

CVE-2017-12615漏洞复现

环境配置

docker拉取镜像

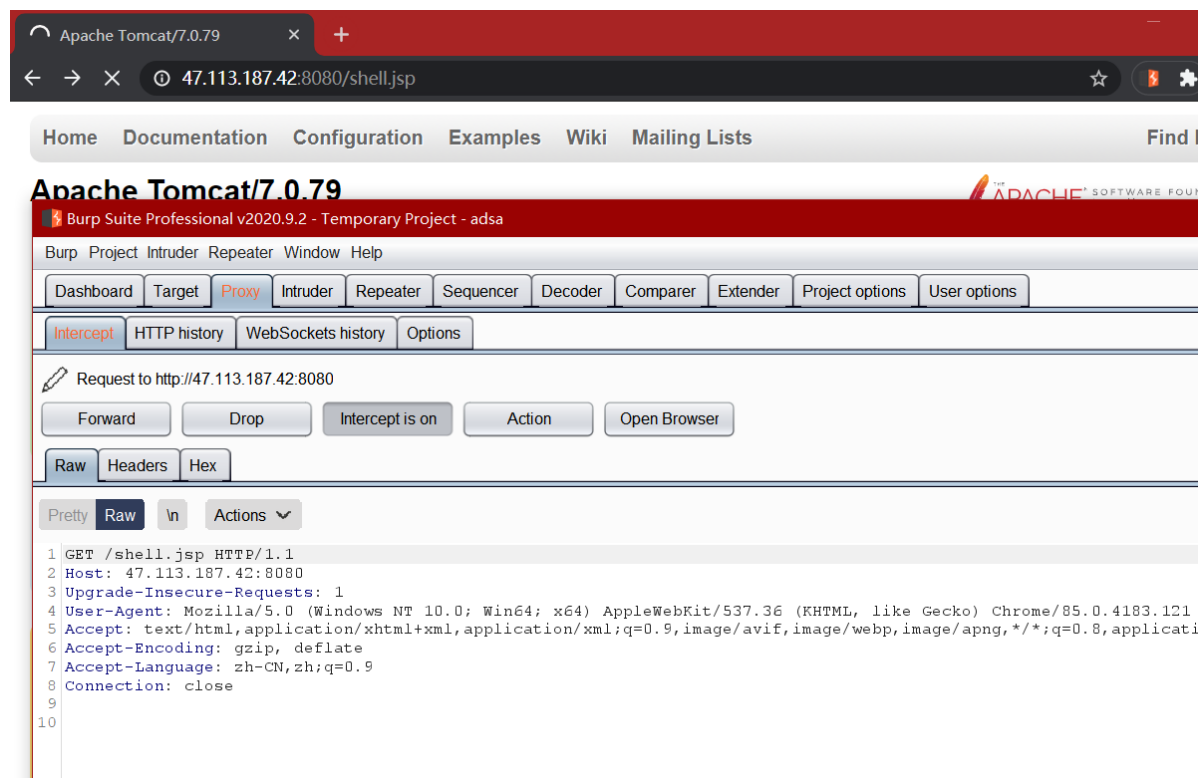
```
docker pull cved/cve-2017-12615:latest
```

后台启动容器

```
docker run -d -p 8080:8080 7633828fbea8
```

漏洞复现

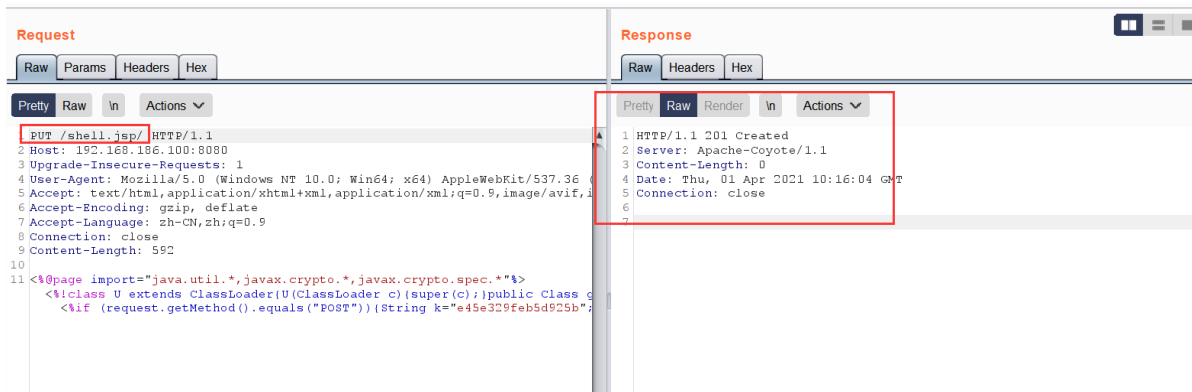
访问tomcat，利用PUT请求创建文件。构造webshell请求，使用bp抓包，如下图



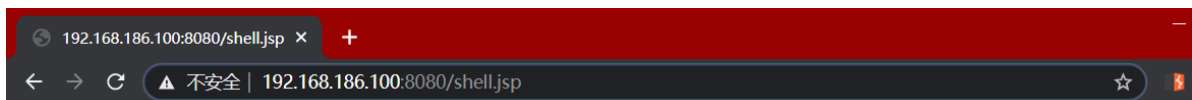
发送到重发器进行测试，利用PUT请求创建文件，构造webshell



其中文件名设为/shell.jsp/绕过（如果文件名后缀是空格那么将会被tomcat给过滤掉）利用文件解析漏洞采用PUT方式上传jsp webshell文件。如下图



上传成功，访问一下



空白，被解析成功，webshell工具连接



环境变量:

```
PATH=/usr/local/tomcat/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
LANGUAGE=C.UTF-8
TOMCAT_TGZ_URL=https://www.apache.org/dyn/closer.cgi?action=download&filename=tomcat/tomcat-7/v7.0.79/bin/apache-tomcat-7.0.79.tar.gz
JAVA_HOME=/docker-java-home/jre
CATALINA_HOME=/usr/local/tomcat
TOMCAT_ASC_FALLBACK_URL=https://archive.apache.org/dist/tomcat/tomcat-7/v7.0.79/bin/apache-tomcat-7.0.79.tar.gz.asc
CA_CERTIFICATES_JAVA_VERSION=20170531+nmul
TOMCAT_TGZ_FALLBACK_URL=https://archive.apache.org/dist/tomcat/tomcat-7/v7.0.79/bin/apache-tomcat-7.0.79.tar.gz
LANG=C.UTF-8
TOMCAT_MAJOR=7
TOMCAT_VERSION=7.0.79
HOSTNAME=5ae054bd125d
JAVA_DEBIAN_VERSION=8u141-b15-1~deb9u1
LC_ALL=C.UTF-8
LD_LIBRARY_PATH=/usr/local/tomcat/native-jni-lib
OPENSSL_VERSION=1.1.0f3
TOMCAT_ASC_URL=https://www.apache.org/dist/tomcat/tomcat-7/v7.0.79/bin/apache-tomcat-7.0.79.tar.gz.asc
```