**文件上传漏洞——JS绕过**

**预备知识**

【BurpSuite】的基本使用

客户端javascript检测的原理

【中国菜刀】的基本使用

**实验目的**

绕过JavaScript验证检测，上传一句话木马。

**实验工具**

BurpSuite、中国菜刀、一句话木马

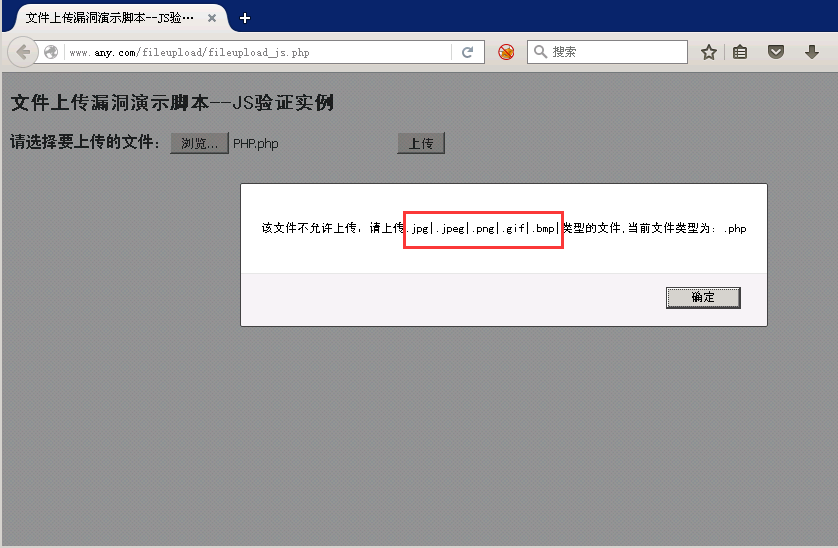
**实验环境**

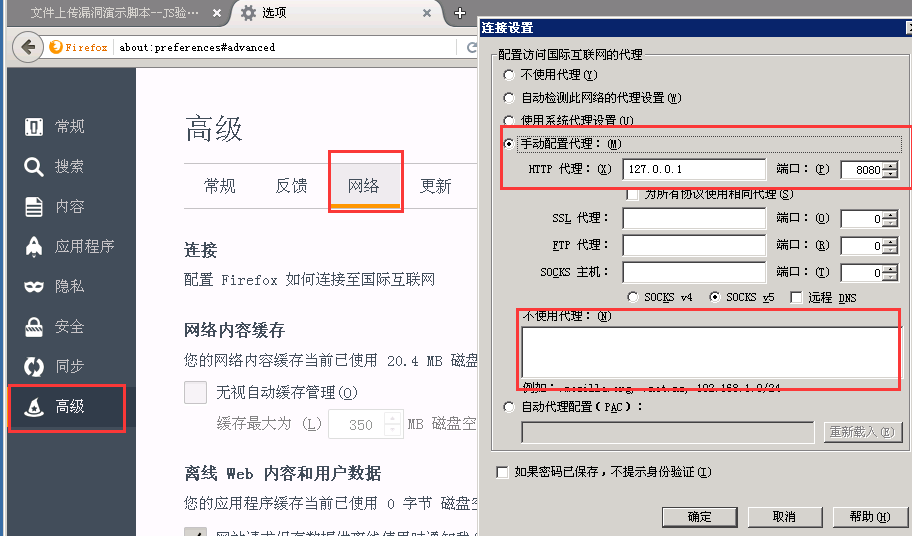
服务器一台（Windows Server 2003）客户机一台（windows Server 2003）

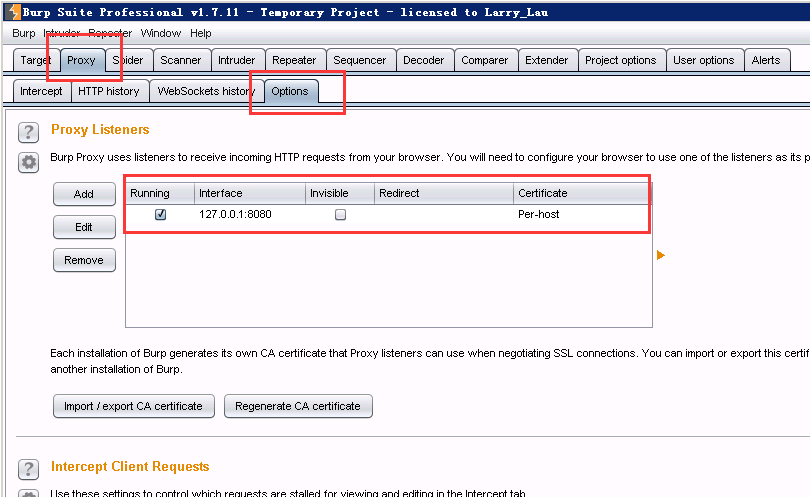
**实验步骤**

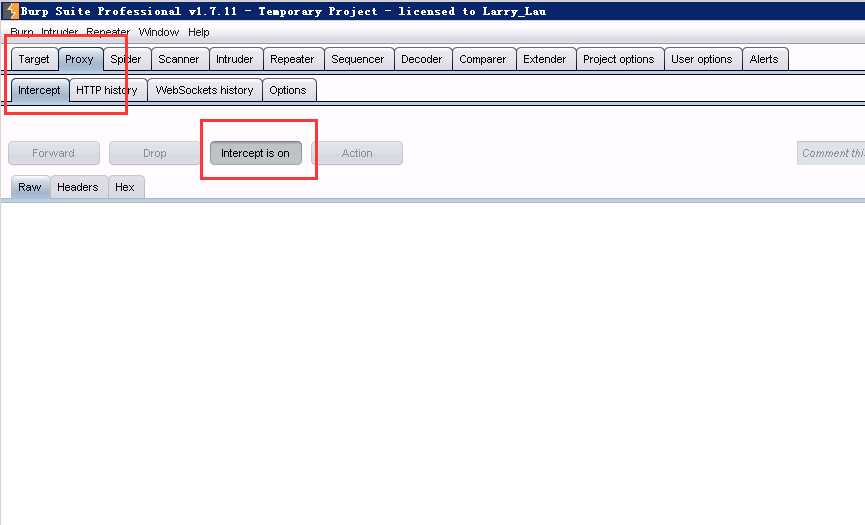
第一步：打开下方网页，上传事先准备好的一句话木马PHP.php（桌面-实验工具文件夹内），发现失败，设置了白名单校验，只能允许白名单内设置好的类型

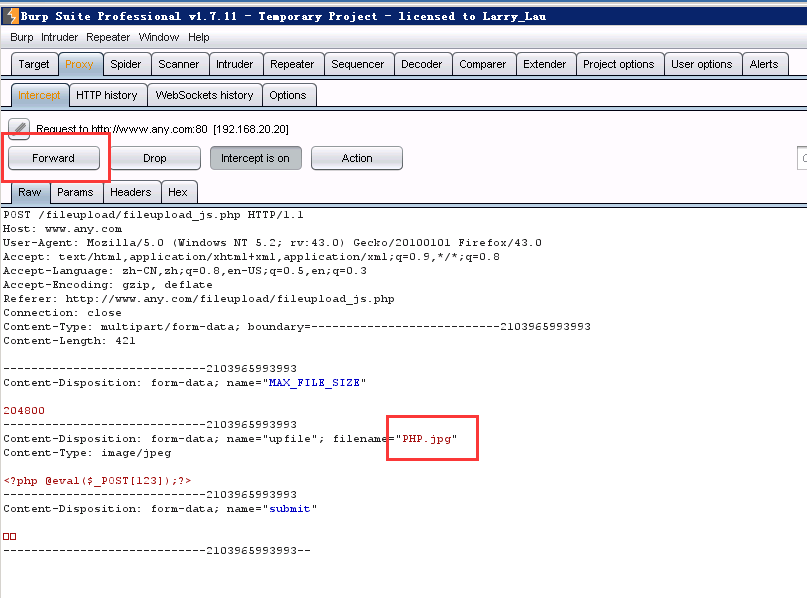
http://127.0.0.1/fileupload/fileupload\_js.php



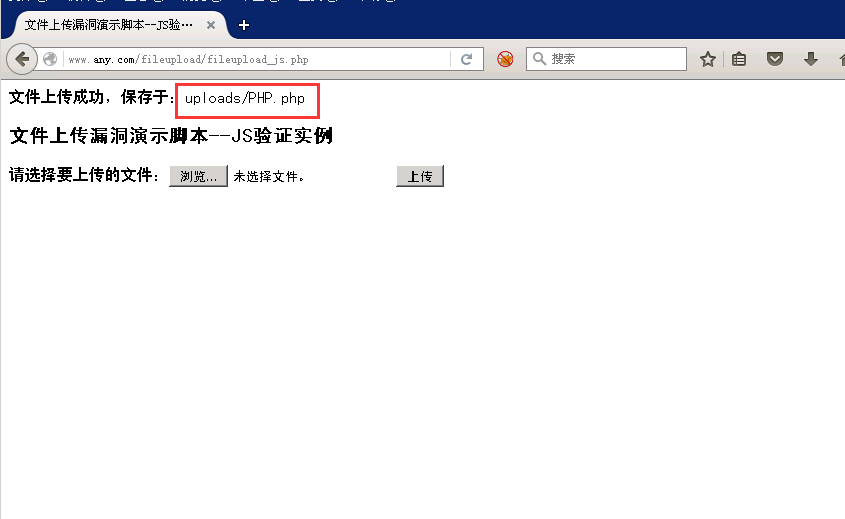
第二步：设置浏览器代理（右上方的菜单-选项-高级-网络-设置）  


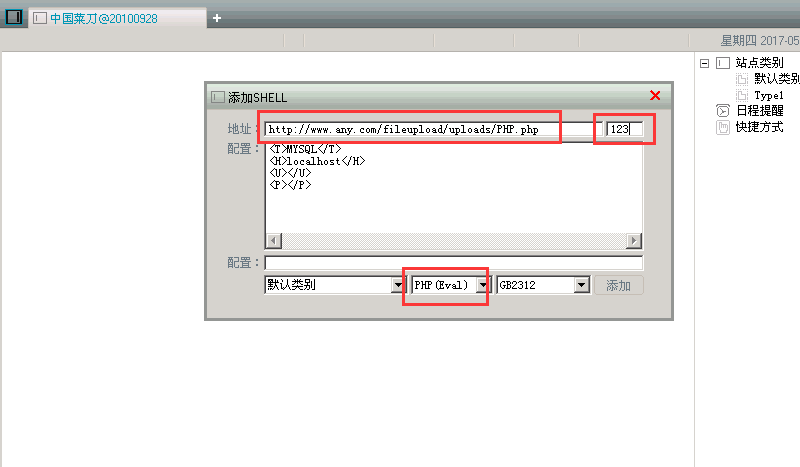
第三步：在桌面实验工具文件夹内打开BurpLoader.jar工具(桌面-实验工具文件夹内)，并设置BurpSuite代理（Proxy-Options）  


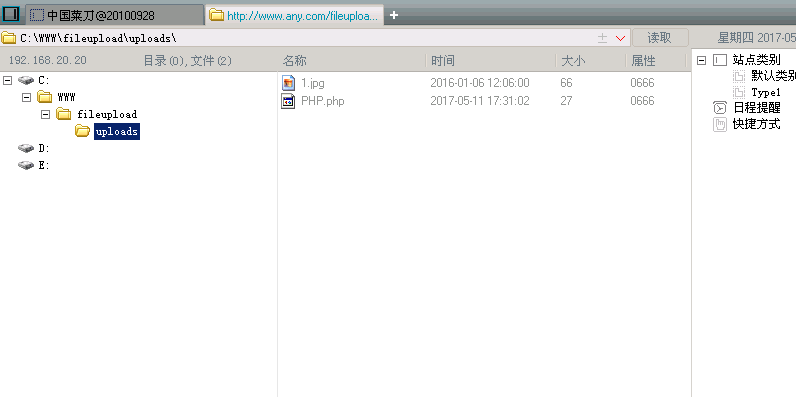
打开Intercept（拦截）  


第三步：将木马文件的后缀先改为“.jpg|.jpeg|.png|.gif|.bmp”中的任意一种格式，以“.jpg”为例。  
修改为PHP.jpg,再次上传，此时上传数据被BurpSuite拦截，修改filename='PHP.php'，点击Forward将数据包发回  
此时返回网页，发现上传成功，文件绝对路径为：

http://127.0.0.1/fileupload/uploads/PHP.php



第四步：中国菜刀连接  
将木马地址添加到中国菜刀，连接菜刀的密码是123，进行其他入侵操作。  




**文件上传漏洞——Content-Type**

**预备知识：**

Content-Type，内容类型，一般是指网页中存在的Content-Type，用于定义网络文件的类型和网页的编码，决定文件接收方将以什么形式、什么编码读取这个文件，这就是经常看到一些Asp网页点击的结果却是下载到的一个文件或一张图片的原因

**实验目的**

掌握通过修改数据包中Content-Type的值，进行文件上传。

**实验工具**

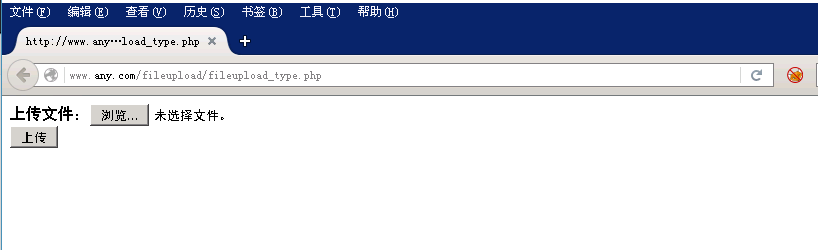
Burp Suite中国菜刀

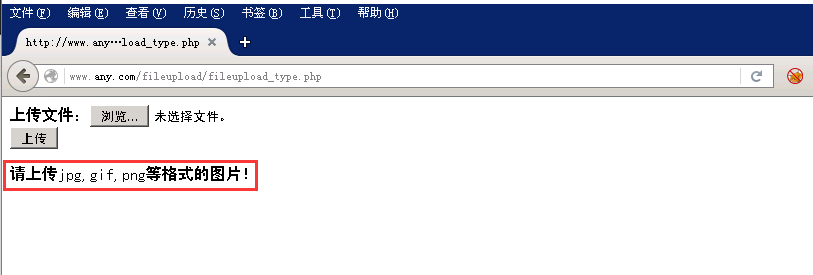
**实验环境**

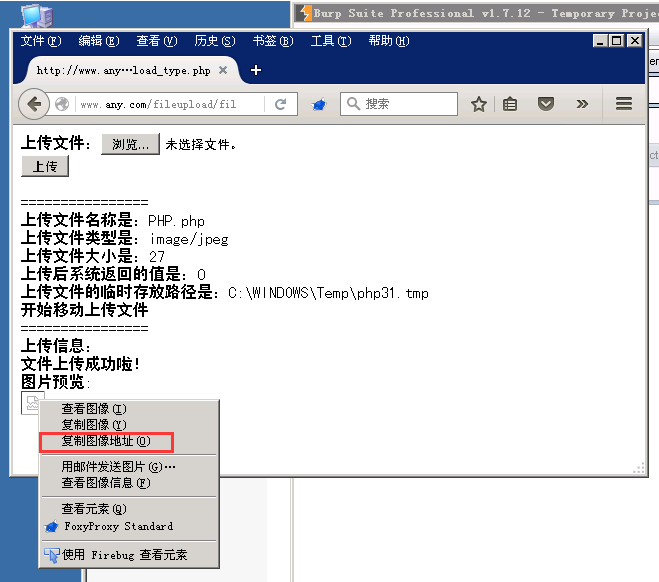
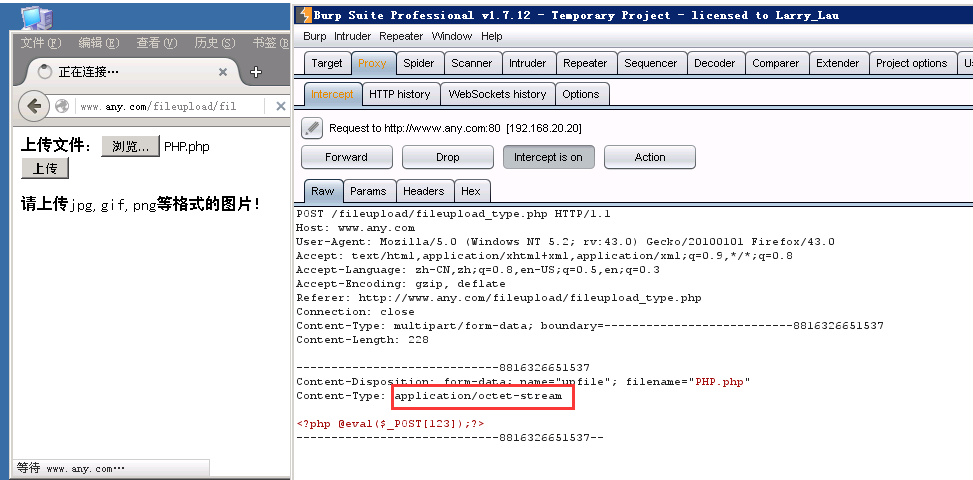
服务器一台（页面：http://127.0.0.1/fileupload/fileupload\_type.php）客户机一台

**实验步骤：**

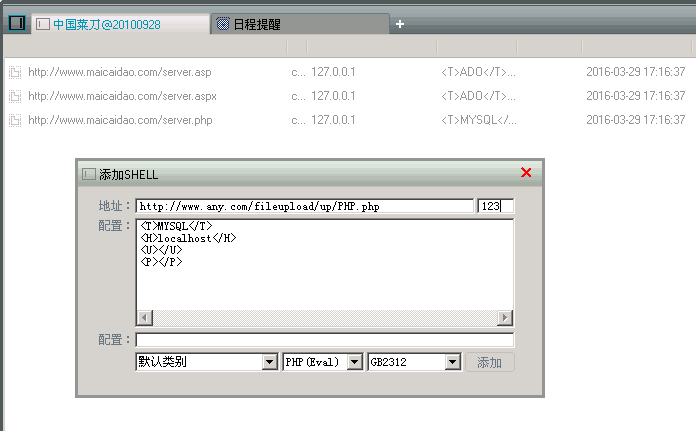
第一步：打开上传网页，右击选择查看页面源代码，页面代码中并没有对上传文件进行限制。

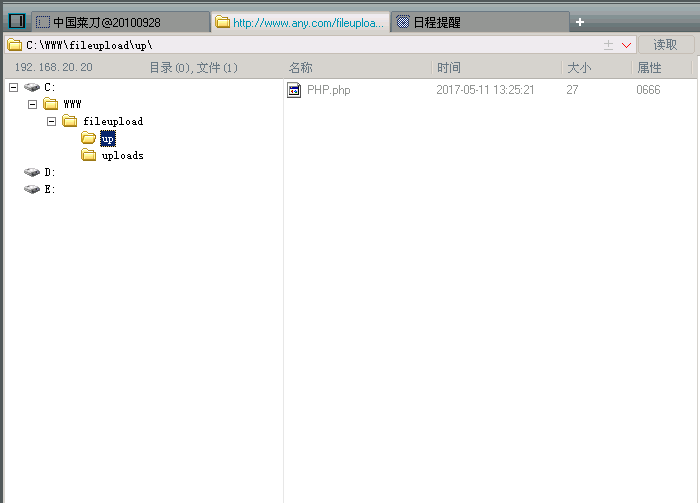


第二步：选择木马文件进行上传，上传失败，可能是后台进行了判断。  


第三步：尝试用Burp Suite抓包，通过修改包内的Content-Type值进行上传，将application/octet-stream修改为image/jpeg。  
上传成功，右击图片，选择复制图像地址，图像地址就是木马文件的地址。  


第四步：将木马地址添加到中国菜刀，密码是123，进行其他入侵操作。





**文件上传漏洞—扩展名绕过**

**预备知识**

利用上传漏洞可以直接得到webshell，危害非常高导致该漏洞的原因在于代码作者没有对访客提交的数据进行检验或者过滤不严，可以直接提交修改过的数据绕过扩展名的检验。

**实验目的**

通过修改文件名，绕过黑名单，上传一句话木马，拿到webshell

**实验工具**

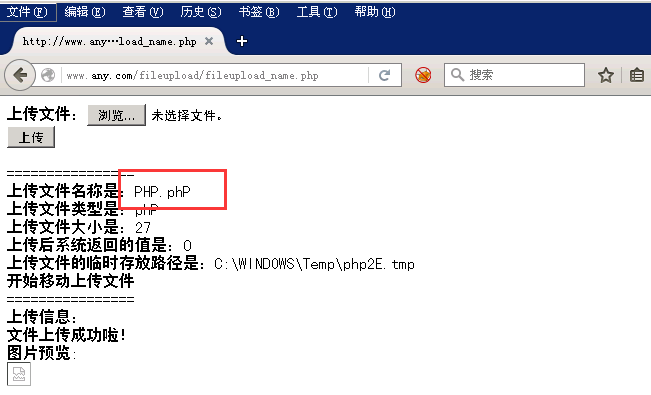
一句话木马、中国菜刀

**实验环境**

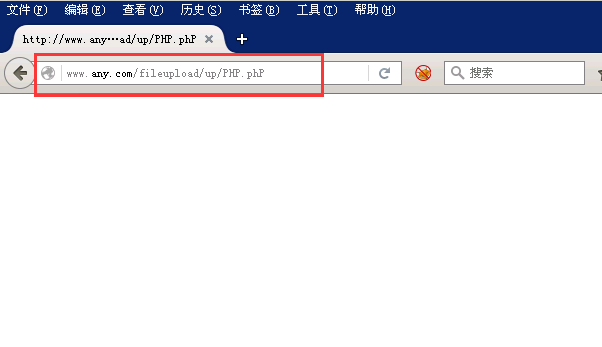
服务器一台(Windows Server 2003)客户机一台(Windows Server 2003)

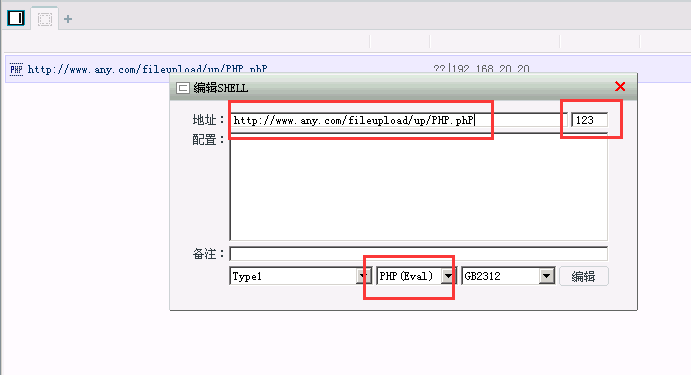
**实验步骤**

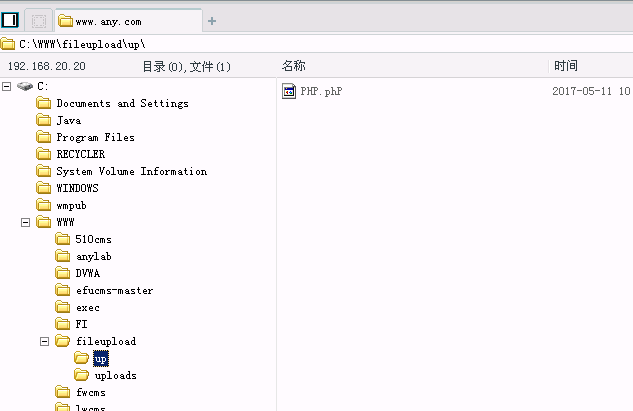
第一步：打开上传界面127.0.0.1/fileupload/fileupload\_name.php，上传事前准备好的一句话木马PHP.php，弹出“不能上传php文件”的提示，猜测是通过客户端黑名单来限制上传文件的类型  


第二步：修改文件名为PHP.phP,再次上传，成功  


第三步：图片预览下方的缩略图，右键-复制图像地址  


[http://127.0.0.1/fileupload/up/PHP.phP](http://www.any.com/fileupload/up/PHP.phP)  


第四步：在【中国菜刀】工具内输入图片绝对路径，以及密码’123’，确认木马类型，成功拿到webshell  




再进行提权，拿到最高权限，将在后续课程进行介绍