THM Spring4Shell Write Up

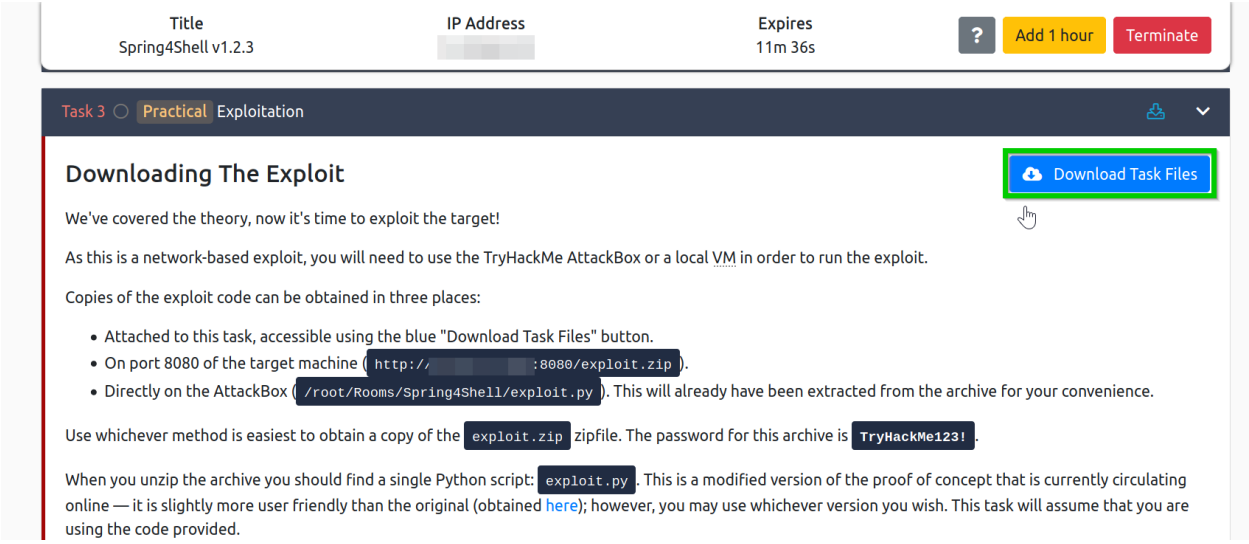
Link to room:
https://tryhackme.com/room/spring4shell

Unlike Log4J, the Spring4Shell vulnerability requires a few prerequisites to properly be exploited. As of date, these requirements include:

- JDK/Java 9+
- A vulnerable version of the Spring Framework (<5.2 | 5.2.0-19 | 5.3.0-17)
- Apache Tomcat as a server for the Spring application, packaged as a WAR
- A dependency on the spring-webmvc and/or spring-webflux components of the Spring Framework

This room will show how to run the exploit and gain access to cmd.

1. **Download the exploit**



   It will save to your downloads folder. May sure to extract it using TryHackMe123!
2. **Code Review**

THM Spring4Shell Write Up

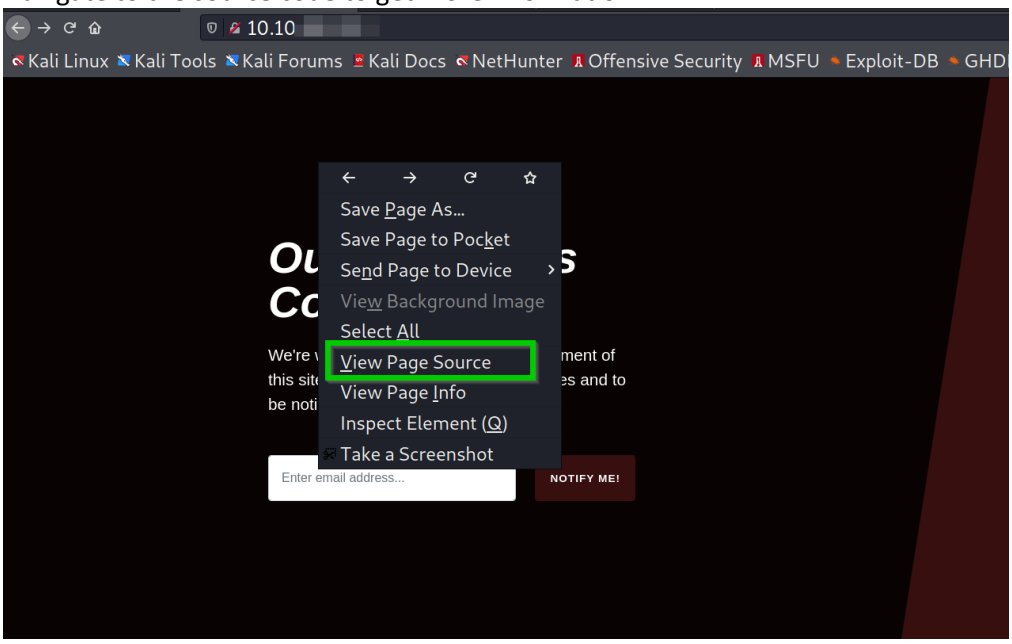
Run a –help command on the exploit to see the arguments:

```
┌──(kali㉿kali)-[~/THM/Spring4Shell]
└─$ cat
^Z
zsh: suspended  cat

┌──(kali㉿kali)-[~/THM/Spring4Shell]
└─$ ./exploit.py --help
usage: exploit.py [-h] [-f FILENAME] [-p PASSWORD] [-d DIRECTORY] url

Spring4Shell RCE Proof of Concept

positional arguments:
  url                   Target URL

optional arguments:
  -h, --help            show this help message and exit
  -f FILENAME, --filename FILENAME
                        Name of the file to upload (Default tomcatwar.jsp)
  -p PASSWORD, --password PASSWORD
                        Password to protect the shell with (Default: thm)
  -d DIRECTORY, --directory DIRECTORY
                        The upload path for the file (Default: ROOT)
```

We will need the target URL. To get this information. You should also do a cat on the exploit to get a better idea of what the exploit is doing.

3. **Target URL**

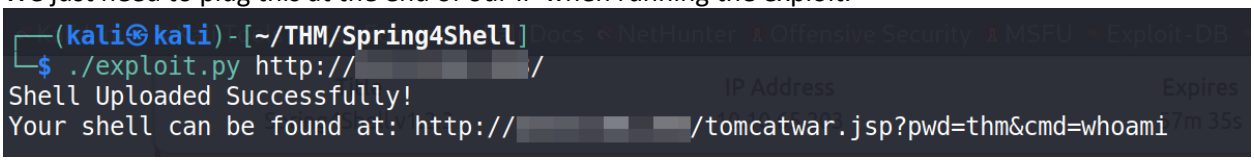
To get the target url, we need to look at the source code of the target.
Open a browser and navigate to the ip address.
Navigate to the source code to get more information.



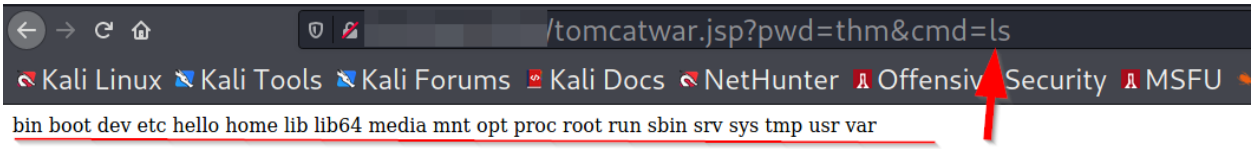
We need to look for the action identifier for POST. In this case, it is a simple forward slash.

THM Spring4Shell Write Up

We just need to plug this at the end of our IP when running the exploit.



The exploit should return a link. This will provide you with terminal access.
Try to change the “whoami” with an “ls” to locate the different directories.



Note the root folder. Let’s run an ls on root and theres the flag!