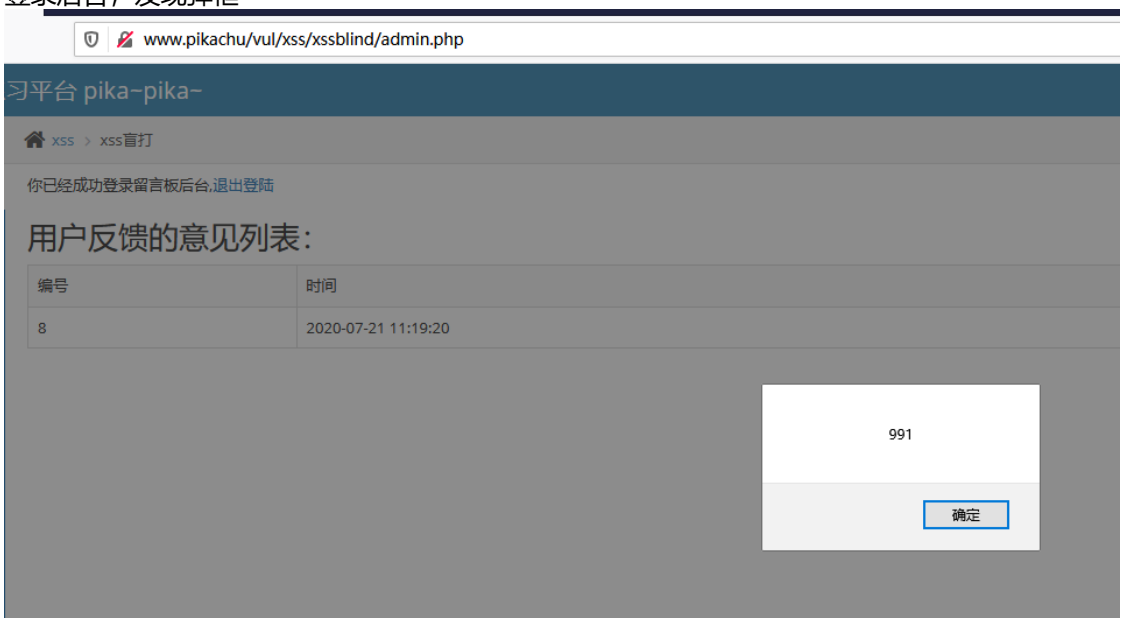
20200721信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/7/21 10:17	**更新时间:**	2020/7/21 23:34
作者:	820410740@qq.com		

XSS盲打

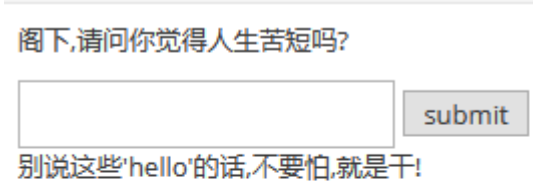
提交xss代码后，不会在前端输出，我们无法判断是否存在xss，我们对文本框进行插入弹窗代码。

登录后台，发现弹框



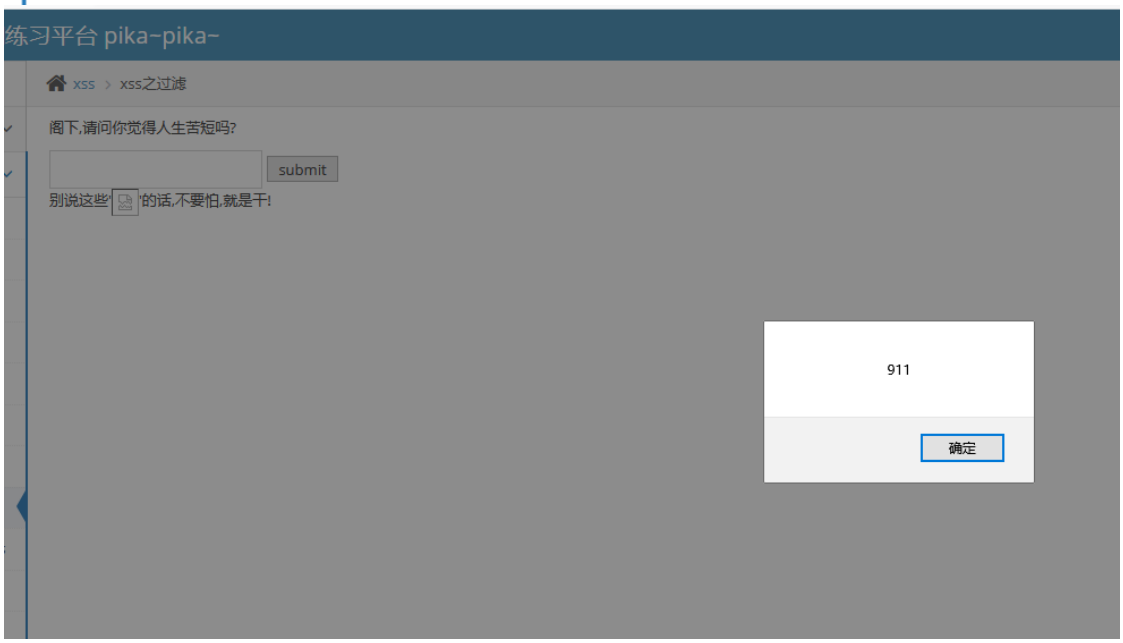
XSS过滤

首先随意输入，观察输出结果



发现会将输入直接输出
尝试进行弹窗

发现输出结果为'>'，考虑到可能是'>'前的字符被过滤
尝试使用事件型弹窗



成功弹窗
查看源码

```
17
18
19  $html = '';
20  if(isset($_GET['submit']) && $_GET['message'] != null){
21      //这里会使用正则对<script进行替换为空,也就是过滤掉
22      $message=preg_replace('/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/', '', $_GET['message']);
23      if($message == 'yes'){
24          $html.="<p>那就去人民广场一个人坐一会儿吧!</p>";
25      }else{
26          $html.="<p>别说这些'{$message}'的话,不要怕,就是干!</p>";
27      }
28
29  }
30
```

可以看出，该源码将<script全部过滤

三种方法绕过
1.大小写绕过 一般是script大小写，alert()不能大小写转换
2.事件型绕过
3.编码绕过，xss过滤时可以使用字符的另一种编码形式绕过，一般使用十六进制编码