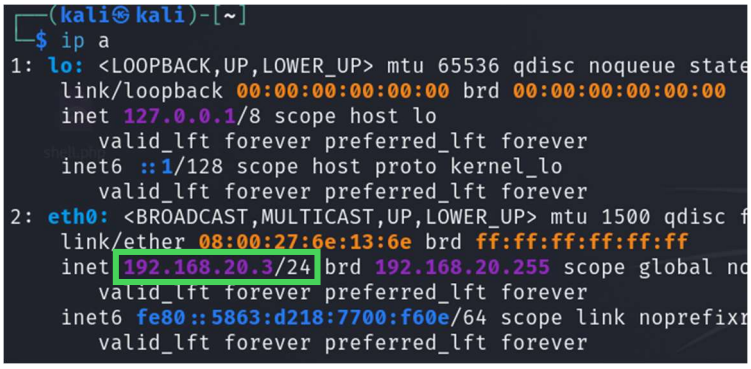
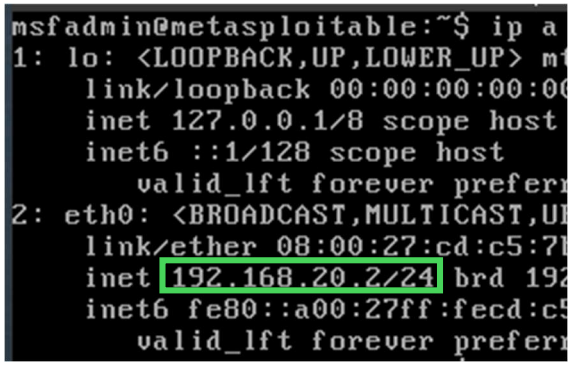
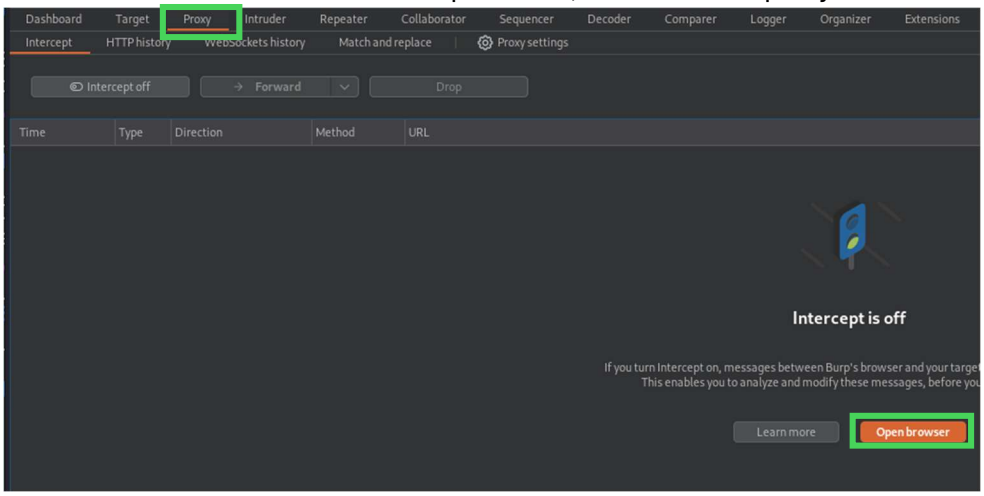
Innanzitutto, modifico gli IP delle due macchine e le impostazioni di VB in maniera tale che siano sotto la stessa rete interna:

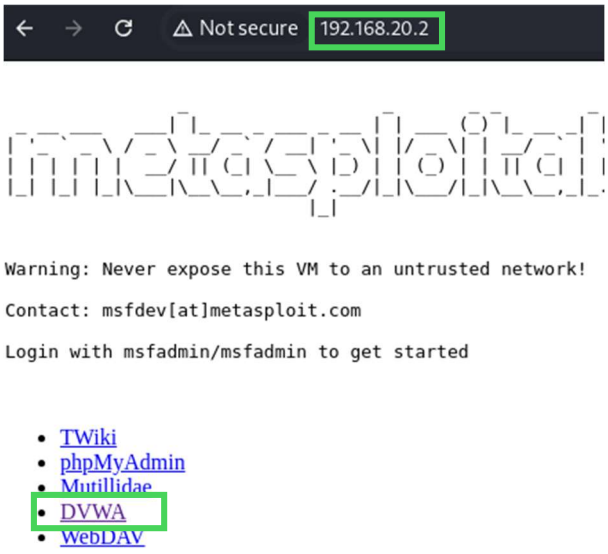


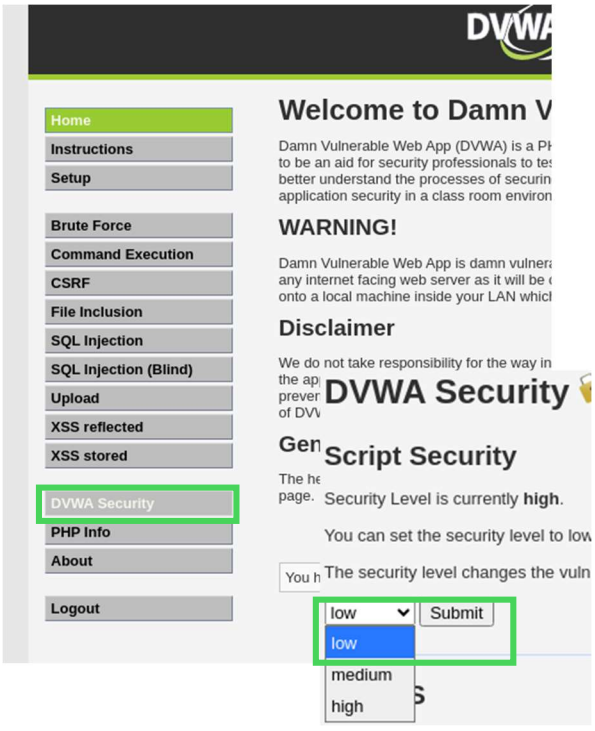


Adesso che entrambe le macchine sono sotto la stessa rete posso aprire il browser per poter modificare le impostazioni di DVWA, scelgo di usare direttamente il browser di burpsuite dato che viene richiesta l'intercettazione dei pacchetti, cliccando su "proxy" nel menu in alto e "open browser"



Ora inserisco l'indirizzo IP di metasploitable per andare nella pagina di DVWA, faccio l'accesso inserendo come credenziali "admin" e "password" e clicco su DVWA security per impostare la sicurezza a "low":

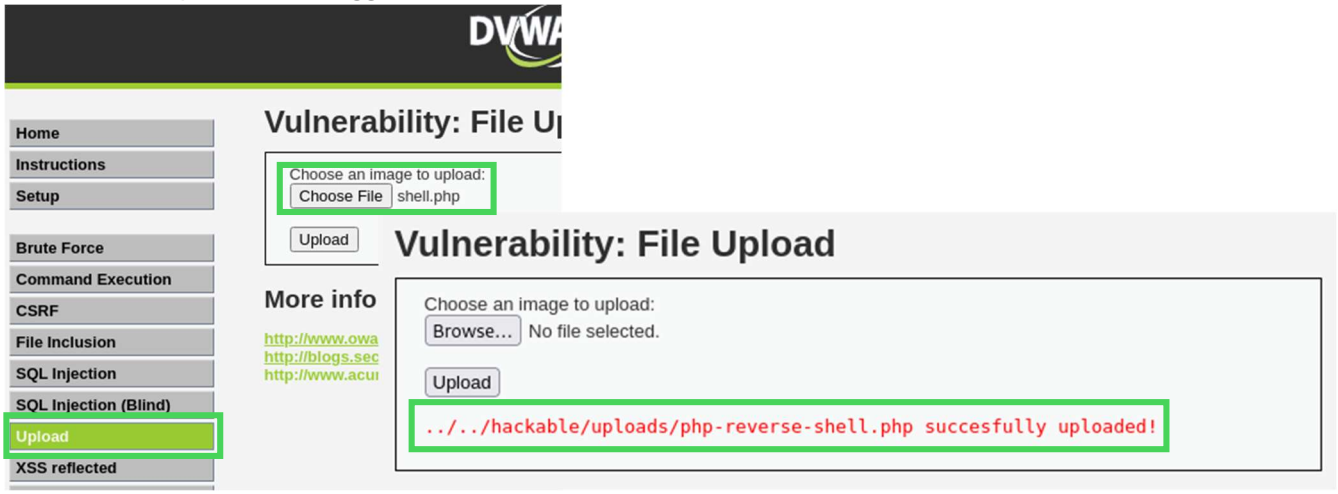




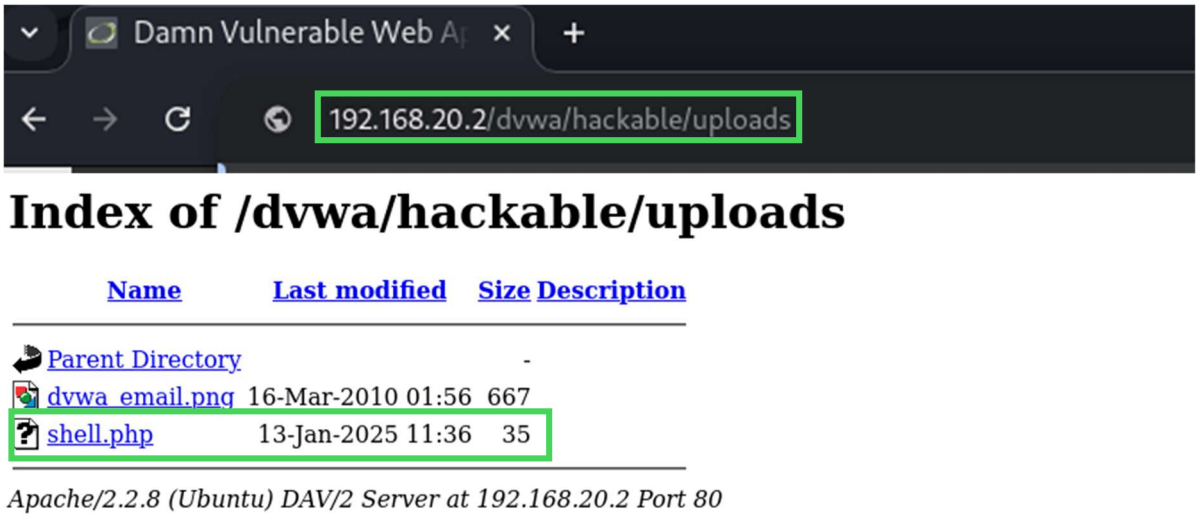
Creo un file chiamato “shell.php” contenente questa stringa:

Che servirà a eseguire comandi sul nostro sito.

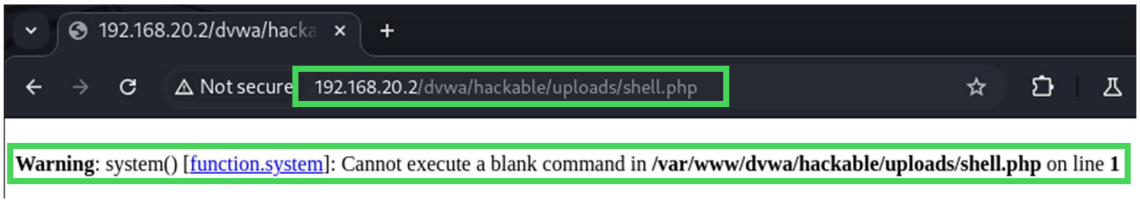
Adesso, per caricare il file shell.php. dentro a DVWA, devo andare nella sezione “Upload” e selezionarlo.
Avremo in output un messaggio rosso che indica che il file è stato caricato con successo:

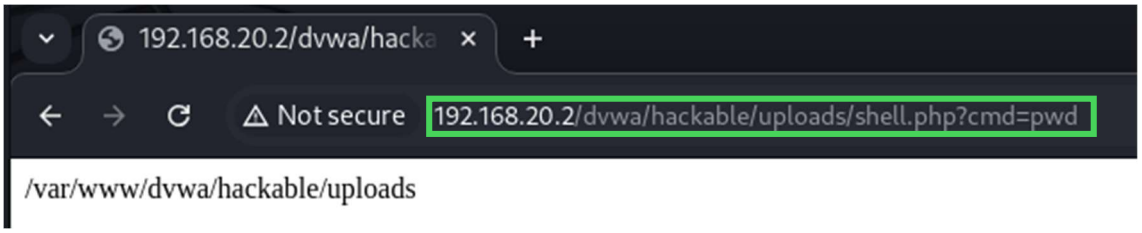


Successivamente, seguendo da browser il percorso che viene scritto nel output rosso, arriveremo in una pagina dove sarà presente il file appena caricato



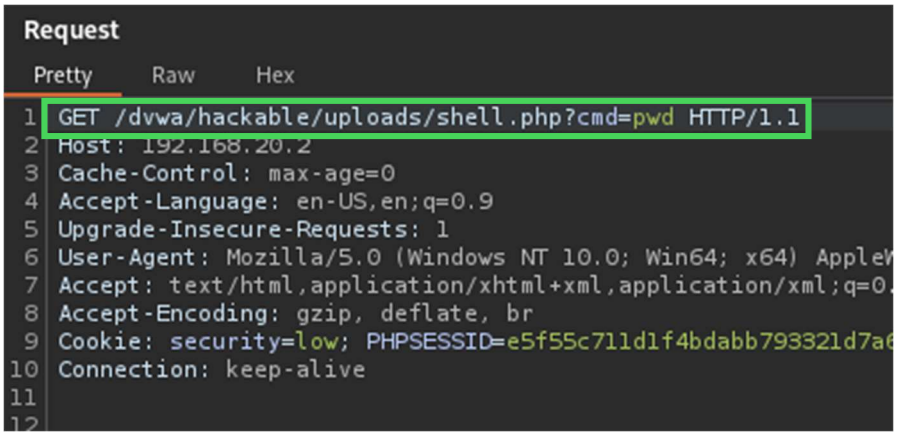
Adesso clicco sul file e deve comparire un messaggio di errore a schermo perché devo aggiungere alla fine del path del browser "?cmd=comandodaeseguire" che nel mio esempio ho eseguito il comando pwd per vedere il percorso attuale





E viene appunto eseguito il comando richiesto dando in output il percorso attuale.

Riprovo a ricaricare la pagina mentre attivo l'intercettazione di BurpSuite:



Vedendo che si tratta di una richiesta GET dato che è stata ricaricata la pagina, se avessi intercettato durante il caricamento del file, avrei letto che la richiesta sarebbe stata di tipo POST.