HTB CozyHosting

Enumeration

`sudo nmap -sC -sV -oA nmap/cozyhosting 10.10.11.230`

Discovery

Endpoints

- `cozyhosting.htb`
  - `/admin`
  - `/error`
  - `/index`
  - `/login`
  - `/logout`
  - `/actuator`
    - `/env`
    - `/mappings`
    - `/sessions`

Technologies

- Java Spring Boot — from `/error` message

Credentials

- postgresql
  - url: `jdbc:postgresql://localhost:5432/cozyhosting`
  - username: `postgres`
  - password: `Vg&nvzAQ7XxR`
- User
  - name : kanderson
  - hashed password: `$2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim`
  - cracked password: `manchesterunited`
  - role: `User`
- admin

  - hashed password: `$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm`
  - role: `Admin`

Vulnerabilities

- Sensitive Information Disclosure on these endpoints
  - `/actuator/env` --> environment variables
  - `/actuator/mappings` --> MVC controller mappings
  - `/actuator/sessions` --> HTTP sessions
- RCE on `/executessh` known by `'"` seems to result a 400 Bad Request

Exploitation

- Steal session cookies to access `/admin` page
- Reverse shell `rev-shell.py`
- Exfil `cloudhosting-0.0.1.jar` application
- Reverse Engineer to find database credential at `BOOT-INF/classes/application.properties`
- Find user credential in the database
- Use hashcat/john to crack the user password
- GTFO bins elevating ssh to root

Appendix

User Flag: `b2da22f0082b31074ea83a2b51da849f`
Root Flag: `9d7afea7a9e468e9b2da602eaf715120`