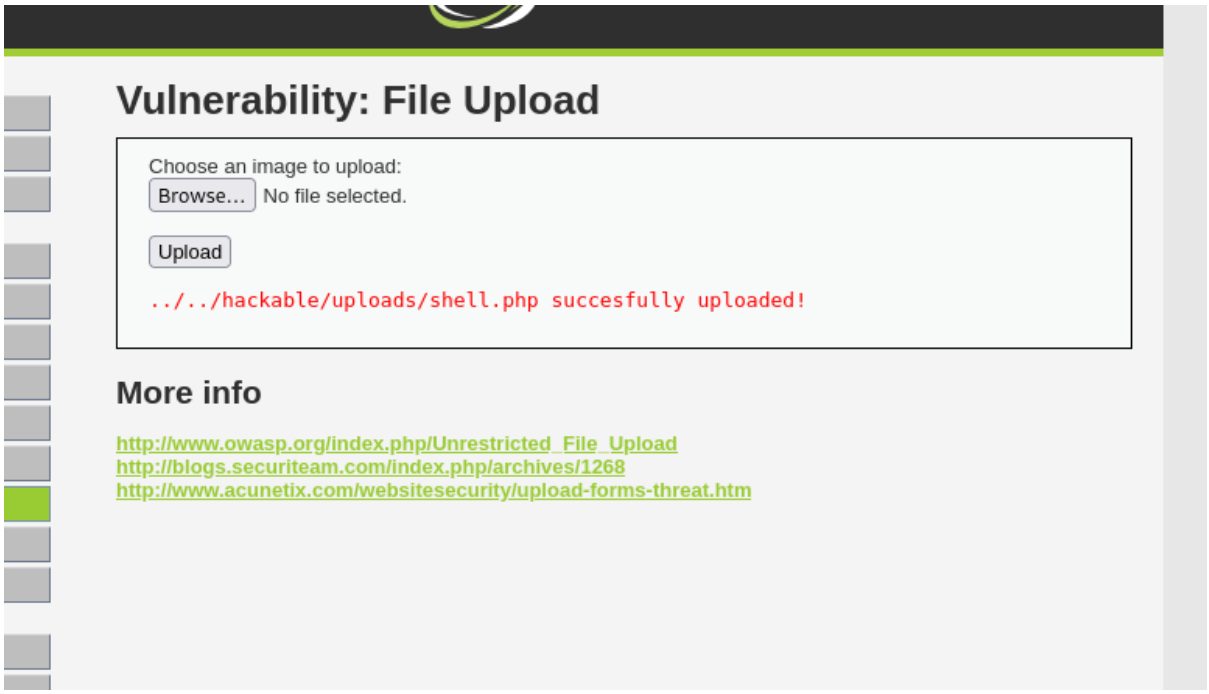
# S6/L1

L’esercizio di oggi consiste nello sfruttare una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP.

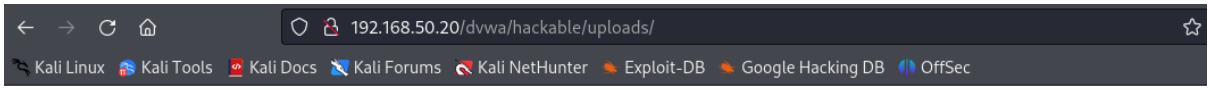
Come prima cosa dobbiamo avere sulla stessa rete interna Kali e metasploitable.

Dopo di che andiamo su internet da kali e scriviamo l’indirizzo ip di meta, dovremmo finire dentro la schermata di meta.


Dobbiamo andare su DVWA, accediamo con “admin” e “password” e mettiamo low come livello di sicurezza andando su DVWA security.




Dobbiamo caricare il file della shell dalla sezione Upload.

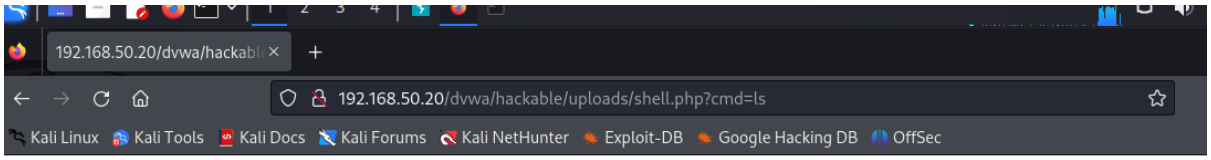



# Index of /dvwa/hackable/uploads

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| dvwa_email.png | 16-Mar-2010 01:56 | 667 | |
| shell.php | 13-Jan-2025 09:39 | 35 | |

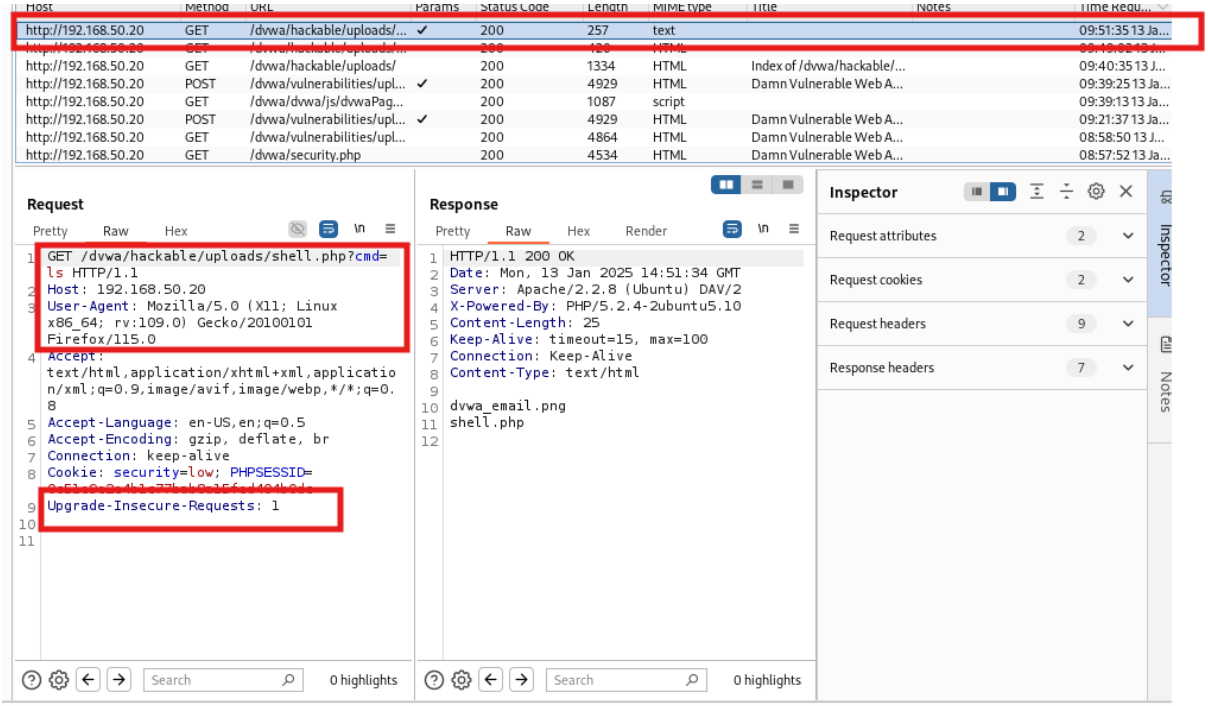
*Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.20 Port 80*

Una volta che abbiamo caricato il file con successo dobbiamo andare nel percorso che ci è uscito dopo il caricamento e ci ritroveremo in questa schermata.




dvwa_email.png shell.php

Se schiacciamo su shell.php ci uscirà questa scritta che indica semplicemente il file che abbiamo caricato.




Come possiamo notare da burpsuite tutte le richieste di GET vengono passate e il livello di sicurezza della richiesta e 1.

Notiamo quindi che questo attacco e andato a buon fine dato che siamo riusciti ad inserire la nostra shell, ovviamente inserendo una shell più forte avremmo la possibilità di avere altri verbi HTTP/HTTPS.