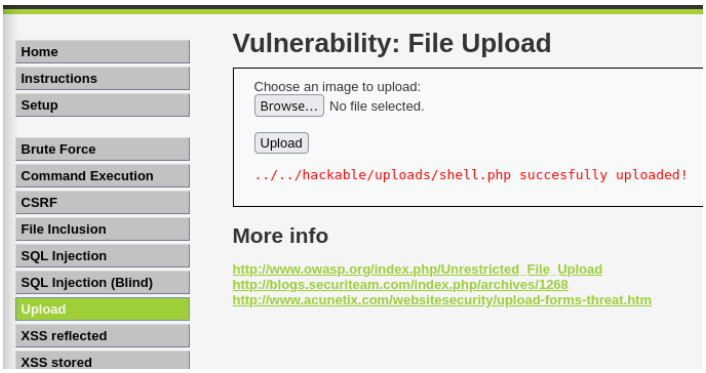
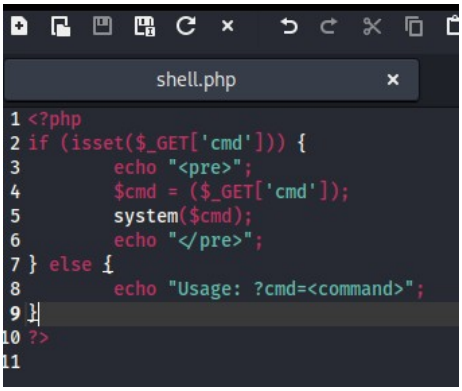
In questo esercizio andrò a sfruttare una vulnerabilità nella piattaforma DVWA (Damn Vulnerable Web Application) relativo all'upload di file per ottenere il controllo remoto della macchina Metasploitable utilizzando un file PHP (shell.php).
Attraverso Burpsuite, intercetto e analizzo il traffico HTTP.

Prima di iniziare configurate il «security level» della DVWA a «LOW» dalla scheda DVWA Security.

Carico il file shell.php nella sezione Upload di DVWA



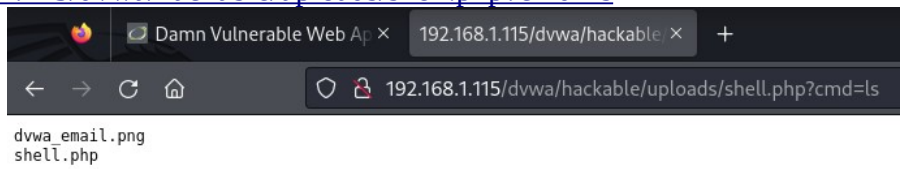
Questo script permette permette di eseguire il comando specificando tramite il parametro cmd nel'URL.



Questo link permette di visualizzare la cartella uploads di DVWA per verificare che il file PHP è stato caricato correttamente

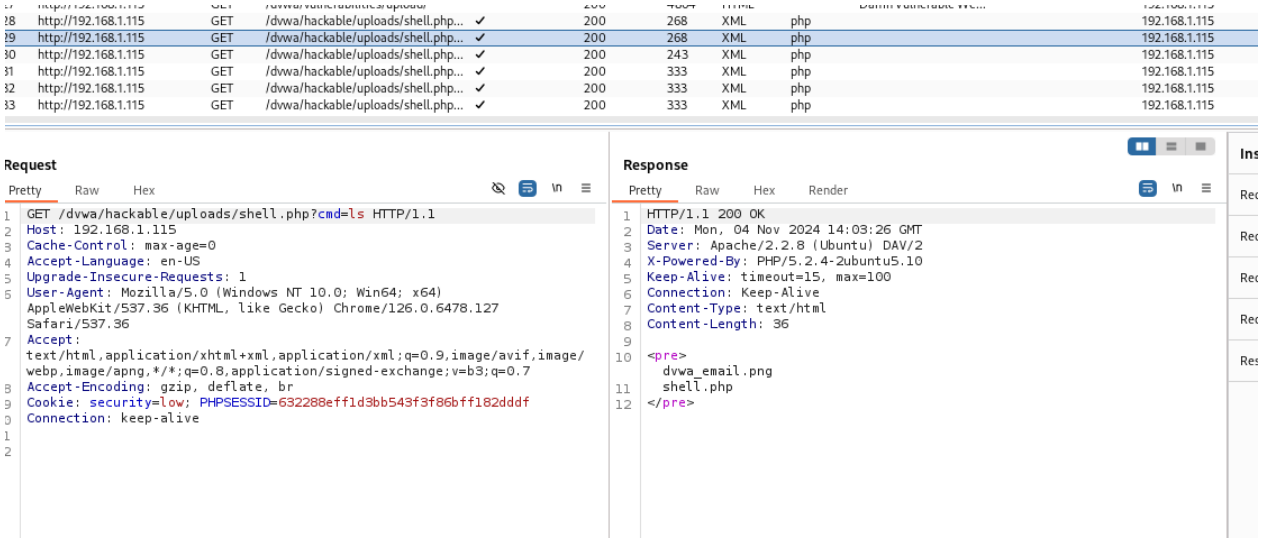
http://192.168.1.115/dvwa/hackable/uploads/

Ho intercettato e analizzato il traffico HTTP e l'esecuzione dei comandi remoti con BurpSuite.
http://192.168.1.115/dvwa/hackable/uploads/shell.php?cmd=ls

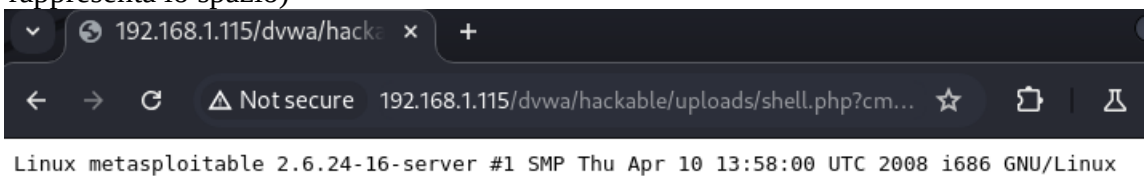


Con questo comando siamo in grado di visualizzare i file contenuti all'interno della cartella di DVWA come se fossimo da terminale.

Da Burpsuite questo viene intercettato e siamo in grado di muoverci a nostro piacimento.

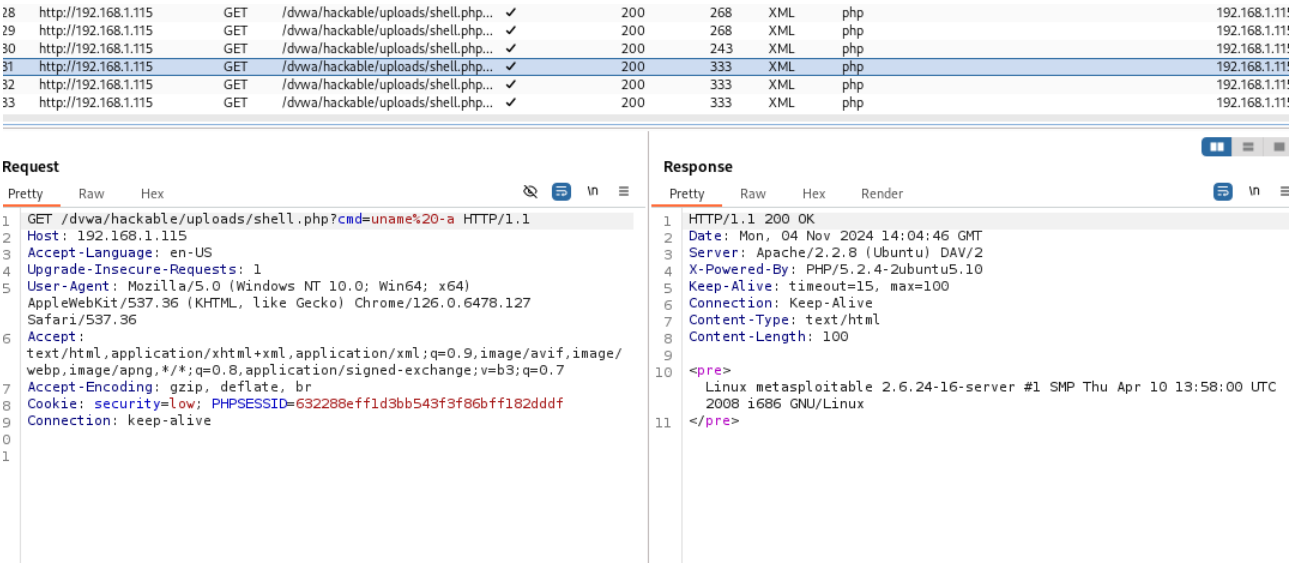


http://192.168.1.115/dvwa/hackable/uploads/shell.php?cmd=uname%20-a
(%20 rappresenta lo spazio)

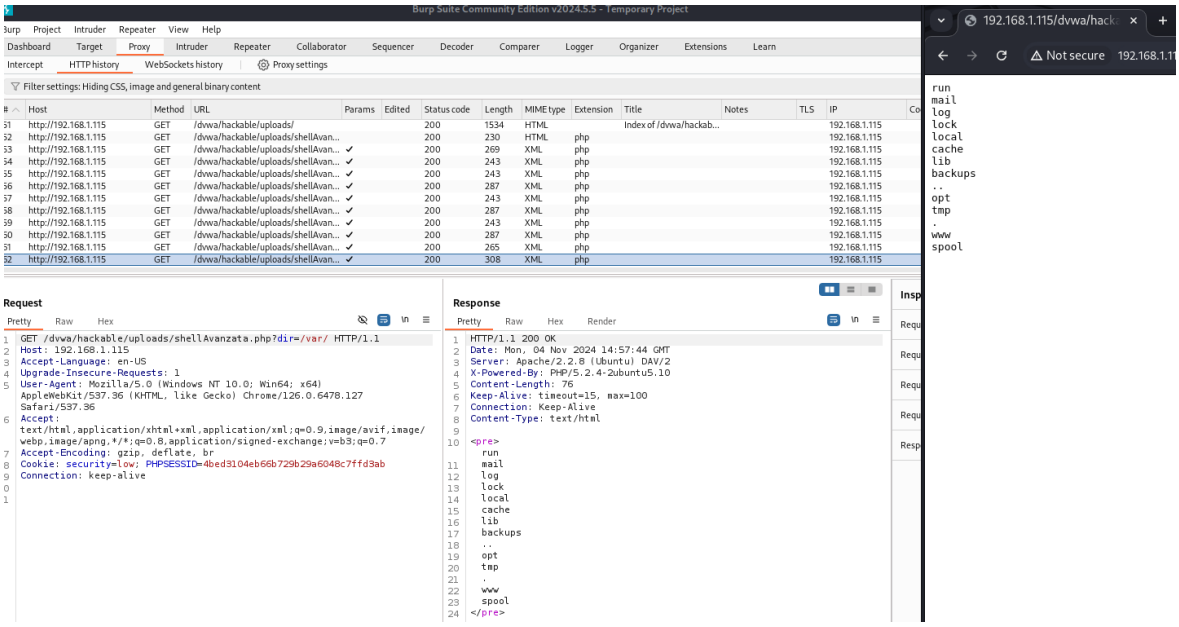


con questo comando siamo in grado di vedere le specifiche del sistema operativo.

Da Burpsuite intercettiamo la GET del comando appena mandato.



Ho chiesto a chatGTP di svilupparmi una shell avanzata PHP per il bonus di questo esercizio.
Una volta eseguito l'upload del file (che si trova in allegato nella cartella di questo esercizio), questa shell permette di:
Supportare la visualizzazione del contenuto di una directory specifica, utilizzando il parametro dir.
Questo mostra tutti i file e le cartelle presenti nel path specificato
http://192.168.1.115/dvwa/hackable/uploads/shellAvanzata.php?dir=/var/www/html



Scaricare File dalla Macchina Bersaglio.

La shell consente di scaricare file dalla macchina Metasploitable usando il parametro download.
Per scaricare un file chiamato dvwa_email.png dalla directory /var/www/dvwa/hackable/uploads, uso:
http://192.168.1.115/dvwa/hackable/uploads/shellAvanzata.php?download=/var/www/dvwa/hackable/uploads/dvwa_email.png

Il browser dovrebbe avviare automaticamente il download del file. Questa funzionalità è utile per ottenere copie di file sensibili dalla macchina bersaglio.