java代码审计深度解析

第一课　不安全的http

PART 01

不安全的http请求

HTTP简介

HTTP1.0定义了三种请求方法： GET, POST 和 HEAD方法

HTTP1.1新增了五种请求方法：OPTIONS, PUT, DELETE, TRACE 和 CONNECT 方法

可利用的PUT方法

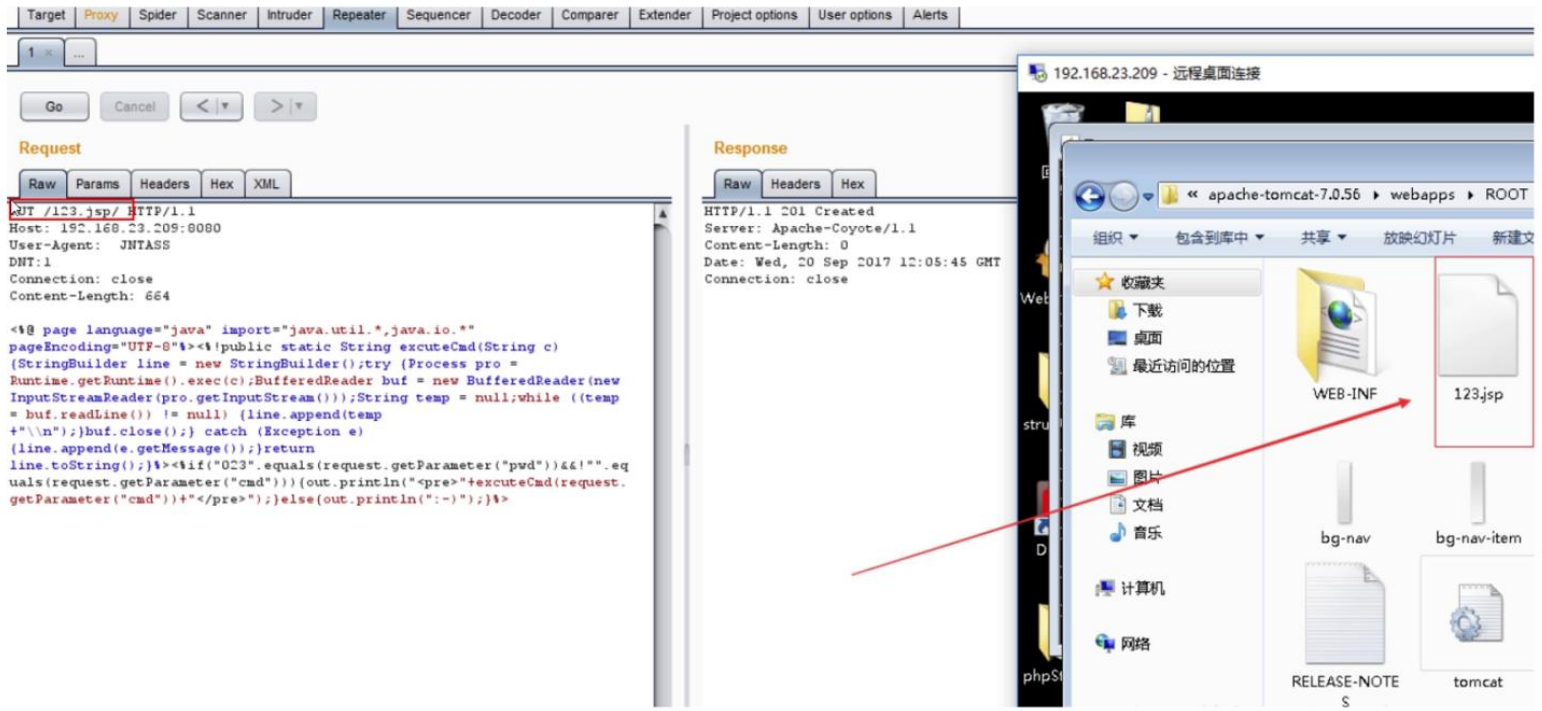
Tomcat 7.0.0-7.0.81

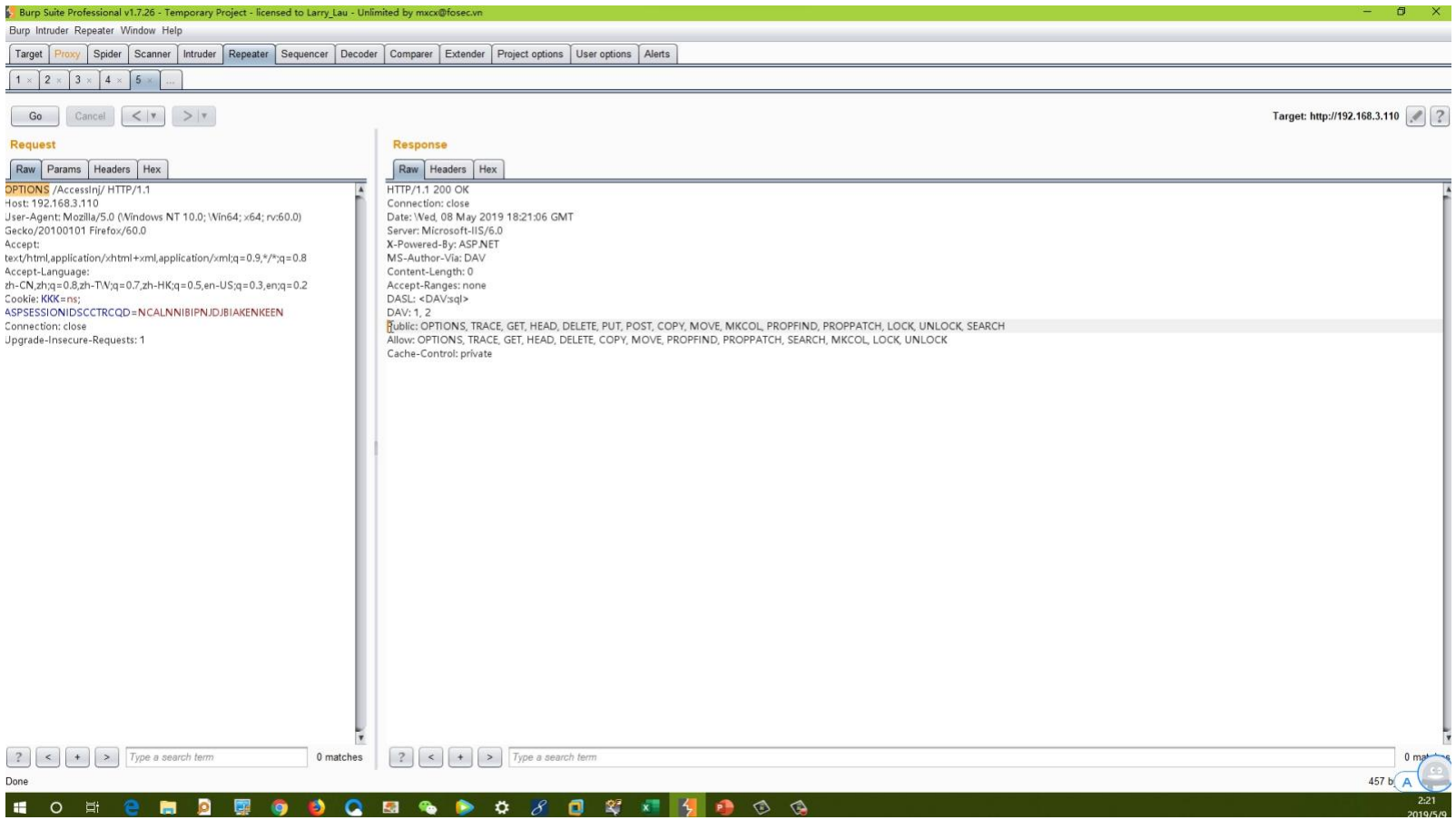
Apache Tomcat

我们来分析tomcat这个漏洞，需要首先允许tomcat进行PUT操作，问题也就在 /conf/web.xml

```
<servlet>
    <servlet-name>default</servlet-name>
    <servlet-class>org.apache.catalina.servlets.DefaultServlet</servlet-class>
    <init-param>
        <param-name>debug</param-name>
        <param-value>0</param-value>
    </init-param>
    <init-param>
        <param-name>listings</param-name>
        <param-value>false</param-value>
    </init-param>
    <init-param>
        <param-name>readonly</param-name>
        <param-value>false</param-value>
    </init-param>
    <load-on-startup>1</load-on-startup>
</servlet>
```

Apache Tomcat PUT上传




Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 5 ...
Go Cancel
Target: http://192.168.3.110
Request
Raw Params Headers Hex
OPTIONS /AccessInj/ HTTP/1.1
Host: 192.168.3.110
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Cookie: KKK=ns;
ASPSESSIONIDSCCTRCQD=NCALNNIBIPNJDJBIAKENKEEN
Connection: close
Upgrade-Insecure-Requests: 1
Response
Raw Headers Hex
HTTP/1.1 200 OK
Connection: close
Date: Wed, 08 May 2019 18:21:06 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
Cache-Control: private
Type a search term
0 matches
Done

谢谢观赏