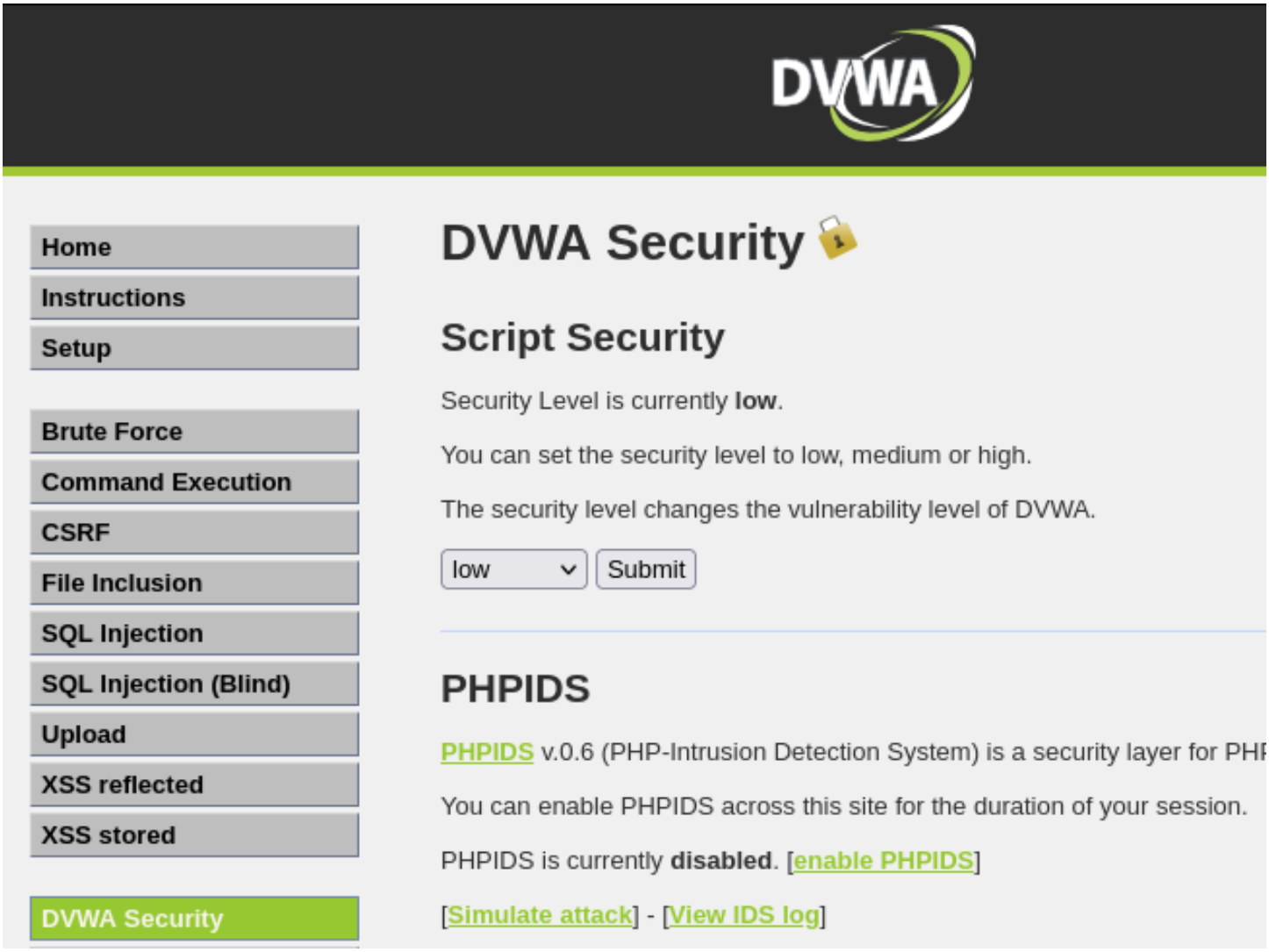
S6L1 Exploit File upload

Introduzione:

In questo esercizio, sono andato a sfruttare una vulnerabilità di upload di file presente nella **DVWA**. Con l'obiettivo di ottenere il controllo remoto, ed intercettare il traffico web grazie a **BurpSuite.**

Preparazione:

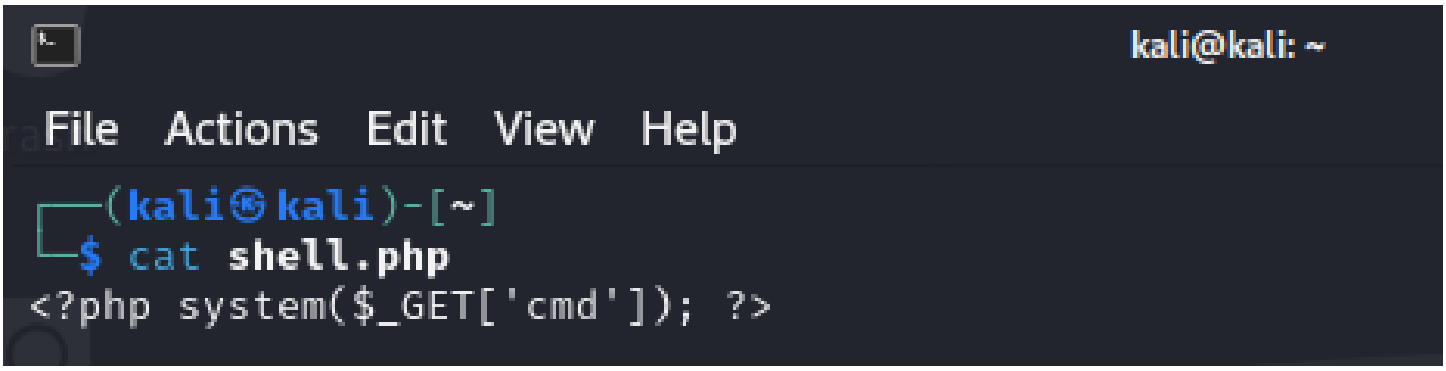
Attraverso Firefox in Kali Linux, ho effettuato l'accesso alla DVWA di Metasploitable, grazie all'indirizzo IP della macchina. Una volta fatto l'accesso sono andato ad impostare il livello di sicurezza di della DVWA al **livello low**.



Ora che ho abbassato i livelli, posso caricare il file **php**, e sono andato sul prompt di Kali, e digitando:

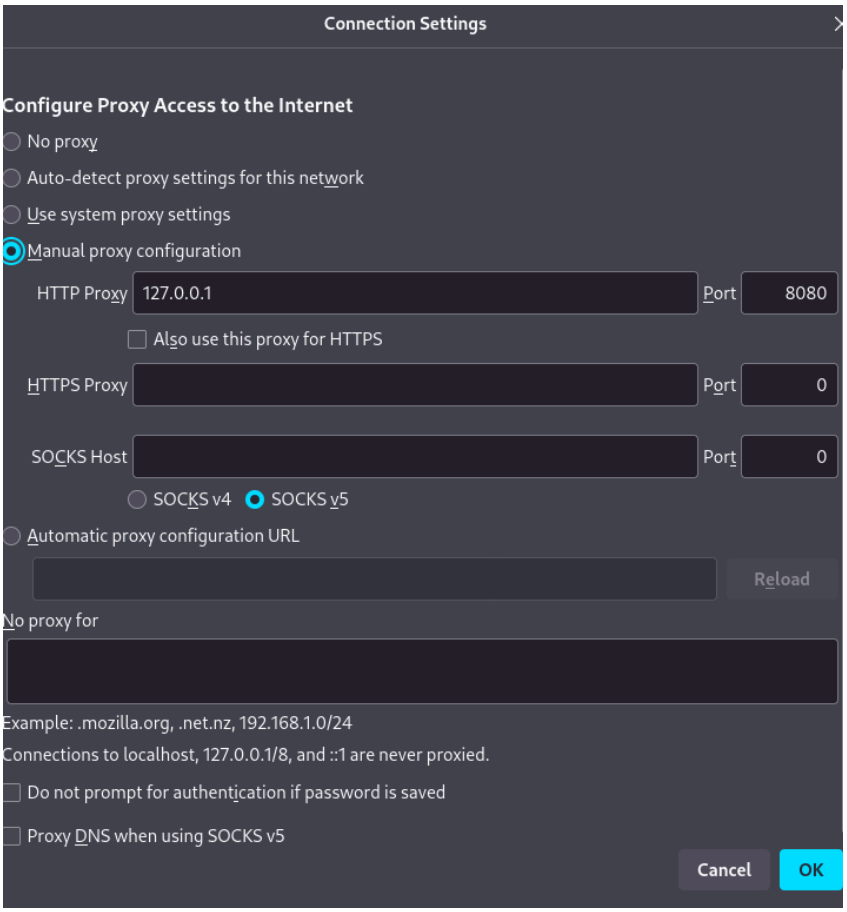
nano shell.php

Ho inserito all'interno questo codice:



E successivamente lo importato nella DVWA:

Successivamente per utilizzare **BurpSuite**, l'ho dovuto impostare come **proxy**, andando nell'impostazione del motore di ricerca:



Cosi da fargli intercettare tutte le richieste all'interno di Firefox.

Pratica:

1) Richiesta:

Appena fatto l'accesso a

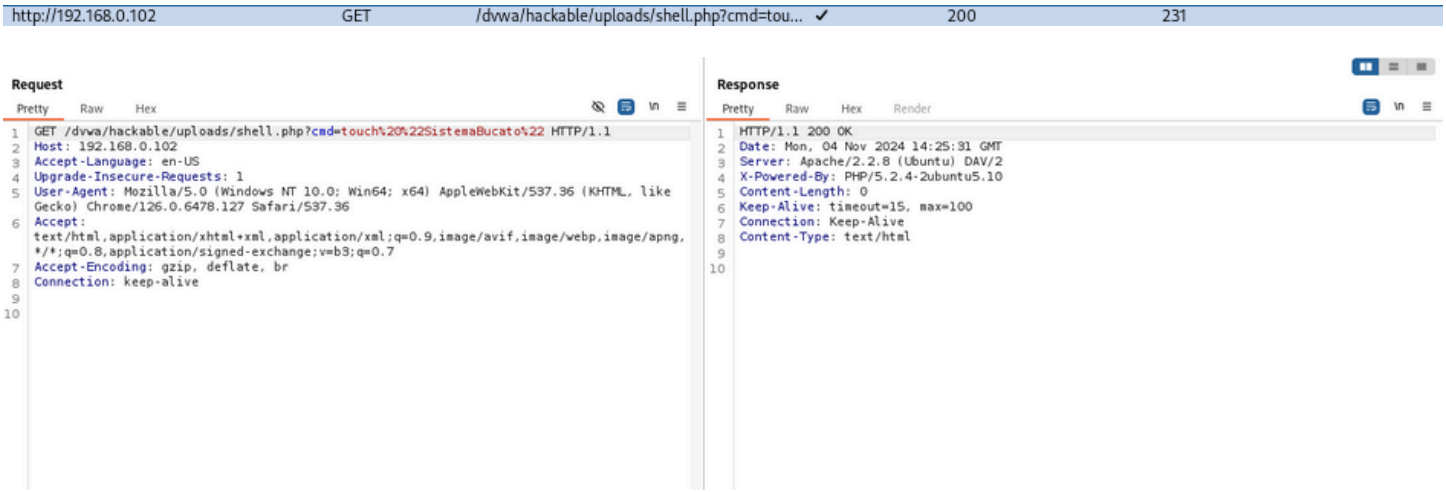
http://192.168.0.102/dvwa/hackable/uploads/shell.php?cmd=ls

è possibile notare subito che ci vengono forniti 2 output, dwva_email.png e shell.php, ovvero il risultato del comando **ls** (**list item**), e qui sotto lo screenshot delle richieste:

Questa richiesta viene utilizzate per eseguire il comando **ls** attraverso la shell PHP

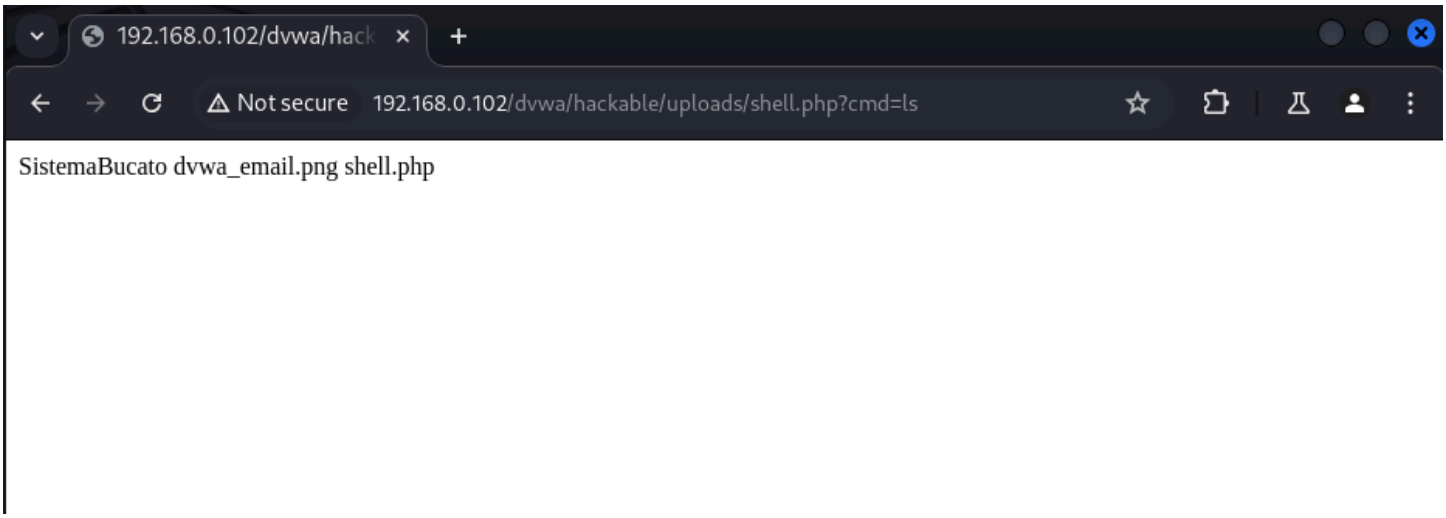
2) Richiesta:

In questa richiesta, il comando touch **testfile** viene eseguito sulla macchina bersaglio per creare un file vuoto chiamato **testfile** appunto.



Ci serve per dimostrare la possibilità di manipolare il file system del server remoto tramite la shell PHP.

E l'output sarà uguale a:



Conclusione:

Queste richieste servono a:

- Testare e verificare il funzionamento della shell PHP;
- Dimostrare la possibilità di eseguire comandi remoti;
- Manipolare il server bersaglio, co la creazione di file, escalation di privilegi etc...