

Sri Lanka Institute of Information Technology



BUG BOUNTY REPORT - 9

Web Security – IE2062

IT22362780

Jayaweera N.S

Report Details

Report # - 09

Domain - <https://pixabay.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
File upload vulnerability testing
Command injection
XSS injection
Nslookup scan

Nmap scan

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

```
(kali@kali)-[~]
$ sudo nmap -sS -T4 pixabay.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 12:30 EDT
Nmap scan report for pixabay.com (104.18.40.96)
Host is up (0.011s latency).
Other addresses for pixabay.com (not scanned): 172.64.147.160 2606:4700:4400::ac40:93a0 2606:4700:4400::6812:2860
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 5.64 seconds
```

No unusual ports are open.

But Smtplib 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 pixabay.com --script=smtp* -p 25
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-01 12:32 EDT
Nmap scan report for pixabay.com (172.64.147.160)
Host is up (0.033s latency).
Other addresses for pixabay.com (not scanned): 104.18.40.96 2606:4700:4400::6812:2860 2606:4700:4400::ac40:93a0

PORT      STATE SERVICE
25/tcp    open  smtp
|_ smtp-enum-users:
|_   SMTP EHLO pixabay.com: failed to receive data: connection closed
|_ smtp-open-relay: SMTP EHLO nmap.scanme.org: failed to receive data: connection closed
|_ smtp-vuln-cve2010-4344:
|_   The SMTP server is not Exim: NOT VULNERABLE
|_ smtp-commands: Couldn't establish connection on port 25

Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
```

Connection cannot be established therefore a vulnerability cannot be identified.

Recon-ng

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

```
[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|passwords|urls|users|vulnerabilities>

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

-----
PIXABAY.COM
-----

[*] Country: None
[*] Host: cdn.pixabay.com
[*] Ip_Address: 172.64.147.160
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] Notes: None
[*] Region: None
-----
[*] Country: None
[*] Host: o2736.e.community.pixabay.com
[*] Ip_Address: 167.89.100.231
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
-----
[*] Country: None
[*] Host: link.pixabay.com
[*] Ip_Address: 172.64.147.160
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
-----
[*] Country: None
[*] Host: safesearch.pixabay.com
[*] Ip_Address: 104.18.40.96
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
-----
[*] Country: None
[*] Host: www.pixabay.com
[*] Ip_Address: 172.64.147.160
[*] Latitude: None
[*] Longitude: None
```

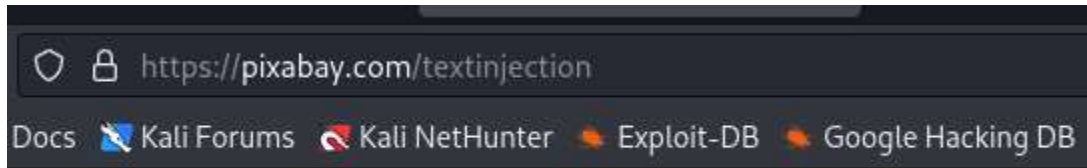
SUMMARY

```
[*] 5 total (5 new) hosts found.
[recon-ng][bb1][hackertarget] > █
```

5 total subdomains found.

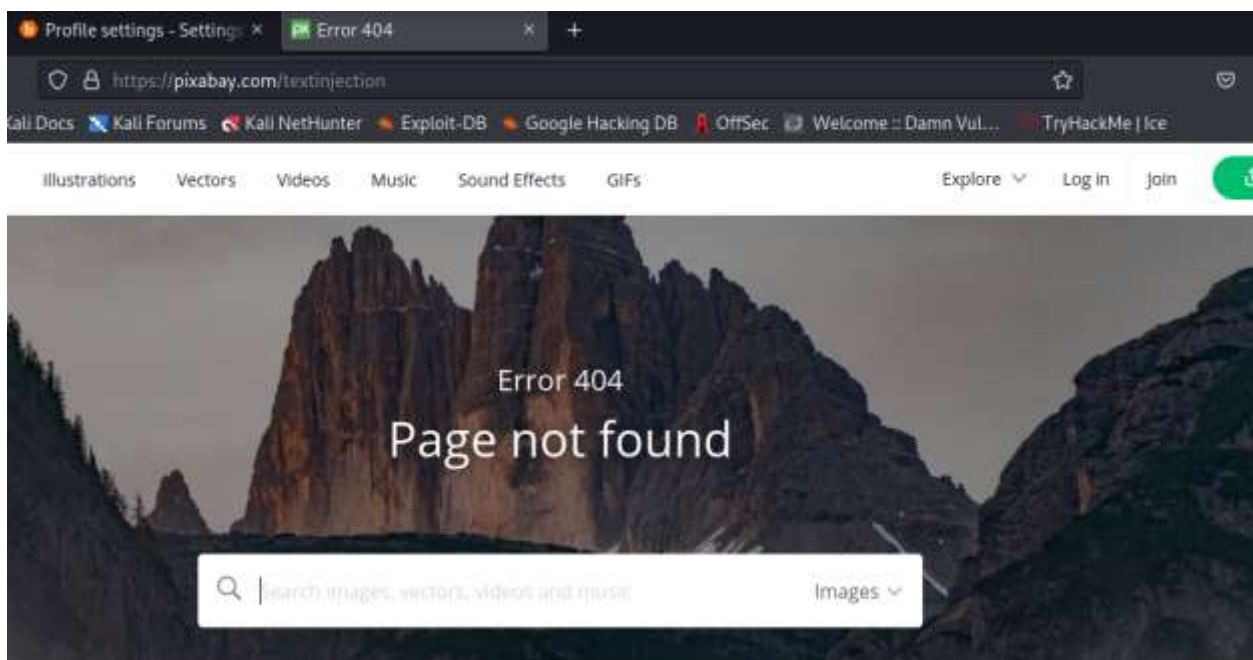
Text injection

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.

Sqlmap

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

```
(kali@kali)-[~]
$ sqlmap -u https://pixabay.com/images/search/?q=hello1234

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
state and federal laws. Developers assume no liability and are not responsible for any misuse or
abuse.

[*] starting @ 13:00:49 /2024-05-01/

[13:00:52] [INFO] testing connection to the target URL
[13:00:53] [WARNING] potential permission problems detected ('Access denied')
[13:00:53] [WARNING] the web server responded with an HTTP error code (403) which could interfere
you have not declared cookie(s), while server wants to set its own ('__cf_bm=BpNyYj2bmP_...5Xc.2
[13:01:01] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:01:01] [CRITICAL] WAF/IPS identified as 'CloudFlare'
[13:01:01] [INFO] testing if the target URL content is stable

It is recommended to perform only basic UNION tests if there is not at least one other (
y
[13:01:26] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:01:28] [WARNING] GET parameter 'q' does not seem to be injectable
[13:01:28] [CRITICAL] all tested parameters do not appear to be injectable. Try to incre
ease retry with the switch '--text-only' (along with --technique=BU) as this case looks
n engine to detect at least one dynamic parameter). If you suspect that there is some ki
n '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[13:01:28] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 83 times
[13:01:28] [WARNING] your sqlmap version is outdated

[*] ending @ 13:01:28 /2024-05-01/
```

There is no injection vulnerability in the above web application.

Nslookup

```
(kali@kali)-[~]  
$ nslookup pixabay.com  
Server:      192.168.8.1  
Address:     192.168.8.1#53  
  
Non-authoritative answer:  
Name:   pixabay.com  
Address: 104.18.40.96  
Name:   pixabay.com  
Address: 172.64.147.160  
Name:   pixabay.com  
Address: 2606:4700:4400::6812:2860  
Name:   pixabay.com  
Address: 2606:4700:4400::ac40:93a0
```

The ip address of the domain is found.

Wafw00f

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

```
(kali㉿kali)-[~]  
$ wafw00f https://pixabay.com
```



```
~ WAFW00F : v2.2.0 ~  
The Web Application Firewall Fingerprinting Toolkit  
[*] Checking https://pixabay.com  
[+] The site https://pixabay.com is behind Cloudflare (Cloudflare Inc.) WAF.  
[~] Number of requests: 2
```

The WAF used : Cloudflare

Dotdotpwn

Dotdotpwn is a directory traversal checker.

```
[+] Report name: Reports/pixabay.com_05-01-2024_11-03.txt

[===== TARGET INFORMATION =====]
[+] Hostname: pixabay.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 3.23 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)

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

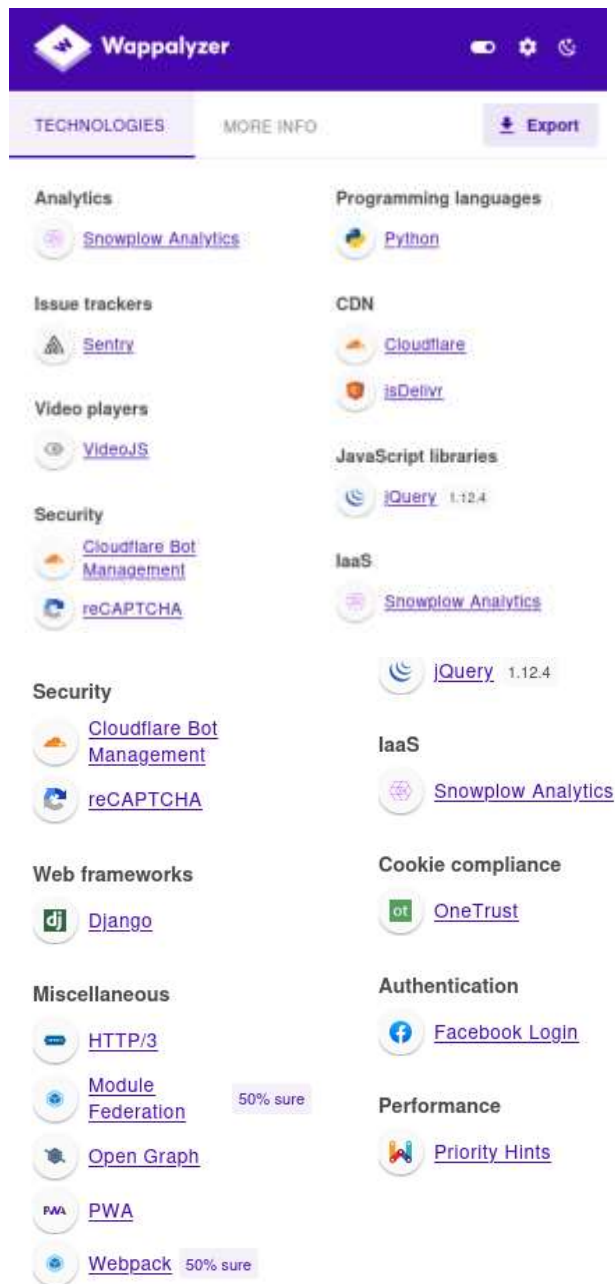
```
[*] HTTP Status: 400 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://pixabay.com:80/../../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://pixabay.com:80/../../../../etc/issue
[*] HTTP Status: 400 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 400 | Testing Path: http://pixabay.com:80/../../../../etc/issue
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/issue
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 403 | Testing Path: http://pixabay.com:80/../../../../etc/issue
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/issue
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/issue
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/issue
[*] HTTP Status: 403 | Testing Path: http://pixabay.com:80/../../../../etc/passwd
[*] HTTP Status: 404 | Testing Path: http://pixabay.com:80/../../../../etc/issue
```

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

Vulnerable paths were found.

Wapplyzer

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



These are the technologies used.

The jquery 1.12.4 used is vulnerable.



Cross-site Scripting (XSS)

<1.12.0

>=1.12.3 <3.0.0-beta1

`jquery` is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.

Affected versions of this package are vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain ajax request is performed without the `dataType` option causing `text/javascript` responses to be executed.

Note: After being implemented in version 1.12.0, the fix of this vulnerability was reverted in 1.12.3, and then was only reintroduced in version 3.0.0-beta1. The fix was never released in any tag of the 2.x.x branch, as it was reverted out of the branch before being released.

Note: CVE-2017-16012 is a duplicate of CVE-2015-9251

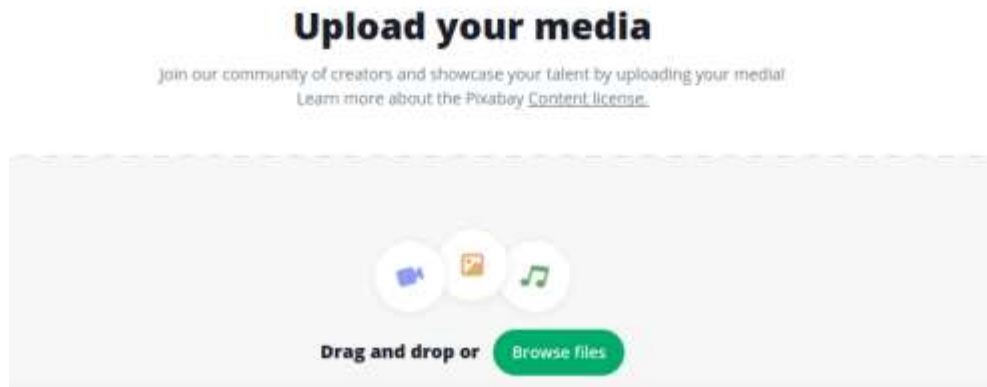
How to fix Cross-site Scripting (XSS)?

Upgrade `jquery` to version 1.12.0, 3.0.0-beta1 or higher.

In order to mitigate the risk, update the jquery scripts to 1.12.0, 3.0.0-beta1 or higher.

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.

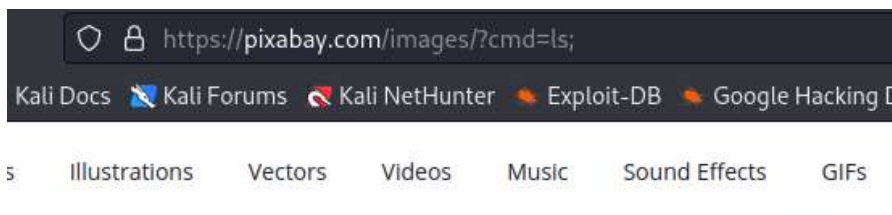
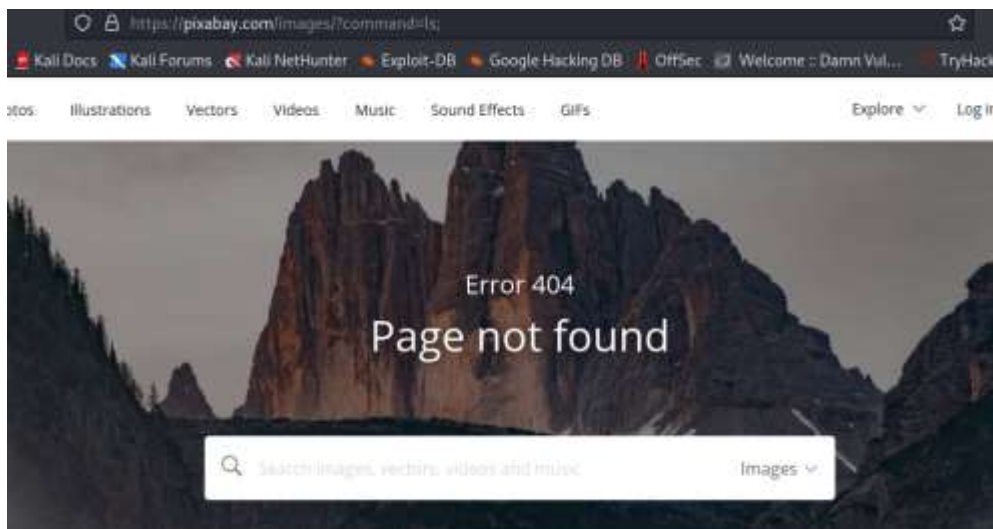
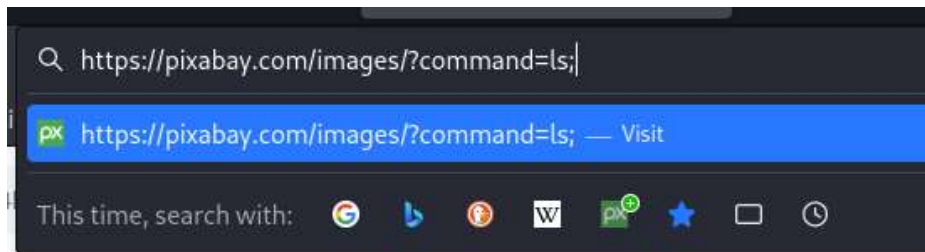


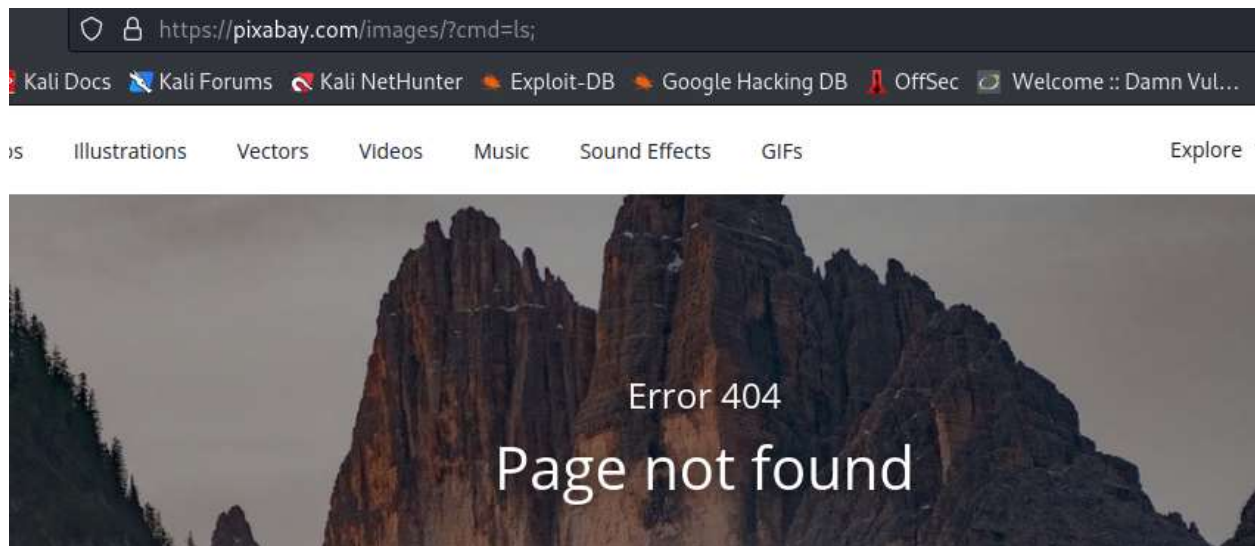
No vulnerability found.

Command injection

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

The “ls” command is appended to the url

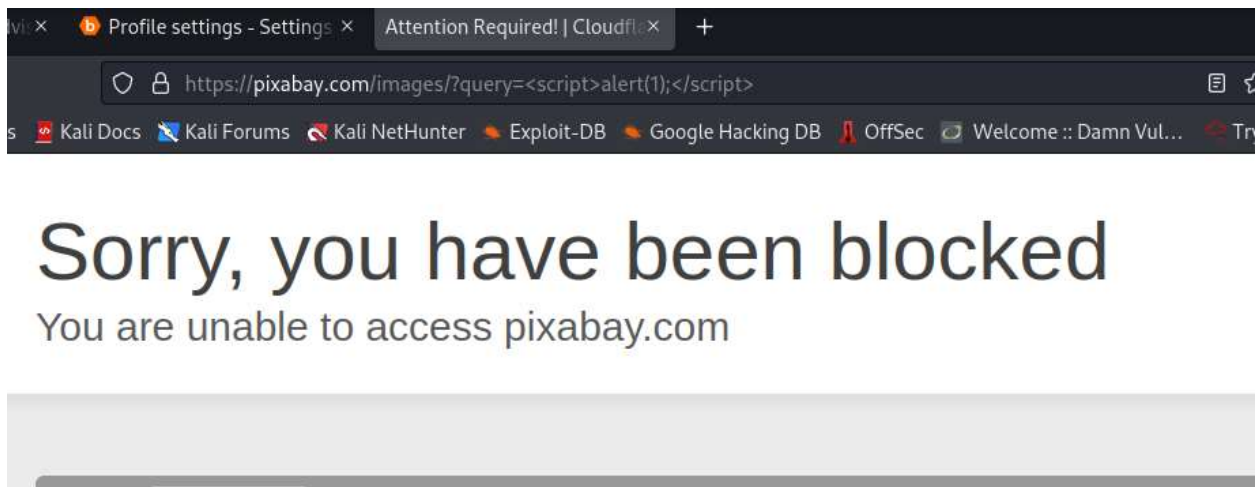
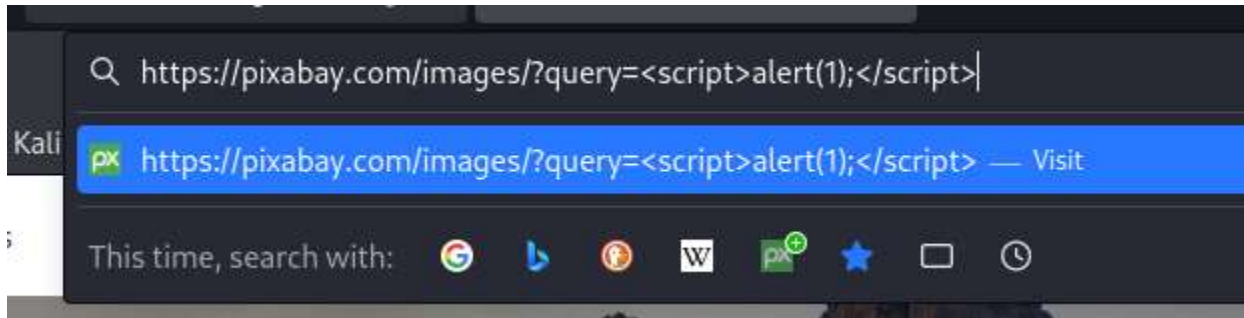




No command injection vulnerability can be found.

XSS injection

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



It's not vulnerable to XSS injection.