

ctf xss注入

LemonSec 2020-06-16 09:49:03

xss注入

这里有两种方法

1.比较耍赖的方法

Challenge

56 Solves



XSS1

50

<http://206.189.214.99:4080/xss/>

就在当前目录下，不要扫，没东西，成功alert弹窗就过了

Flag

Submit



微信号: lemon-sec

打开网址



我们右键，f12。都会收到提示。并且不会执行。
我们直接去设置里找web开发者查看源代码。

```

4         confirm("此路不通!!!");
5     }
6 }
7 if (document.layers) {
8     document.captureEvents(Event.MOUSEDOWN);
9 }
10 document.onmousedown = click;
11 document.oncontextmenu = new Function("return false;")
12 document.onkeydown = document.onkeyup = document.onkeypress = function () {
13     if (window.event.keyCode == 123 || window.event.keyCode == 17) {
14         confirm("不让你用F12和Ctrl!!!");
15         window.event.returnValue = false;
16         return (false);
17     }
18 }
19 // <--123——112是F1-F12的代码数-->
20 window.alert = function()
21 {
22     confirm("恭喜你成功弹窗, d0g3{xss_is_easy}");
23 }
24 </script>
25 <title>欢迎来到d0g3 xss</title>
26 </head>
27 <body>
28 <h1 align=center>d0g3 xss</h1>
29 <h2 align=center>没有找到和相关的结果.</h2><center>
30 <form action=index.php method=GET>
31 <input name=keyword value="">
32 <input type=submit name=submit value="搜索"/>
33 </form>
34 </center><center><img src=logo.jpg></center>
35 <center>记得闭合标签, chrome内核浏览器 (国内的qq, 360等浏览器用的也是chrome内核) 有
36 <h3 align=center>payload的长度:0</h3></body>
37 </html>
38

```

被标注出来的字就是我们要的flag。

2.题目告诉我们alert弹窗就会成功。
所以我们需要想办法让含有图片的那个界面弹窗。
我们先去web开发者选项中找到控制台。

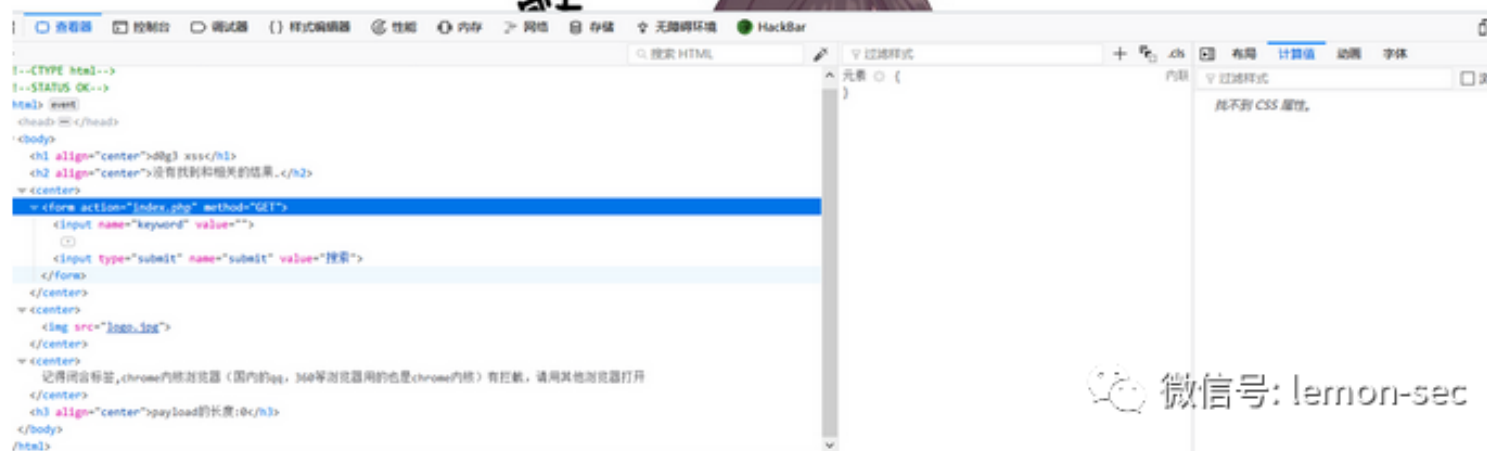
微信号: lemon-sec

d0g3 xss

没有找到和相关的结果.

form 1503.2 + 22.4

搜索



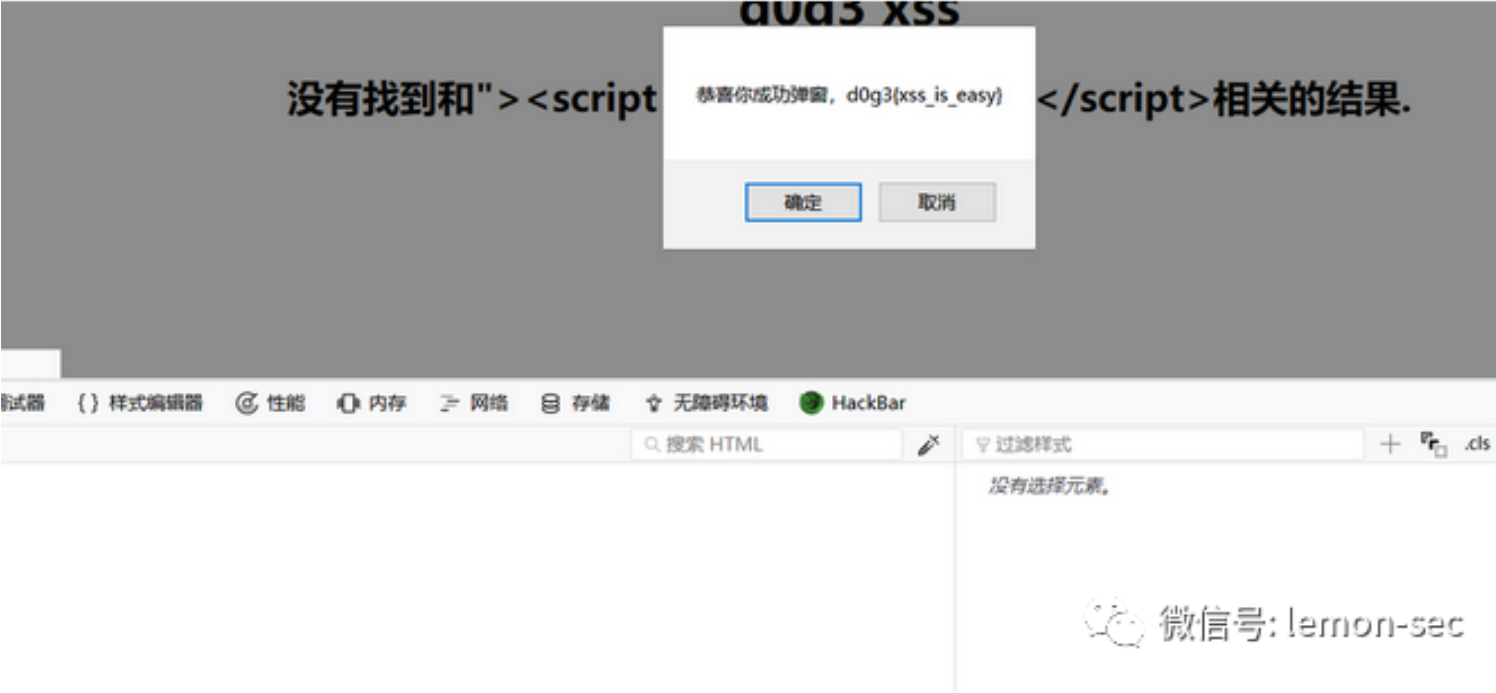
微信号: lemon-sec



微信号: lemon-sec



这个时候我们就会看到value里有123。
所以我们要想办法插入Javascript 中的 alert () 函数使其弹框。只要弹框我们就会得到我们想要的东西。能输入的地方只有白框内。
我们会用到<script></script>标签。也就是我们需要闭合标签。
<inputname="keyword"value=" ">
我们输入的东西在value的双引号里，首先闭合标签。
"><script>alert (2312313135)</script>



转载链接: <https://www.jianshu.com/p/576694d0d29f>

图表分析 LemonSec

公众号文章

换一批

ctf xss注入

微信原文链接

LemonSec

xss game挑战笔记

微信原文链接

LemonSec