**Exploit File upload**

**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.

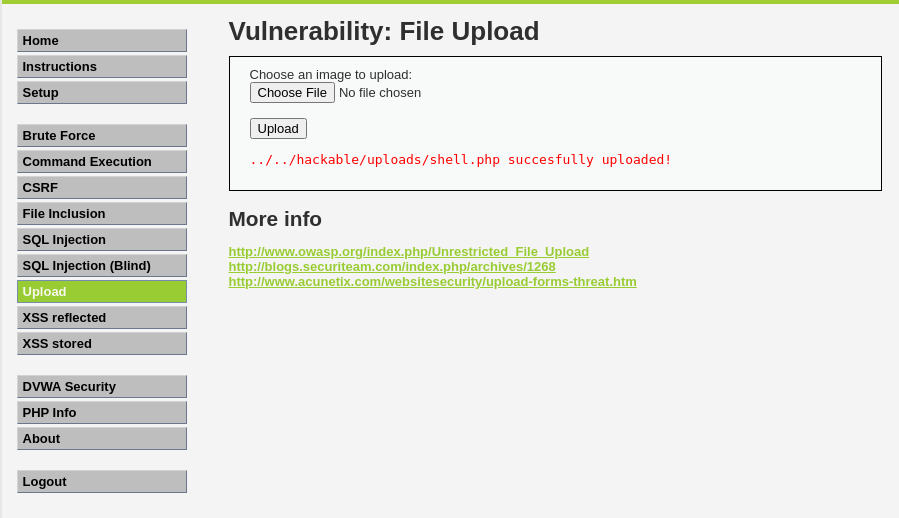
Consegna:

* Codice php usato:

A screenshot of a computer

Description automatically generated

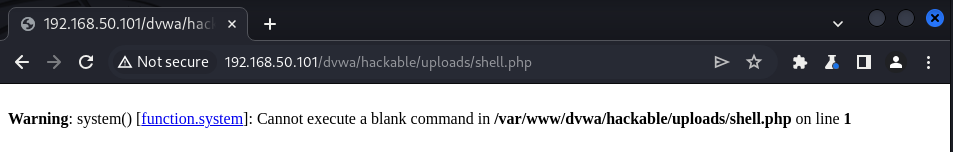
* Risultato del caricamento (screenshot del browser).



* Intercettazioni (screenshot di burpsuite).



* Risultato delle varie richieste



Questo errore è presente perché la nostra shell si aspetta un parametro cmd nella get con un comando da eseguire, mentre noi al momento non abbiamo passato nessun argomento.

A screenshot of a computer

Description automatically generated

In questo caso non riceviamo nessun errore perché abbiamo inserito la cmd con il comando whoami

e in risposta ci ha detto che noi siamo www-data