

Dotdotpwn

Dotdotpwn is a directory traversal checker.

```
[========== TARGET INFORMATION ==========]
[+] Hostname: tripadvisor.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 sufixes
[+] 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: 403 | Testing Path: http://tripadvisor.com:80/../etc/passwd
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/../etc/issue
```

```
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5cetc%5cissue
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5cetc%5cissue
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5c..%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5c..%5cetc%5cissue
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5c..%5c..%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5c..%5c..%5cetc%5cissue
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5c..%5c..%5c..%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5c..%5c..%5c..%5c..%5cetc%5cissue
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5c..%5c..%5c..%5c..%5cetc%5cpasswd
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%5c..%5c..%5c..%5c..%5c..%5cetc%5cissue
```

```
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%25c0%25a
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%25c0%25a
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%25c0%25a
[*] HTTP Status: 403 | Testing Path: http://tripadvisor.com:80/..%25c0%25a

[+] Fuzz testing finished after 8.82 minutes (529 seconds)
[+] Total Traversals found (so far): 0
[-] Web server (tripadvisor.com) didn't respond !
```

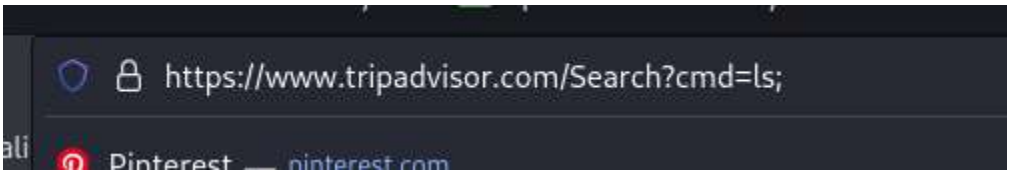
The scan results returned status codes within the range 400 (400-499). It shows a client error.

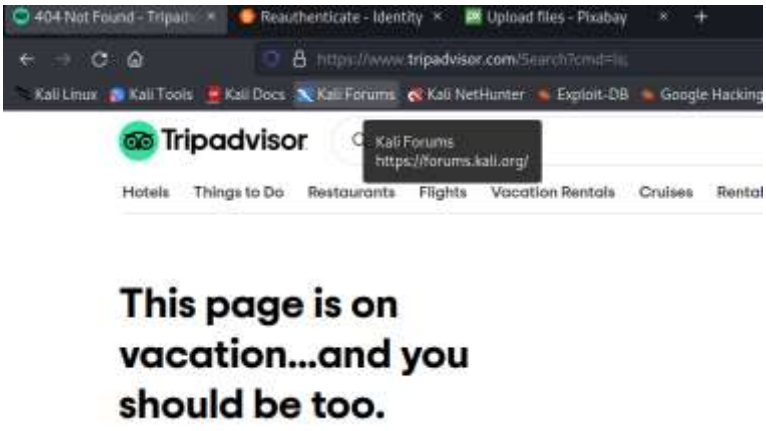
Therefore, we can conclude that the tested destinations are not vulnerable to a directory traversal.

Command injection

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

The “ls” command is appended to the url.

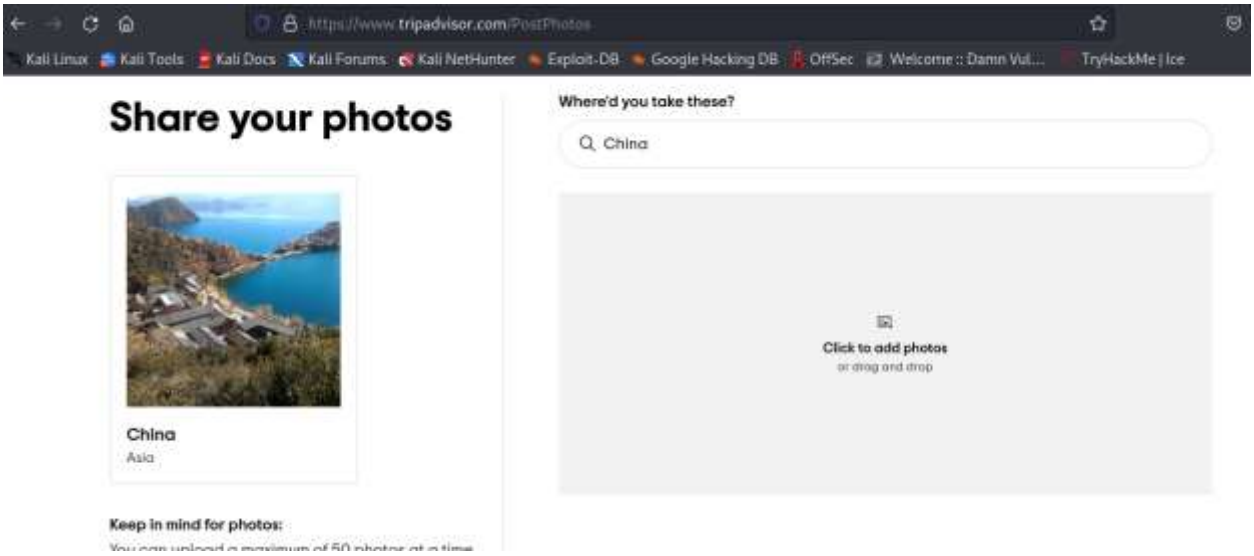




No command injection vulnerability can be found.

File upload vulnerability

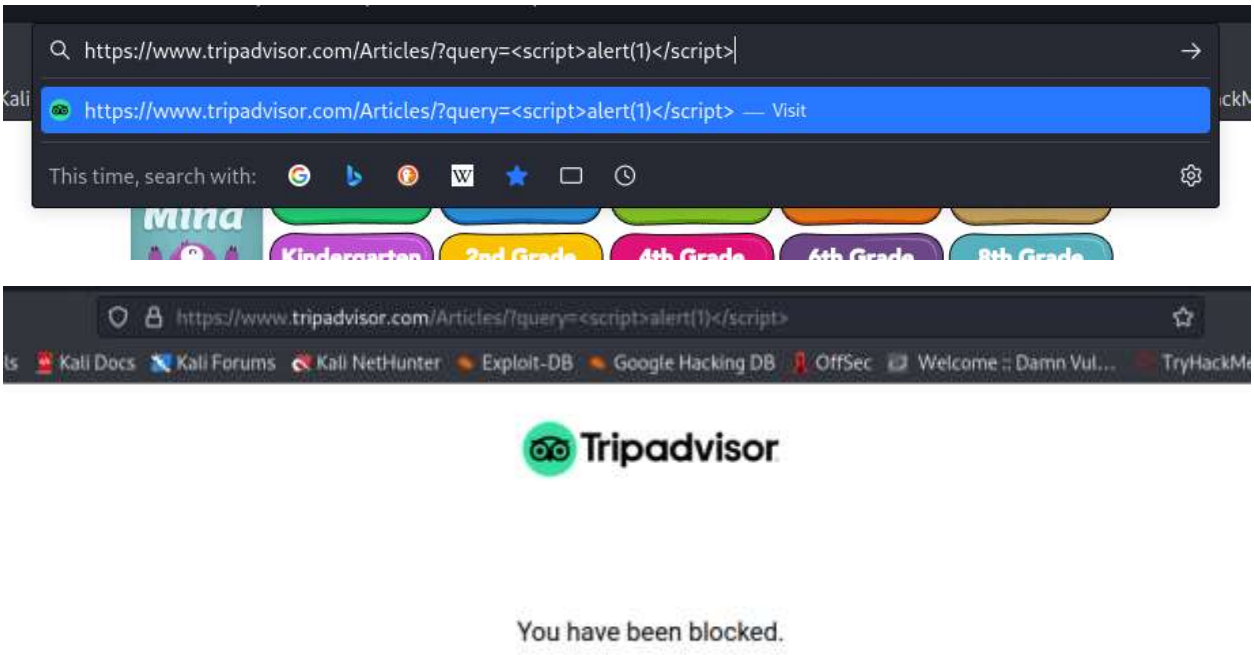
If a .php file can be uploaded from the file uploading facility, there is a possibility to upload and execute a reverse shell php code.



No vulnerability found.

XSS injection

A payload is apended to the url to test against xss injection.



It’s not vulnerable to XSS injection.