pentesterlab xss(writeup)

原创

tnt阿信 于 2018-04-03 20:30:49 发布 1437 收藏

分类专栏： Web安全 文章标签： pentesterlab xss

本文链接：https://blog.csdn.net/he_and/article/details/79798958

example1

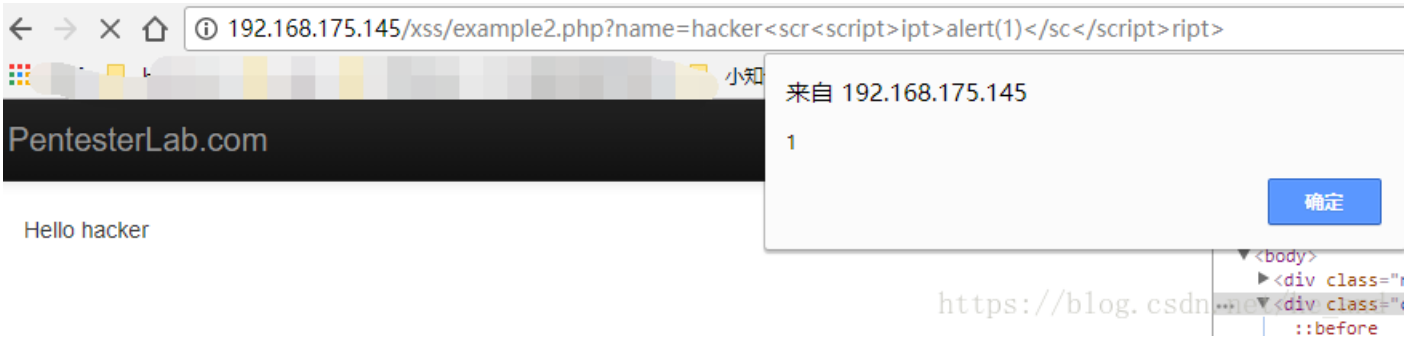
第一题往往都是热身题，没有任何的过滤。通过查看源码发现我们输入的内容时直接输出在html标签之间的，所以直接插入：

```
<script>alert(1)</script>
```

> 注：这里我自己一直有一个误区，今天偶然看到一篇文章才发现，原来审查元素看到的并不是源代码，之前一直是这样查看源码的,有时候会有一些差异，因为源码是我们直接从服务器取过来的代码，没有经过任何js加工渲染，但是审查元素看到的就是经过渲染过后的代码呈现。

example2

同样的输出位置，这次我还是先尝试使用`<script>alert(1)</script>`进行测试。但是发现`<script>`与`</script>`都被过滤了，预测后台使用正则把这两个标签进行了替换，把他们都替换为空，那么绕过姿势也就很简单：



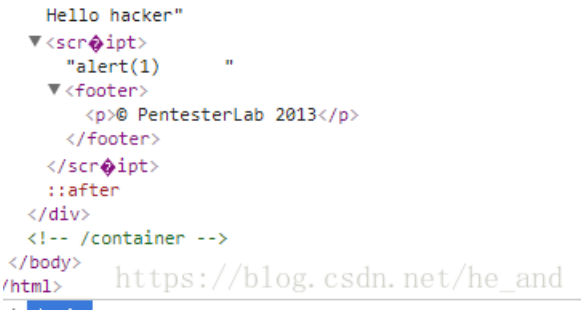
补充：后来经过测试，后台的正则匹配应该只是匹配了小写，所以我们同样可以使用大小写混合来绕过：`<scriPt>alert(1)</scRipt>`,当然这并不意味着没有其它的方式了，当然可以借助一些其它的标签进行绕过，例如：`<img><input>`之类的。

example3

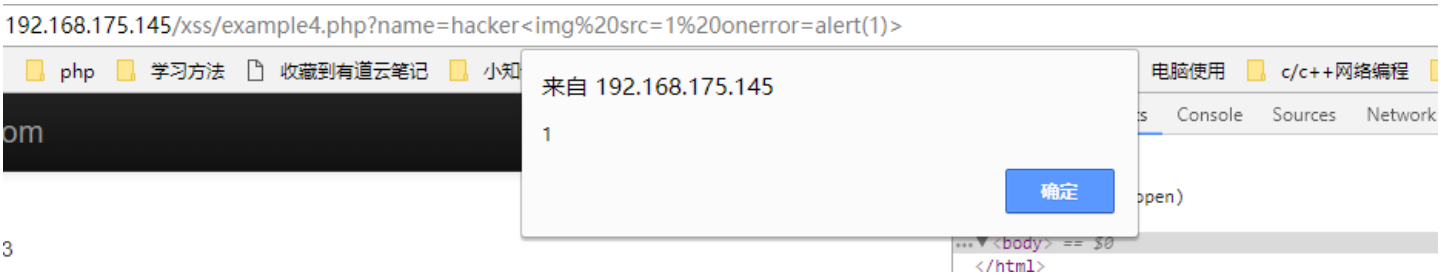
可以使用与example2第一种策略进行绕过。

example4

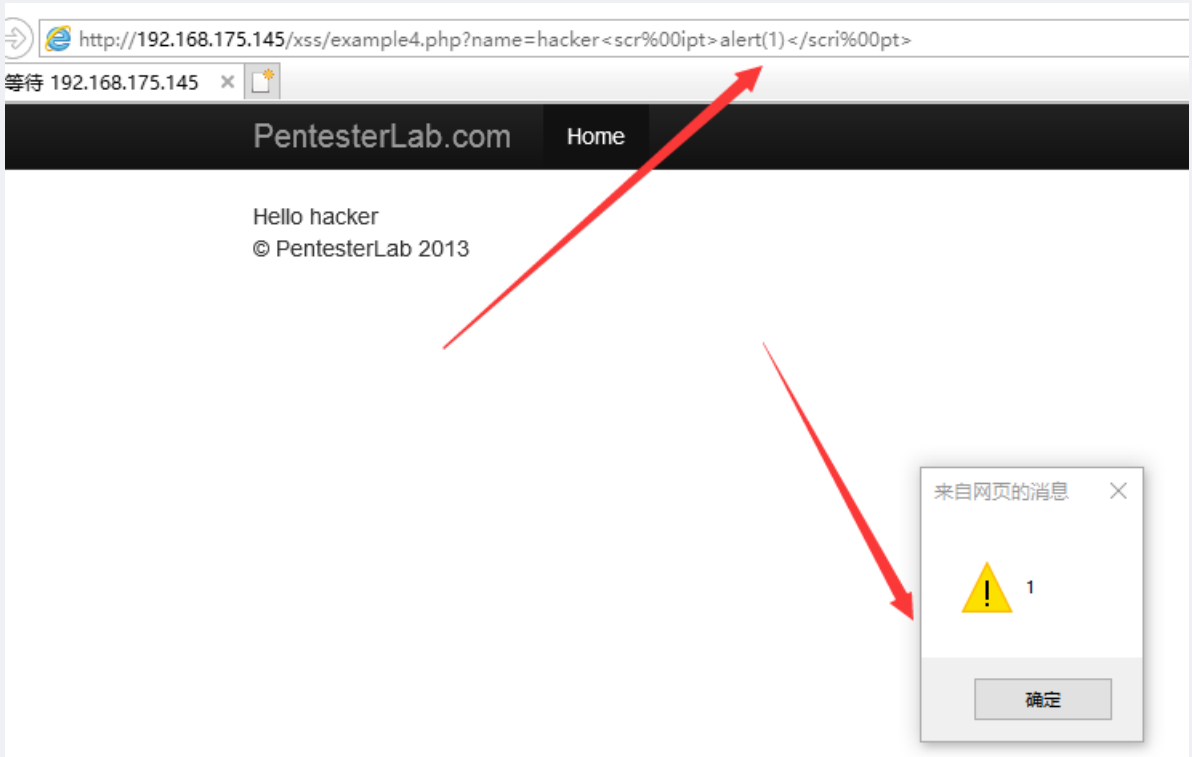
这次是过滤了script(SCRIPT)这几个字母，当然还是可以用其它标签来绕过，不顾我也尽量想了想其它办法，比如通过在script这几个字母之间插入一些浏览器能够解析的字符，比如我们可以将`<script>`改为`<scr%00ipt>`，不顾哦我测试了一下，却出现了奇怪的事情：



我有点不懂这是什么情况，可能是由于浏览器识别不了这个script标签，也可能是做了什么其它过滤，希望大佬看到答疑解惑。我还是老老老实实用其它标签x一下吧：`<img src=1 alert(1)>`



补充：我就记得这道题是可以通过我说的那种方式绕过的，但是值适用于ie浏览器，我们可以试试：



example5

这次是过滤了alert,一旦出现了alert，页面就会显示error,但是这个过滤也太脑残了吧，我们可以用prompt(1),与confirm(1)来弹窗。

example6

这次我们的输入作为js变量的值，就需要绕过双引号。而且又没有过滤双引号：

```
"
<script>
    var $a= "hacker111";alert(1);//";
</script> == $0
▶<footer>…</footer>
```

就这样…

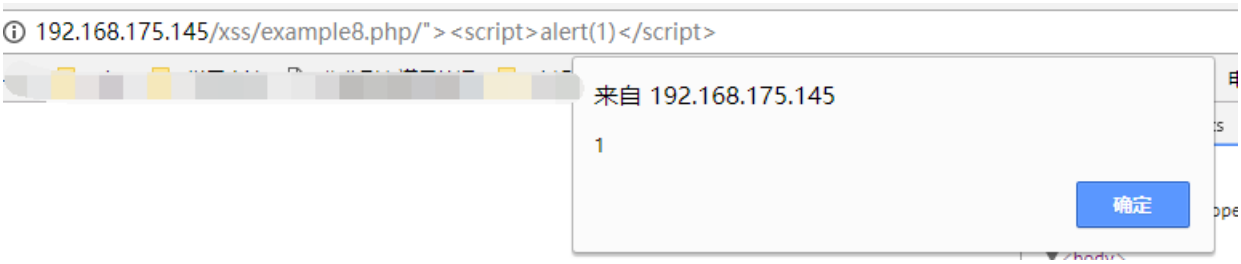
example7

就把上一次的双引号改为单引号：

```
<script>
    var $a= 'hacker';alert(1)//';
</script>
```

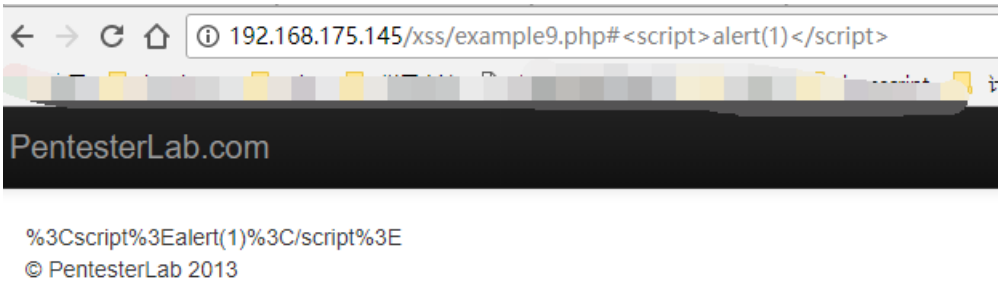
example8

这一题我没做出来，主要是思维被前面的题限制住了，只是局限在了表单的数入上面了，完全忽略了其它部分，表单部分经过了严格的html编码，目前我想不到什么姿势可以绕过，但是看了别人的wp才发现自己忽略了url，表单部分的action应该是这么写的：`$_SERVER[PHP_SELF]`,这样我们可以通过闭合form表单来绕过：



example9

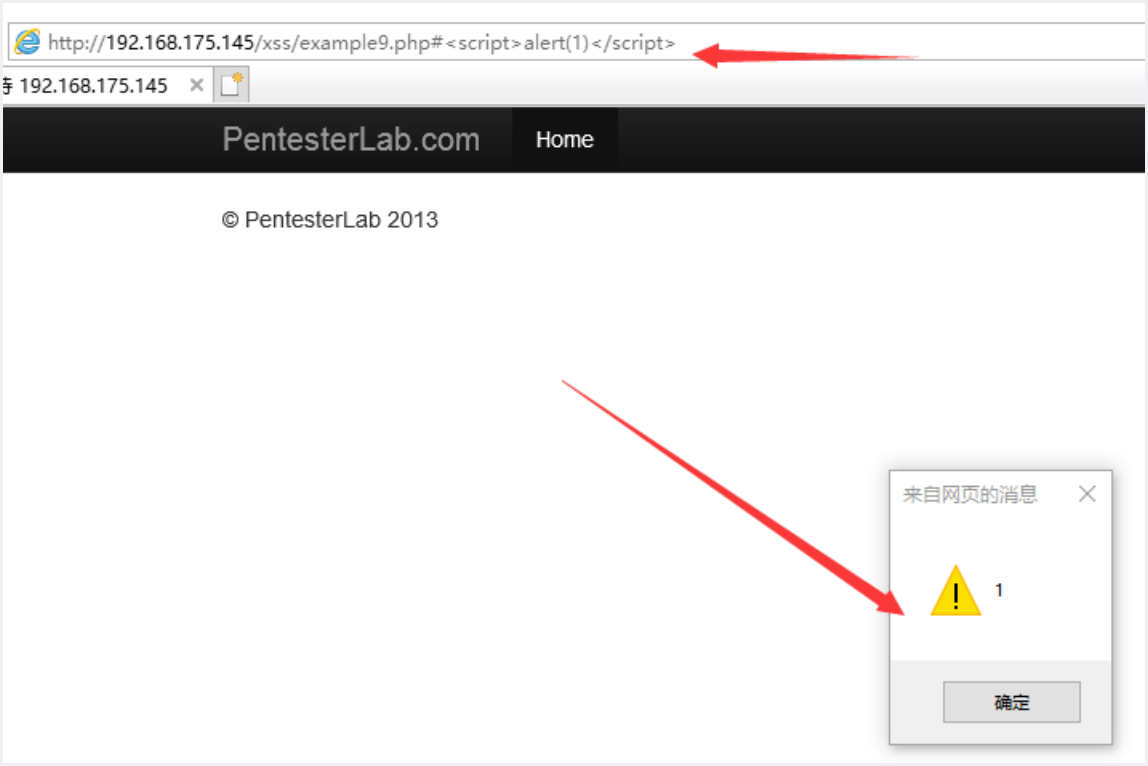
第九题是我最困惑的，根据源代码：`document.write(location.href.substring(1))`，这是直接将锚点的内容输出在了页面中啊，讲道理是很简单的，但是，但是，我居然过不了，我构造了：`<script>alert(1)</script>`,却发现被转义了，结果如下：



%3Cscript%3Ealert(1)%3C/script%3E
© PentesterLab 2013

，居然被url转义了， 反正我通过各种编码是没有绕过的。但是官方的答案给的就是：`<script>alert(1)</script>`,大家试试吧，可能与浏览器版本有关吧

注：说一点比较重要的吧，今天拜读《web前端黑客技术揭秘》，看到了不通浏览器的url编码差异，而这一题就涉及到这一不同浏览器的特性，这里我一开始没有成功弹窗就是因为chrome与firefox编码了<>这两个特殊符号，当时就是没有测试ie,今天特地测试了一下，成功弹窗：



可以说是相当刺激了，又涨姿势了

小结

虽然这些题目相对来说比较简单，但是很有拓展性。