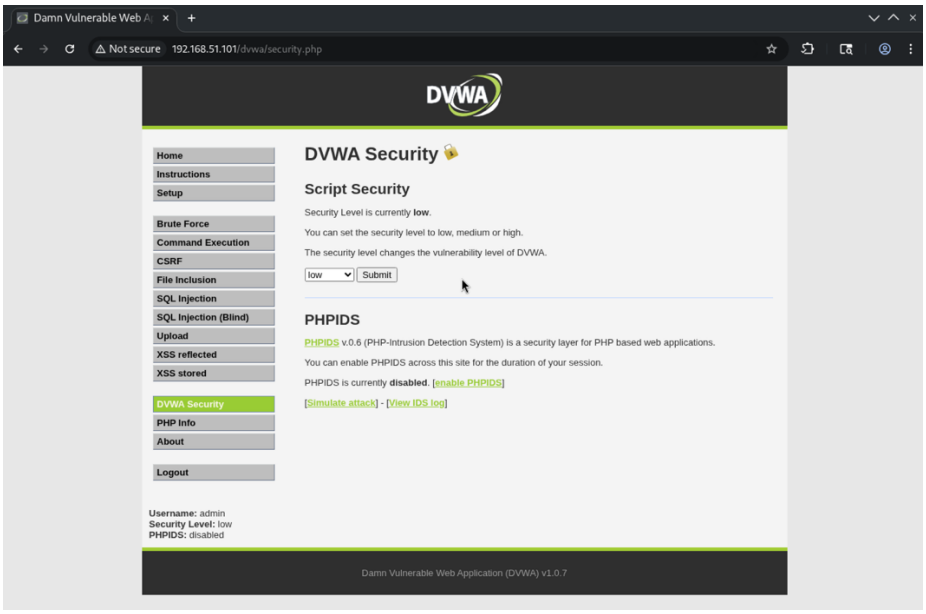
Raul Pastor

Exploit file upload

Nell'esercizio di oggi viene richiesto di utilizzare l'exploit attraverso il file upload di un file .php utilizzando la DVWA di meta attraverso la macchina Kali ed osservare le richieste con Burpsuite.

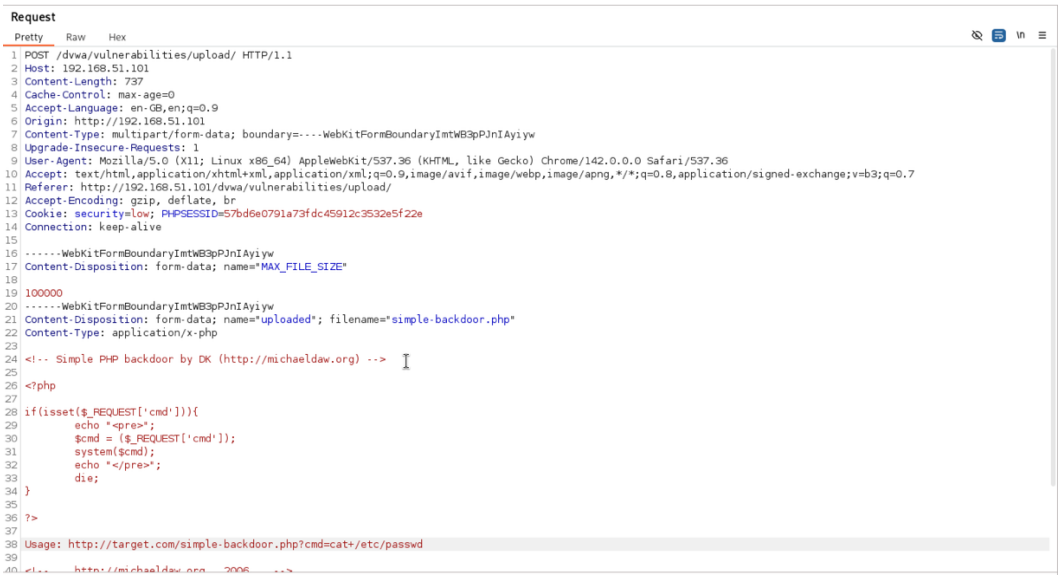
La prima cosa fatta è stata mettere in collegamento le due macchine, dopodiché mi sono collegato alla DVWA di Meta sempre da Burpsuite per verificare la tracciabilità delle richieste.

Ho Settato la sicurezza a Low (con richiesta POST in HTTP):



Raul Pastor

Per continuare ho preso una shell .php da kali chiamata “simple-backdoor.php” e l’ho caricata sulla DVWA di Meta:



Infine ho carcato di accedere al path “/dwa/vulnerabilities/uploads/simple-backdoor-php” con il comando “?cmd=cat+/etc/passwd”:

Il comando mi ha restituito una lista di username con password nascoste con “x” e una serie di informazioni (come home directory, shell e altre):