xss challenges writeup

原创

tnt阿信 于 2018-03-21 16:53:29 发布 480 收藏 1
分类专栏： Web安全 文章标签： xss_challenges writeup

Stage#1

该题属于签到题，完全没有过滤任何东西，用户数入直接输出在了b标签中，但是有双引号包裹，所以我们只需要闭合双引号就行了
输入：

```
"<script>alert(document.domain)</script>
```

Stage#2

同样的这一题也属于没有过滤的，我们看下用户的输入被输出在了哪里，我随便输入一个数据（探子），查看下源代码：

可以看到输出在html属性中，这时候只需要闭合一下双引号就过了，构造：

```
"><script>alert(document.domain)</script>
" onmouseover="alert(document.domain)" x="等等
```

Stage #3

同样的先看下我们的输出都出现在了哪里，第一个是文本框的输出在b标签内，并被引号包裹起来了，还有一个输入就是我们的select,输出在b标签内，没有任何包裹。所以现在我们有两条路可以走：1.绕过双引号 2.修改select数据，提交我们想要的
通过输入，我发现双引号是被某种转义了，那么就采用第二方案吧，通过bp抓包修改第二个输入点的数据（如果不会抓包改数据的，请自行恶补）

Stage#4

乍一看怎么与第三题是一样的呢？仔细看源码我们发现，多了一个隐藏的input,而且改表单的value是hackme，这么嚣张，当然要试一下啦，于是老规矩，抓包，该数据，我们可以控制的就是这个value,由于这个input的type为hidden，所以我们平时经常用的触发时间的一些方法（onmouseover\onfous等）都不可行了，只有闭合整个标签了，于是就有了下面的poc

Stage #5

一开始输入数据时没看出什么端倪，但是当我准备写poc:"onmouseover=alert(document.domain)//时，却发现表单限制了maxlength,由于只是客户端的限制，所以很容易绕过（你懂我意思吧）抓包修改数据，写入我们的poc

Stage #6

这题就太简单了，看了下输出在input的value属性中，就直接看看能不能闭合双引号，输入双引号，发现居然没过滤，那我就直接输入："onclick=alert(document.domain)

Stage #7

这题还是比较有意思，如果不知道这个技巧的人可能完全过不了，因为这个是只有在ie浏览器才可以触发的，而且很怪异，在ie两个反引号可以闭合双引号的html属性,（这道题的双引号与<>都是被过滤了的）构造：‥onclick=alert(document.domain)//

> 注：要在ie下，本人亲测有效

Stage #8

这题也属于比较简单的，因为实在url中嘛，我们可以使用伪协议javascript，来写js语句，输入：
javascript:alert(document.domain)

Stage #9

这一题我觉得对我来说算是直接没见过的类型了，虽然根据源代码可以判断，大概是与编码有关的，因为有一个input和编码有关嘛

看了下别人的writeup,原来有一种东西叫做utf7编码，这种编码方式，由源码可以知道我们可以控制页面的编码，那么我们可以通过指定utf7编码来绕过服务端的过滤。
通过抓包修改数据：
p1=1%2bACI- onmouseover=%2bACI-alert(document.domain)%2bADsAIg- x=%2bACI-&charset=UTF-7
Stage #10
这一关还是挺简单的，根据几次输入，我们发现domain被替换为空了，那么只需要这样：document.dodomainmain
这样，当domain被替换掉后，又会新拼接成一个domain

> 每天进步一点点