Exploit File Upload

Descrizione dell'esercizio

L'esercizio di oggi consiste nell'uploadare una semplice shell in PHP su DVWA e monitorare gli step usando Burp Suite.

La consegna prevede:

- Codice php.
- Risultato del caricamento (screenshot del browser).
- Intercettazioni (screenshot di burpsuite).
- Risultato delle varie richieste.
- Eventuali altre informazioni scoperte della macchina interna.
- BONUS: usare una shell php più sofisticata.

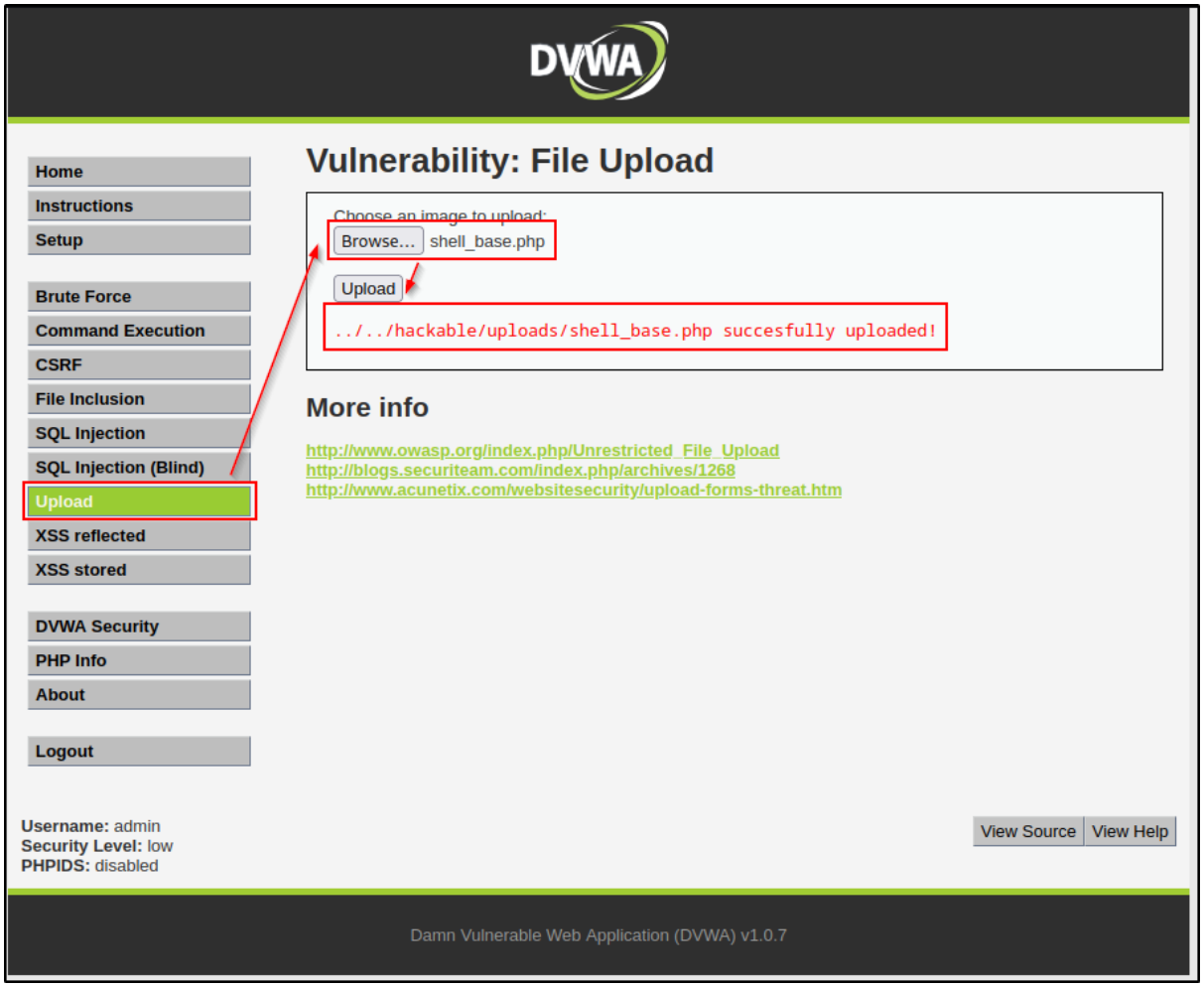
Codice PHP

Per la shell base ho usato il codice PHP fornito nell'esercizio riportato di seguito:

```
└─$ cat shell_base.php
<?php system($_REQUEST["cmd"]); ?>
```

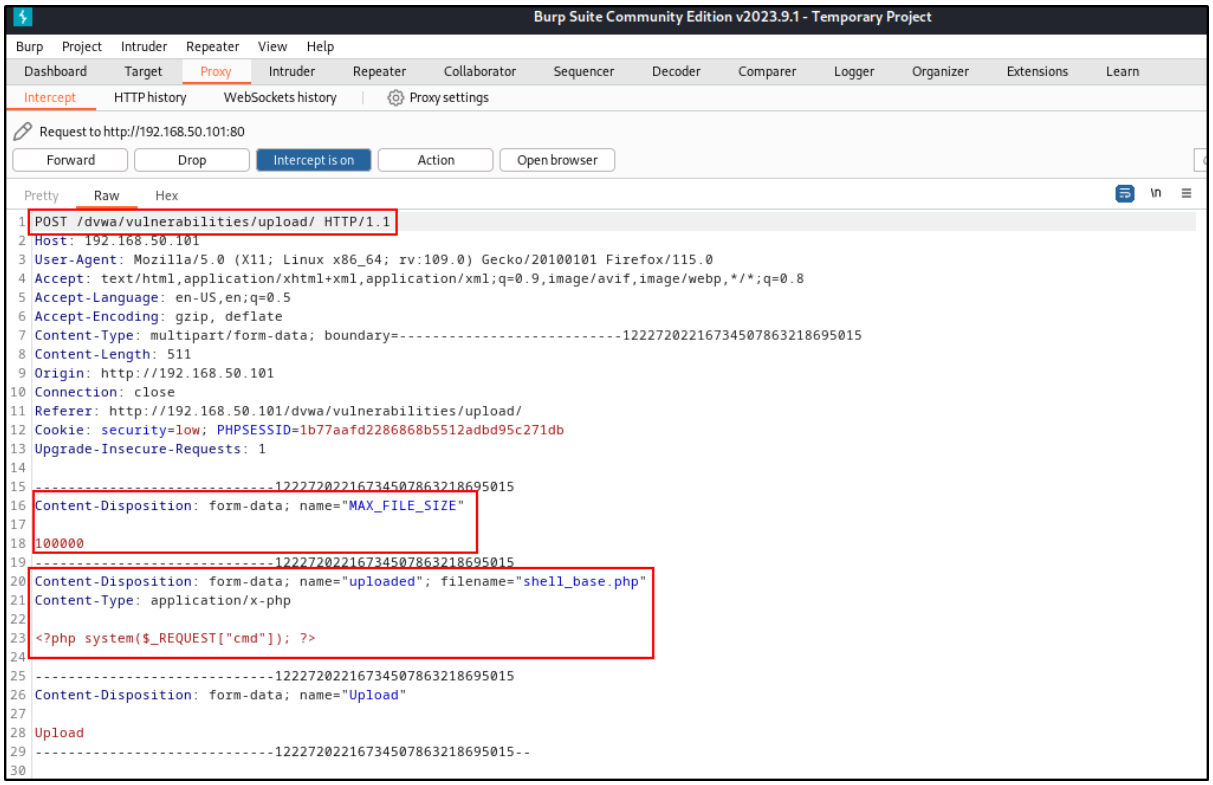
Risultato del caricamento

Dopo aver accesso alla DVWA sono andato nella sezione Upload, ho cliccato su Browse per selezionare il file da caricare ed infine ho cliccato su Upload per caricarlo.
Leggendo l'output del risultato posso ottenere una risposta di esito positivo del caricamento e dedurre in quale directory è stato caricato il file (in questo caso dvwa/hackable/uploads/).



Intercettazioni

Se eseguo lo step precedente intercettando il traffico con Burp Suite ottengo il seguente risultato:



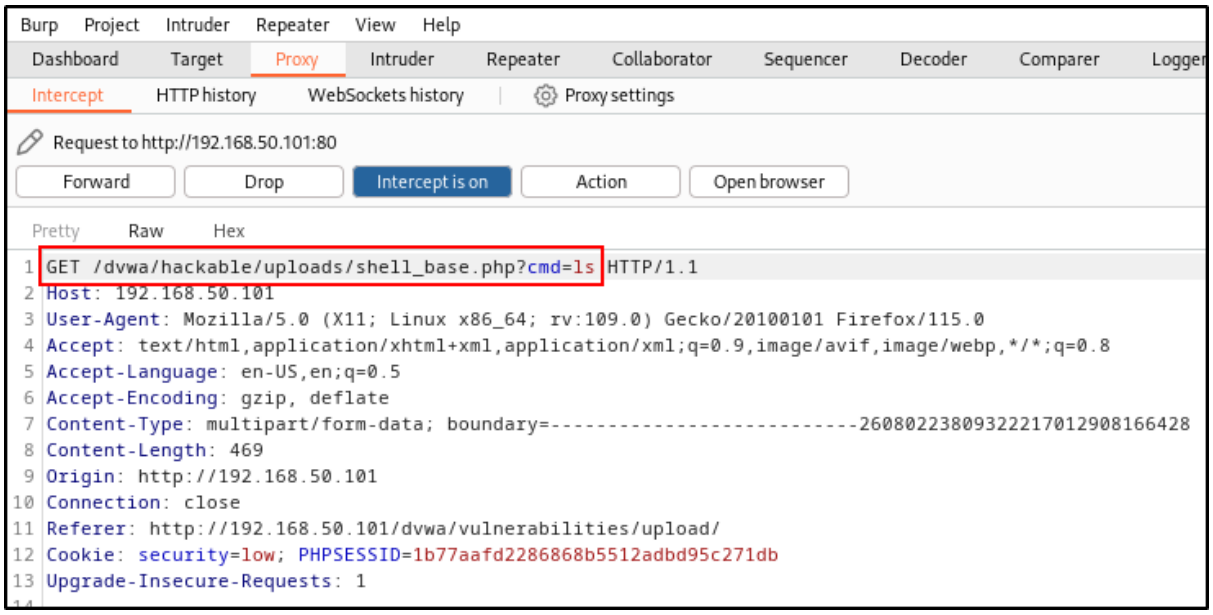
Le due cose che mi saltano subito all'occhio sono la richiesta di POST che gestisce l'upload del file, un parametro che definisce la dimensione massima del file accettato e un altro parametro che racchiude diversi parametri relativi al file quali ad esempio: nome, tipo di file e contenuto dello stesso.

Risultato delle varie richieste

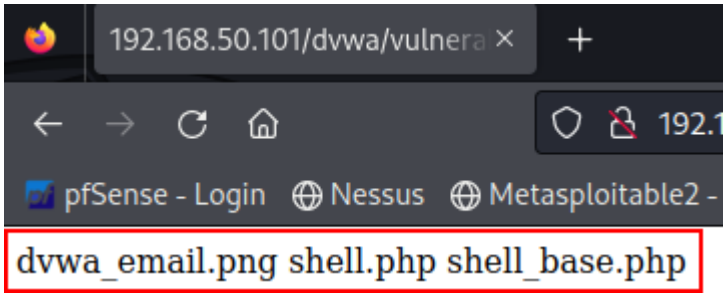
Per testare che la shell funzioni posso modificare la richiesta precedente intercettata con Burp Suite modificato il metodo POST con GET e passando la seguente stringa:

GET /dvwa/hackable/uploads/shell_base.php?cmd=ls

Questa stringa prende il file che ho caricato e passa il comando ls aggiungendo ?cmd=ls dopo il nome del file.



Il risultato viene mostrato nel browser ed è la lista dei file presenti nella directory dov'è caricato il file (ovvero l'output del comando ls)

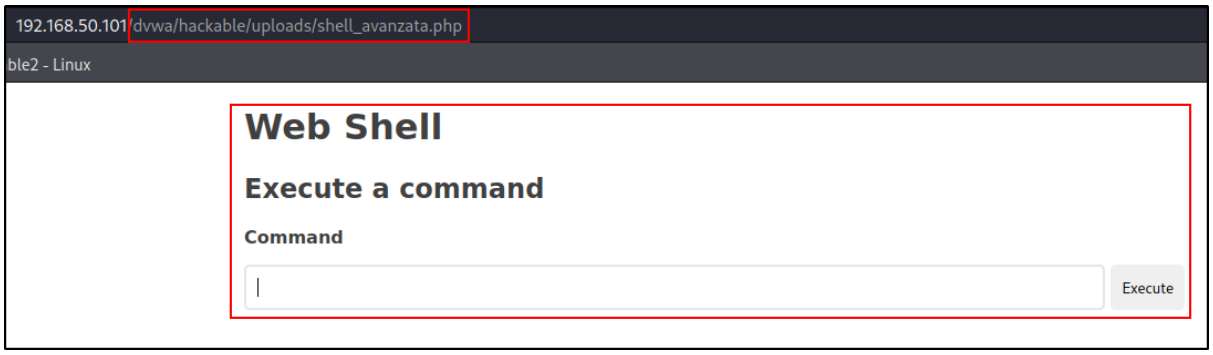


Eventuali altre informazioni scoperte della macchina interna.

BONUS: usare una shell php più sofisticata.

Per facilitare la penultima consegna ho deciso di caricare una shell più avanzata che mi permette di inserire i comandi direttamente sul browser e poter esplorare la macchina in maniera più agevolata.

Dopo averla caricata nello stesso metodo usato in precedenza ho inserito il path del file nella barra degli indirizzi del browser facendo così aprire la shell.



Da qui ho provato a mostrare il contenuto della cartella /etc/passwd dove solitamente sono contenute informazioni dettagliate sugli utenti del sistema e il comando ha avuto esito positivo.