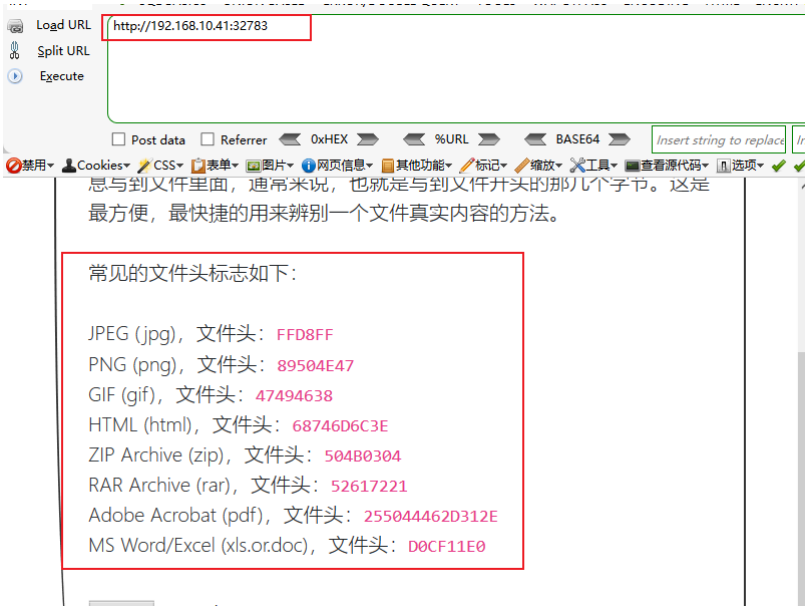
文件上传-文件头绕过

访问环境

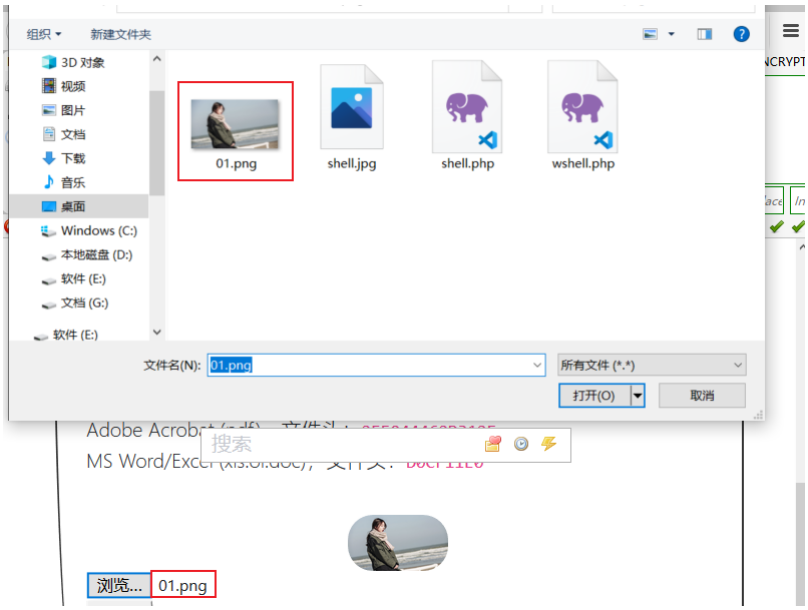
1. URL为：`http://192.168.10.41`，端口为默认`80`端口，请勿访问图片中端口。



上传普通图片

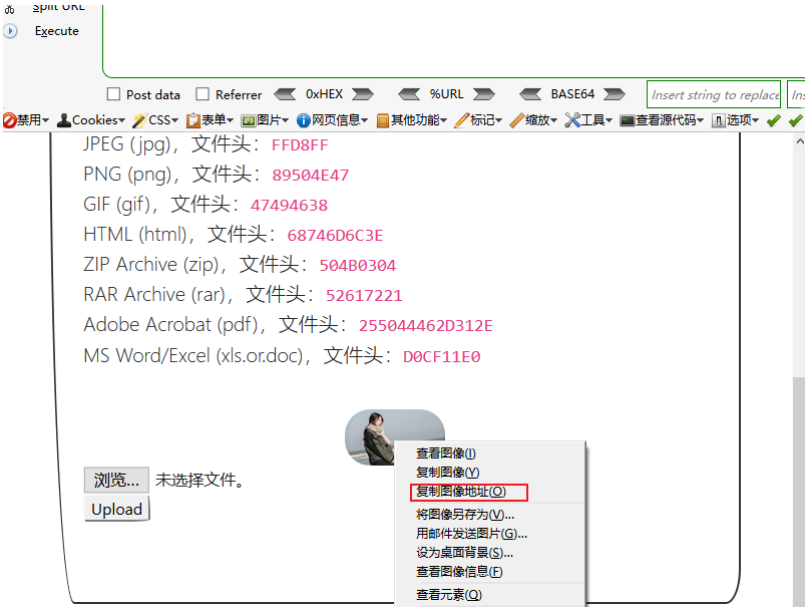
步骤一：上传普通图像查看图片地址

1. 浏览选择`01.jpg`

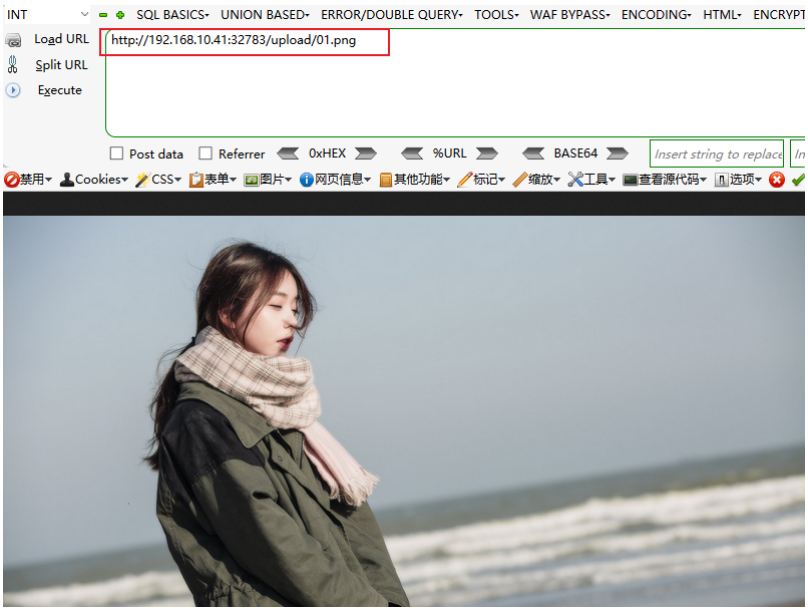


2. 点击`Upload`上传，页面中显示图片。

3. 右键复制图片地址。



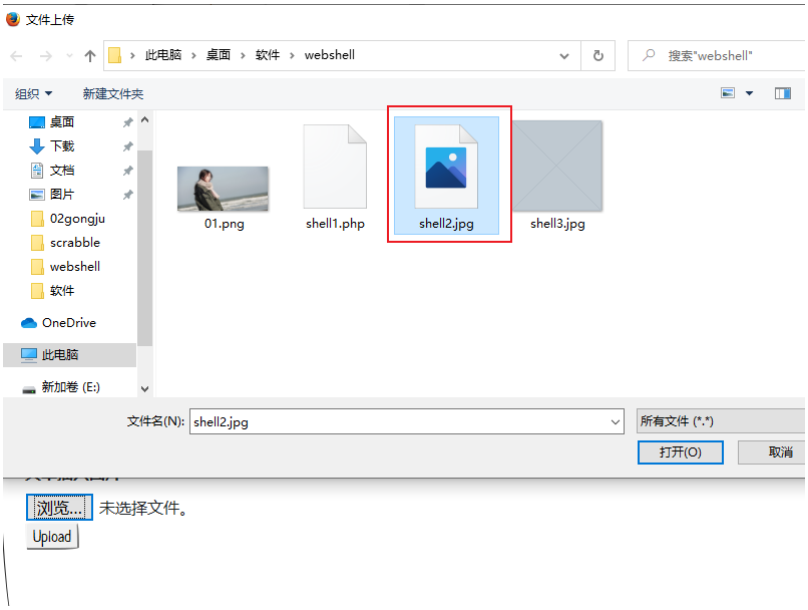
4. 访问图片地址，查看图片是否正常。图片正常。



上传木马文件

步骤一：上传php木马文件。

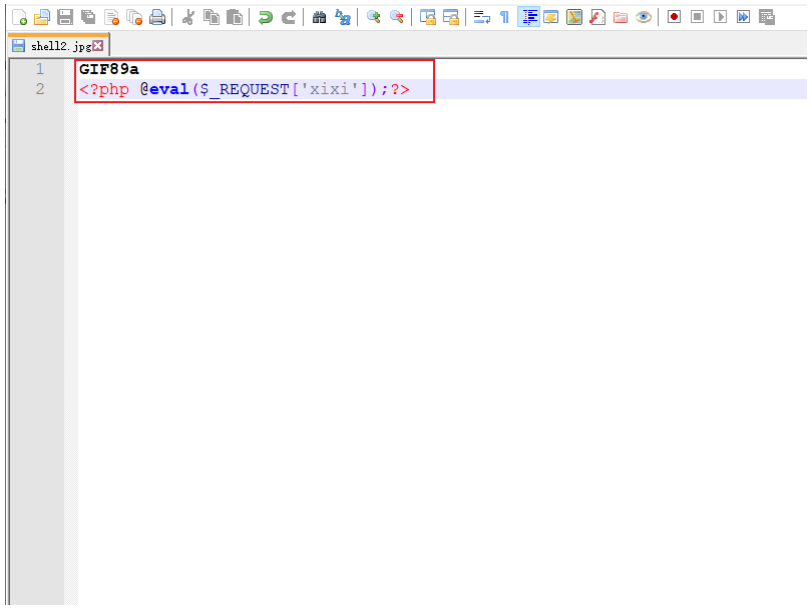
1. 上传`shell2.jpg`文件。



2. 点击`Upload`上传，提示允许上传`jepg jpg png gif`类型的问。

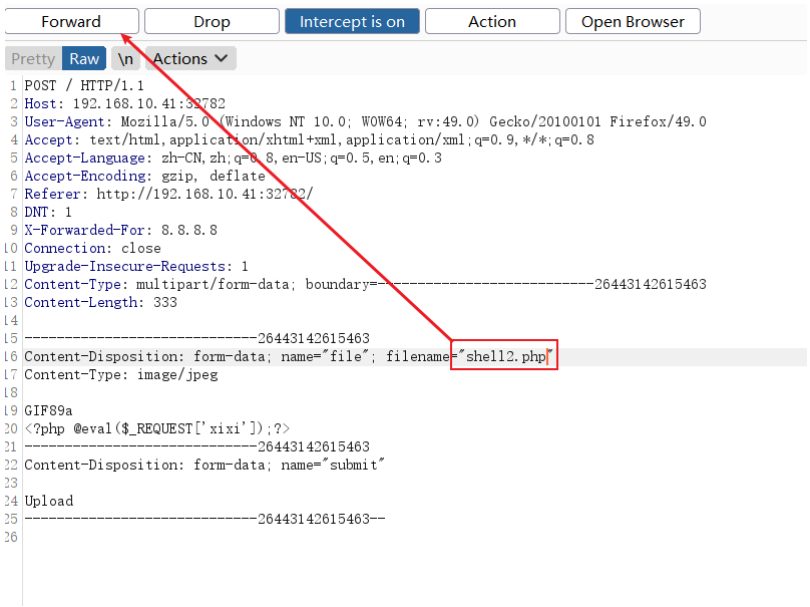
修改文件类型

1. 得知只允许上传`jepg jpg png gif`文件，在根据题目提示，应该是做了文件头校验。
2. 右键编辑`shell2.jpg`文件，添加gif文件头类型`GIF89a`



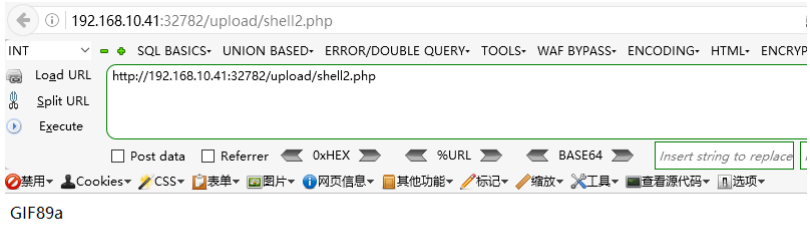
3. 再次上传，并使用Burp进行拦截。Burp成功拦截到请求。

4. 再次将`shell.jpg`修改为`shell.php`，点击`Forward`



5. 成功上传，右键复制文件地址。

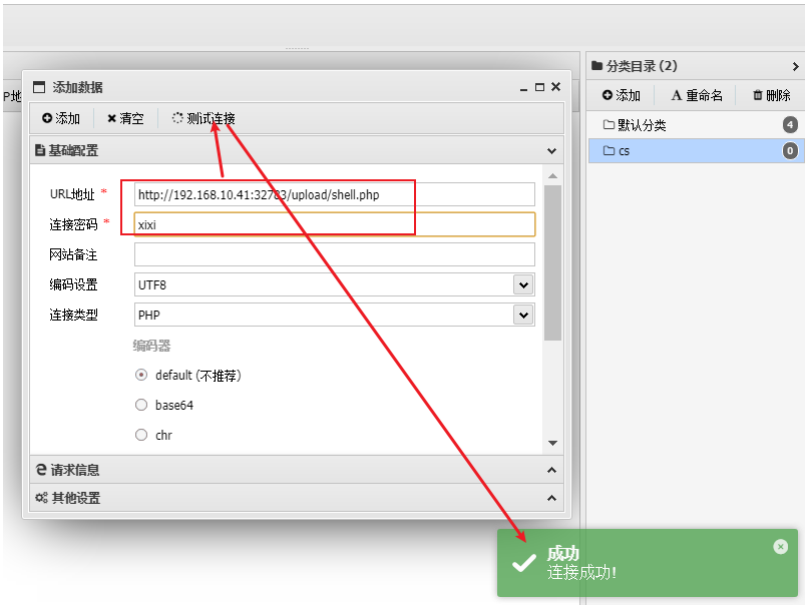
6. 访问文件地址，页面只显示了`GIF89a`，但是没用报错，使用蚁剑进连接木马。



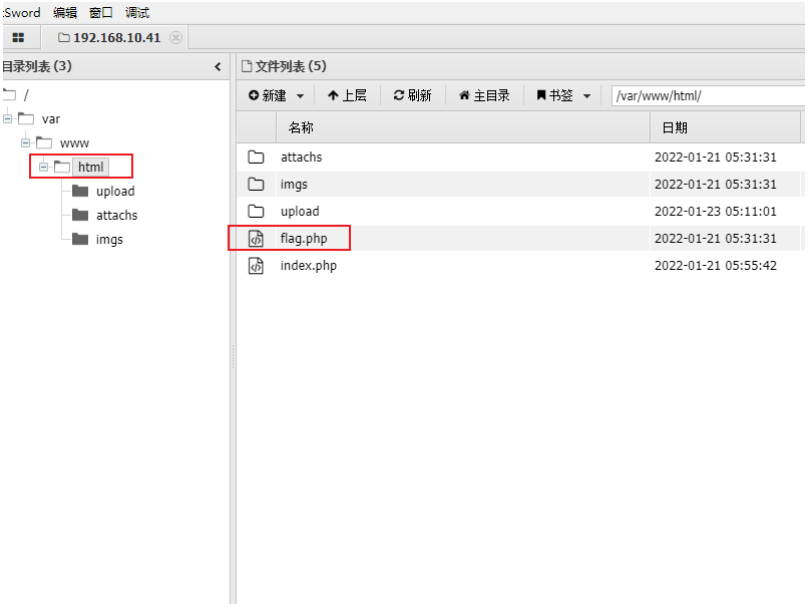
寻找Flag

步骤一：使用蚁剑连接php木马。

1. 打开蚁剑，右键空白处，点击添加数据。输入URL`http://192.168.10.41/upload/shell2.php`和密码`xixi`，点击测试连接，返回正常。



2. 点添加之后，右键文件管理。在 HTML 目录下找到了 flag.php 文件。



3. 双击 flag.php 文件，找到 flag{xxxxx}