XSS (CROSS SITE SCRIPTING) - ESERCIZIO

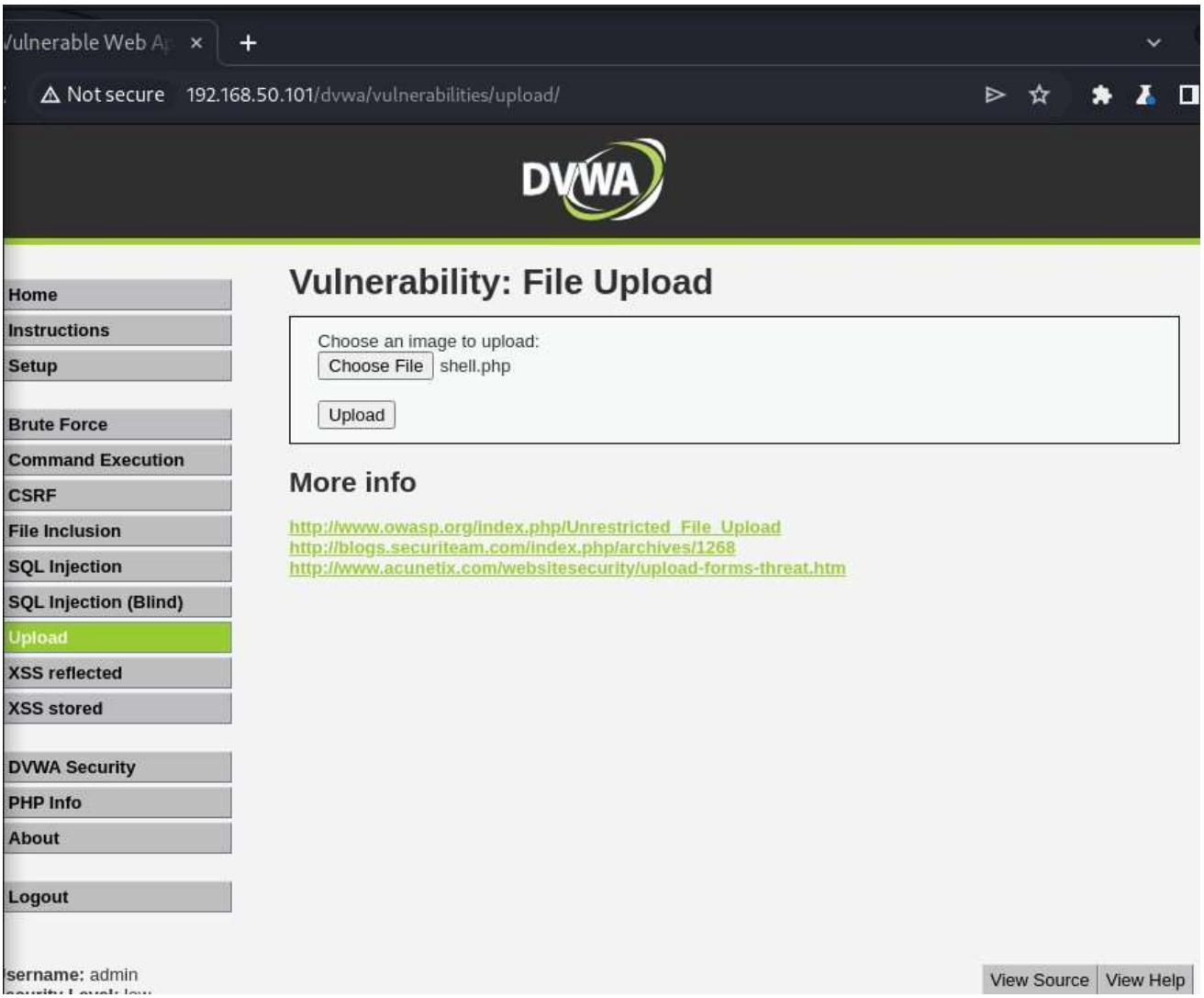
Traccia:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine. Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

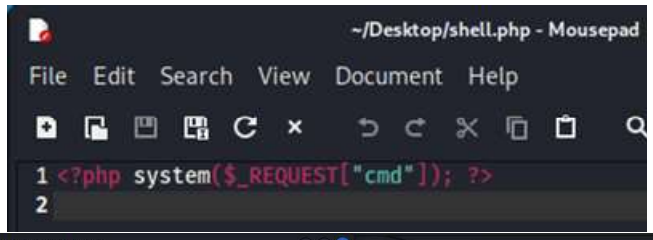
Esecuzione:

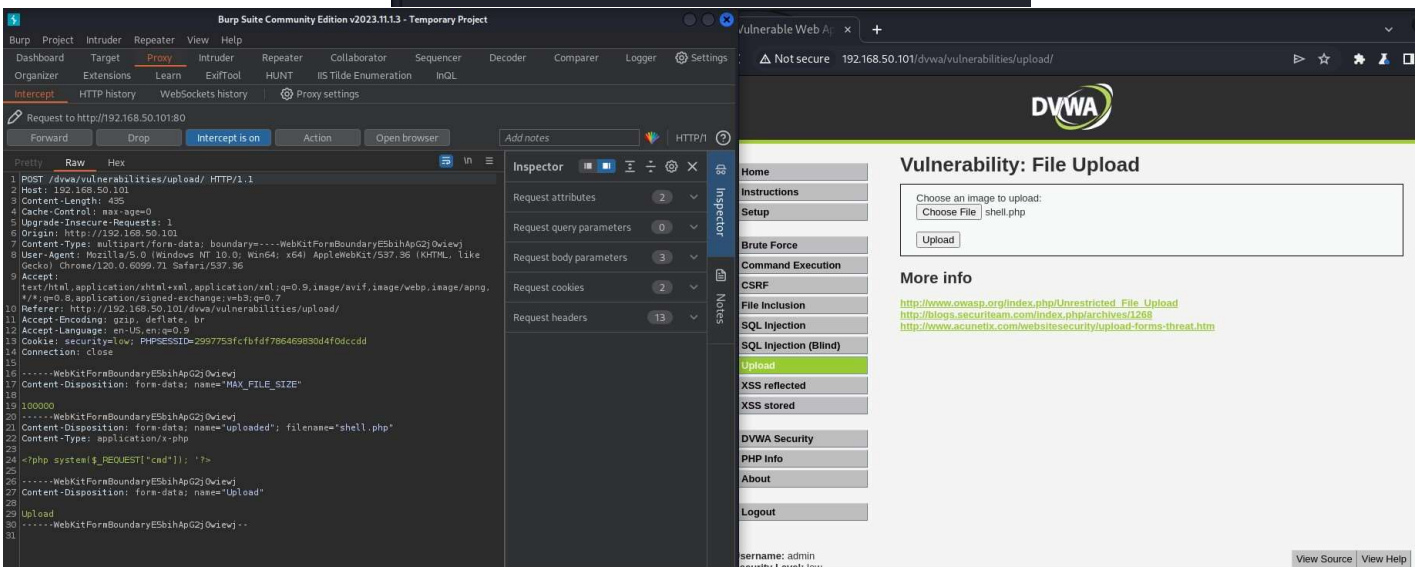
Accedo alla pagina web DVWA presente in Metasploitable 2 con indirizzo IP 192.168.51.11

Abbasso il livello di sicurezza in "LOW" ed entro nella sezione di "Upload" della Web App.



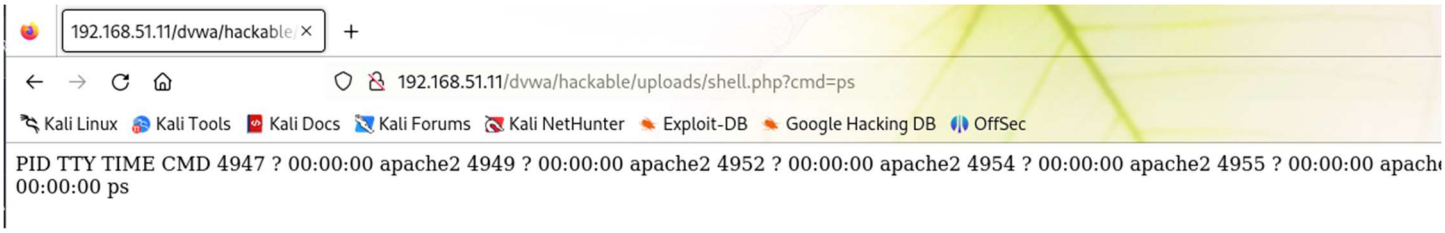
Carico il seguente file “shell.php” contenente il seguente codice.





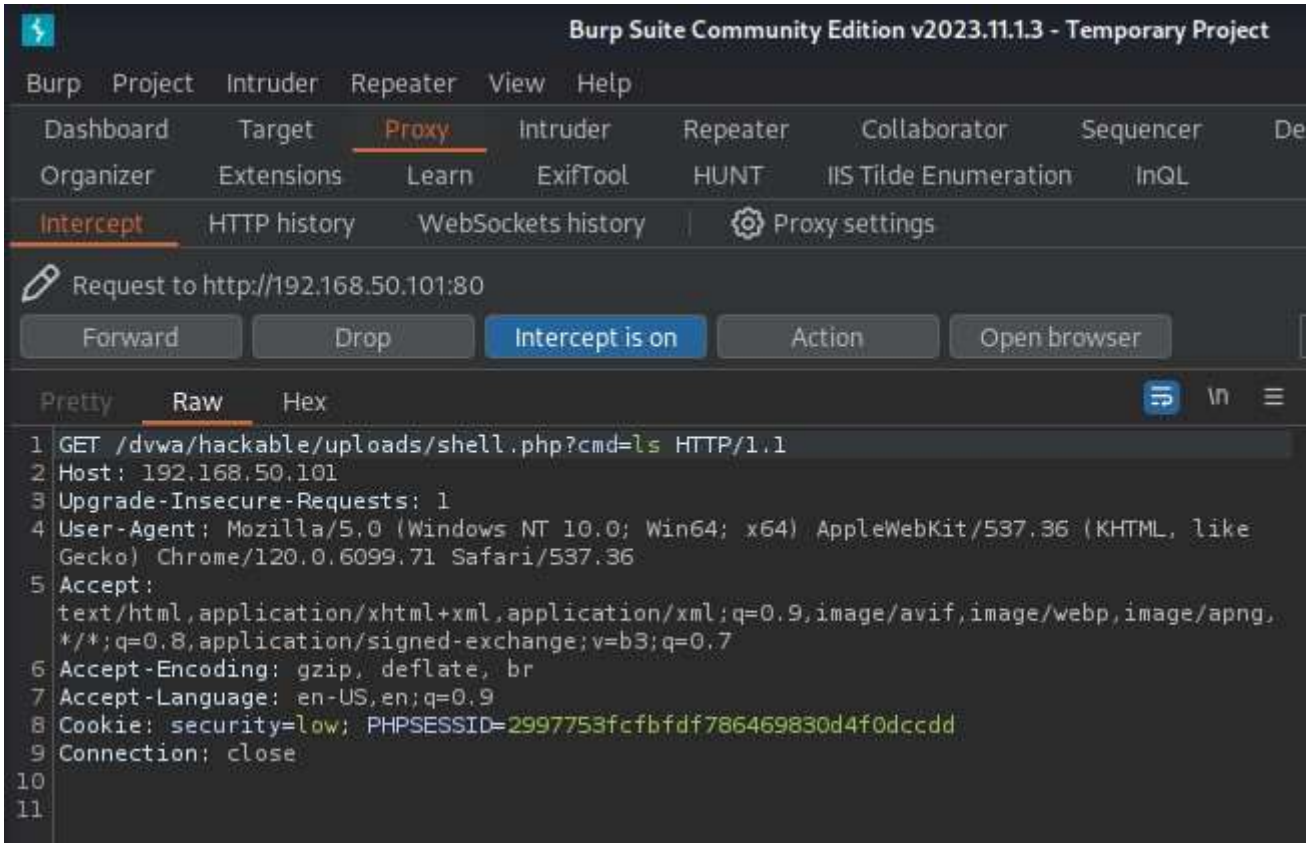
Come si può notare, la Web App non esegue un controllo sul file che viene caricato.

Il percorso che viene visualizzato ci permette di accedere al file da noi caricato.



Inserendo alla fine dell’URL della pagina la seguente stringa “?cmd=ls” stiamo sfruttando il codice PHP caricato in precedenza e con il simbolo “?” stiamo dicendo di eseguirlo. “cmd=ps” sta a prendere il parametro presente nel sorgente PHP e con “=” assegniamo il comando per la sua esecuzione. Di fatto il risultato è quello che ne uscirebbe se il comando fosse eseguito da Shell Linux.

Se catturiamo il pacchetto con Burspuite, possiamo anche verificare che come il comando viene passato durante la richiesta da parte del Client. Inoltre è anche possibile modificare il comando che si sta cercando di passare. Nell'esempio cambio il comando "ps" con "ls".



Di fatto il risultato non sarà più quello che darebbe il comando "ps" ma bensì quello di "ls" che restituisce l'elenco dei file presenti nella cartella in cui è stato salvato il file **shell.php.**