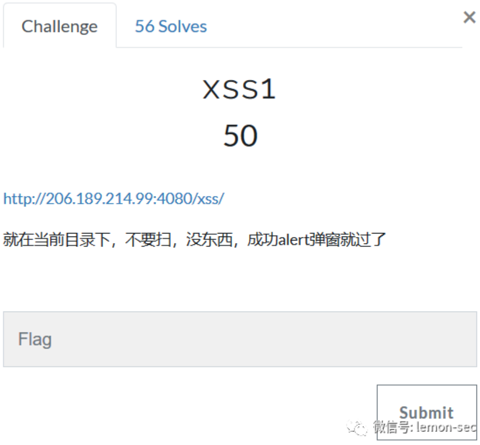
xss 注入

这里有两种方法

1.比较要赖的方法



XSS1

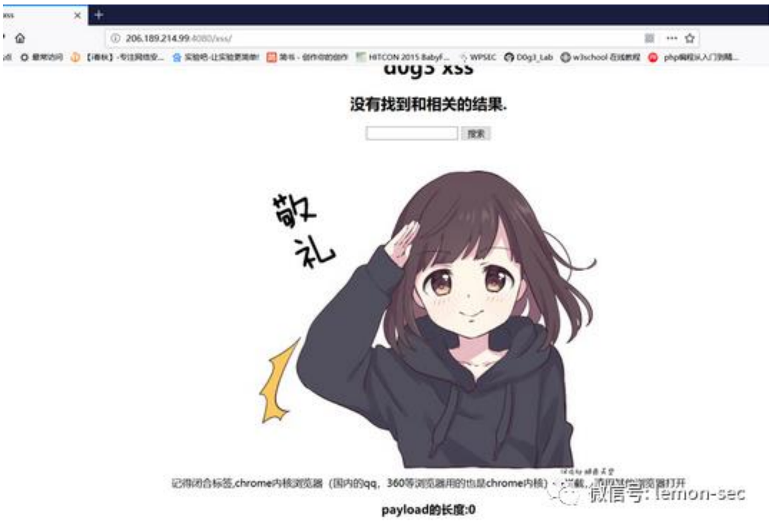
50

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

http://206.189.214.99:4080/xss/

打开网址



206.189.214.99:4080/xss/

d0g3 xss

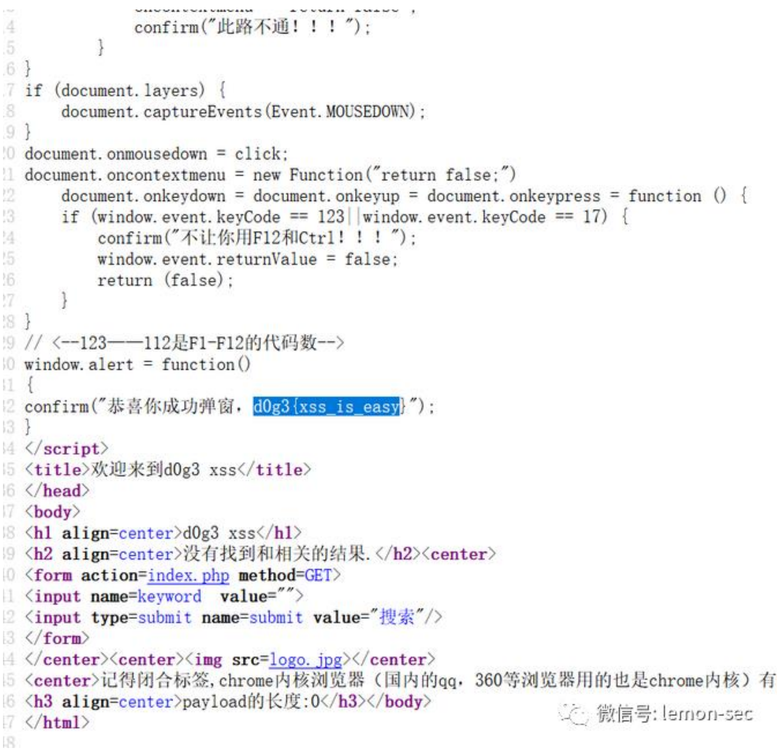
没有找到和相关的结果.

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）...请用其他浏览器打开

payload的长度:0

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。

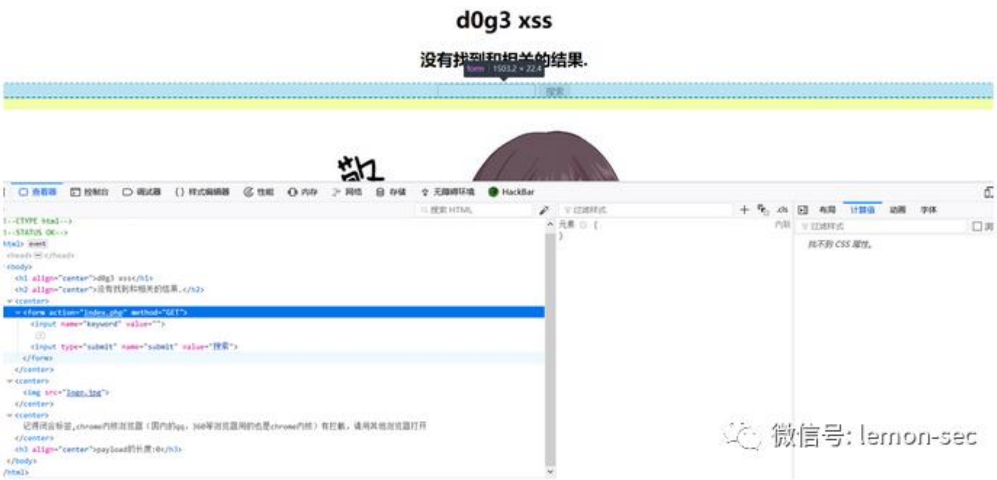


```
            confirm("此路不通！！！");
        }
}
if (document.layers) {
    document.captureEvents(Event.MOUSEDOWN);
}
document.onmousedown = click;
document.oncontextmenu = new Function("return false;")
    document.onkeydown = document.onkeyup = document.onkeypress = function () {
    if (window.event.keyCode == 123||window.event.keyCode == 17) {
        confirm("不让你用F12和Ctrl！！！");
        window.event.returnValue = false;
        return (false);
    }
}
// <--123——112是F1-F12的代码数-->
window.alert = function()
{
confirm("恭喜你成功弹窗，d0g3{xss_is_easy}");
}
</script>
<title>欢迎来到d0g3 xss</title>
</head>
<body>
<h1 align=center>d0g3 xss</h1>
<h2 align=center>没有找到和相关的结果.</h2><center>
<form action=index.php method=GET>
<input name=keyword  value="">
<input type=submit name=submit value="搜索"/>
</form>
</center><center><img src=logo.jpg></center>
<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
<h3 align=center>payload的长度:0</h3></body>
</html>
```

被标注出来的字就是我们要的 flag。

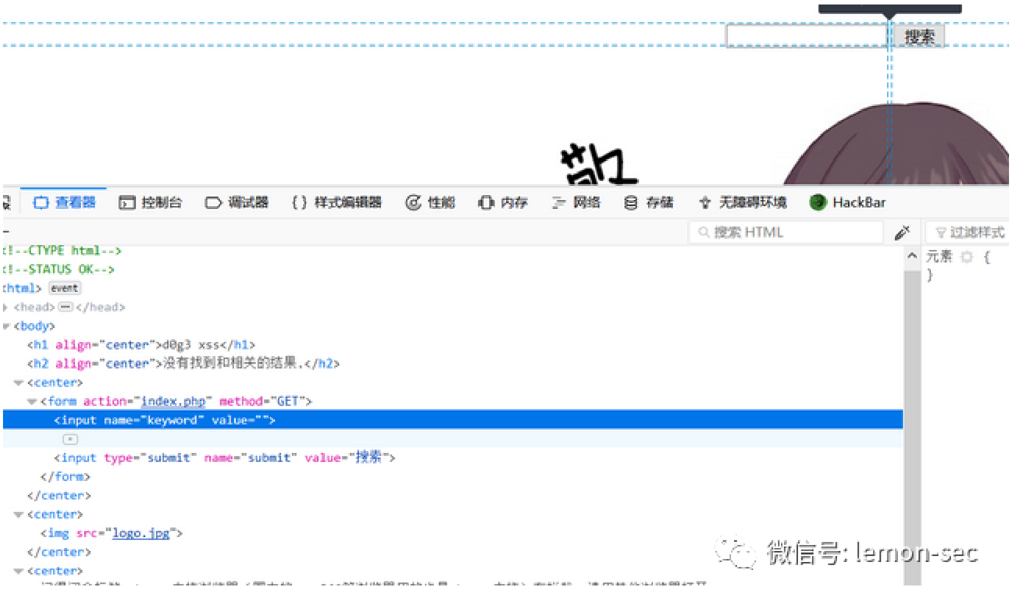
2.题目告诉我们 alert 弹窗就会成功。

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。



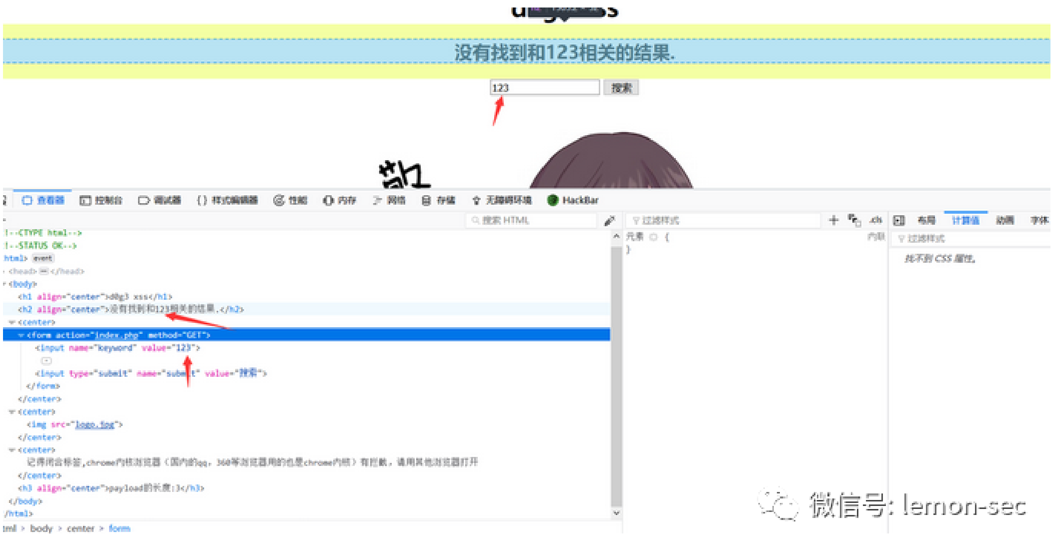
```
<!--CTYPE html-->
<!--STATUS OK-->
<html> event
  <head> </head>
  <body>
    <h1 align="center">d0g3 xss</h1>
    <h2 align="center">没有找到和相关的结果.</h2>
    <center>
      <form action="index.php" method="GET">
        <input name="keyword" value="">
        
        <input type="submit" name="submit" value="搜索">
      </form>
    </center>
    <center>
      <img src="logo.jpg">
    </center>
    <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）有拦截，请用其他浏览器打开
    </center>
    <h3 align="center">payload的长度:0</h3>
  </body>
</html>
```

我们同样可已看到源代码，这时我们需要在空白框里做文章。



```
<!--CTYPE html-->
<!--STATUS OK-->
<html> event
  <head> </head>
  <body>
    <h1 align="center">d0g3 xss</h1>
    <h2 align="center">没有找到和相关的结果.</h2>
    <center>
      <form action="index.php" method="GET">
        <input name="keyword" value="">
        
        <input type="submit" name="submit" value="搜索">
      </form>
    </center>
    <center>
      <img src="logo.jpg">
    </center>
    <center>
```

每当我们向白框输入东西的时候，总会返回我们输入的东西。



没有找到和123相关的结果.

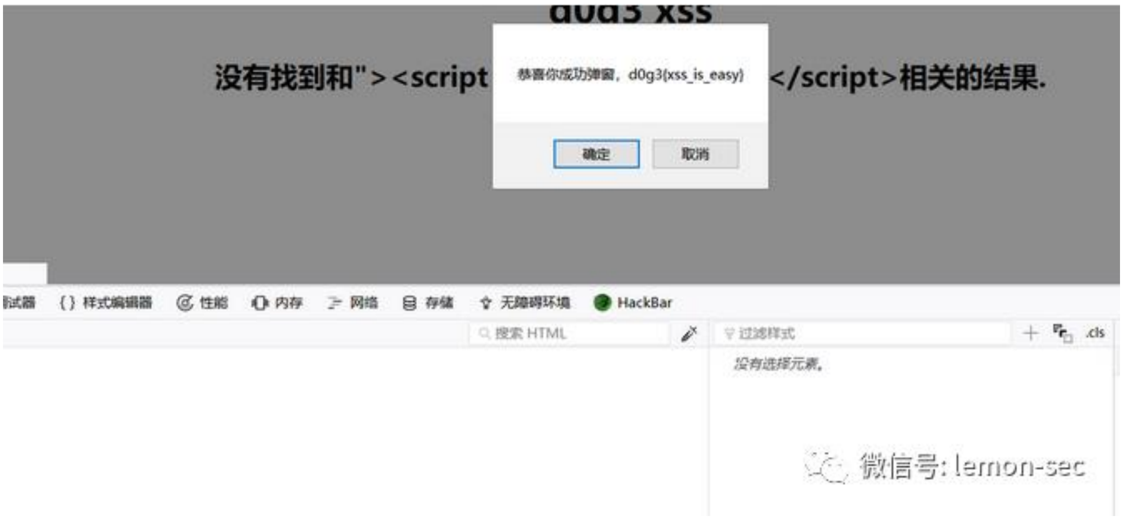
```
!--CTYPE html-->
!--STATUS OK-->
html>
<head>…</head>
<body>
  <h1 align="center">d0g3 xss</h1>
  <h2 align="center">没有找到和123相关的结果.</h2>
  <center>
    <form action="index.php" method="GET">
      <input name="keyword" value="123">
      <input type="submit" name="submit" value="搜索">
    </form>
  </center>
  <center>
    <img src="logo.jpg">
  </center>
  <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）有拦截，请用其他浏览器打开
  </center>
  <h3 align="center">payload的长度:3</h3>
</body>
/html>
```

这个时候我们就会看到 vlaue 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。

<input name="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>



没有找到和"><script 恭喜你成功弹窗，d0g3{xss_is_easy} </script>相关的结果.

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