CVE-2017-12615漏洞复现

环境配置

docker拉取镜像

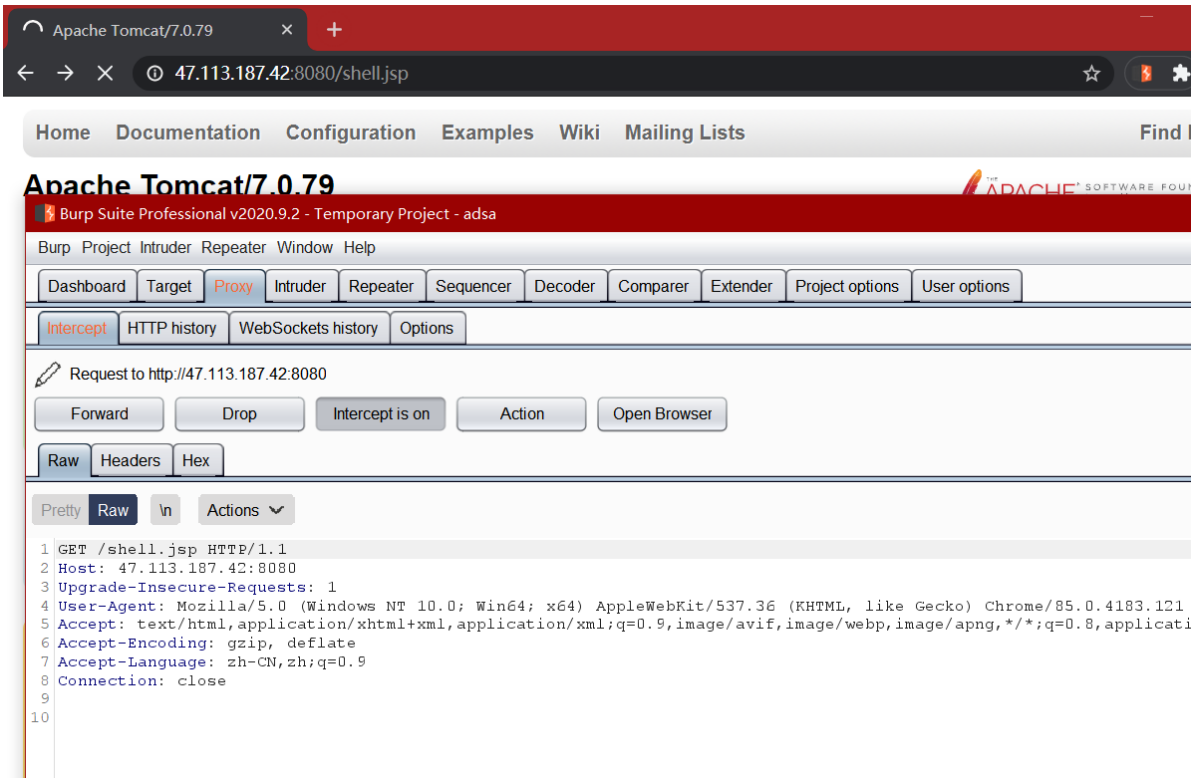
```
docker pull cved/cve-2017-12615:latest
```

后台启动容器

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

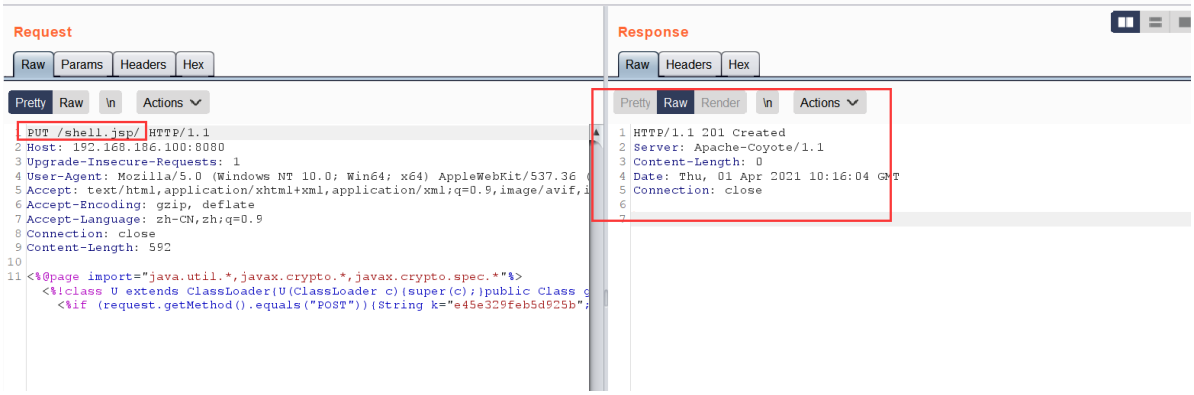
漏洞复现

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