

光棍节程序员闯关秀writeup

转载

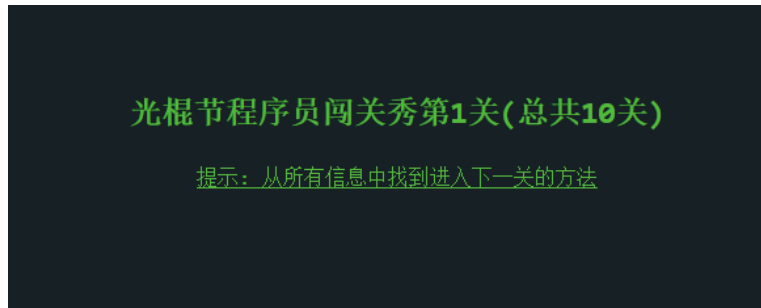
[weixin_30765577](#) 于 2017-07-22 11:49:00 发布 82 收藏

原文链接: <http://www.cnblogs.com/hongren/p/7220829.html>

版权

答题链接<https://1111.segmentfault.com/>

第一关



首先当然是右键查看源码啊

```
<html>
<head><title>光棍节程序员闯关秀第1关(总共10关)</title></head>
<body style="background: #172024; color: #54BA3E; font: 100%/1.5 Menlo, Consolas, Courier, monospace; tex
<h2>光棍节程序员闯关秀第1关(总共10关)</h2>
<u>提示: 从所有信息中找到进入下一关的方法</u>
<p><a style="color: #172024" href="?"k=c91c109023faa8f606b10a76d03fffe4">进入下一关</a></p>
</body>
</html>
```

点击链接进入下一关

第二关



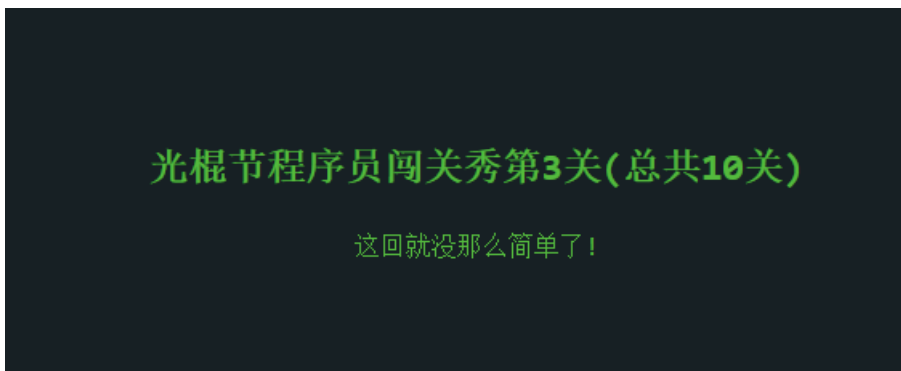
还是老样子, 右键查看源码

```
1 <html>
2 <head><title>光棍节程序员闯关秀第2关(总共10关)</title></head>
3 <body style="background: #172024; color: #54BA3E; font: 100%/1.5 Menlo, Consolas, Courier, 1
4 <h2>光棍节程序员闯关秀第2关(总共10关)</h2>
5 <!-- 不错嘛,密码在此:f715152c50fd784b3d72113180a0716e -->
6 <!-- 强插广告: 欢迎访问 http://segmentfault.com 或者 http://sf.gs -->
7 <p>密码在哪呢?</p>
8 <form><input autocomplete="off" placeholder="输入密码" name="k" /></form>
9 <p><a style="color: #172024" href="javascript:alert('你太天真了');">进入下一关</a></p>
0 </body>
1 </html>
```

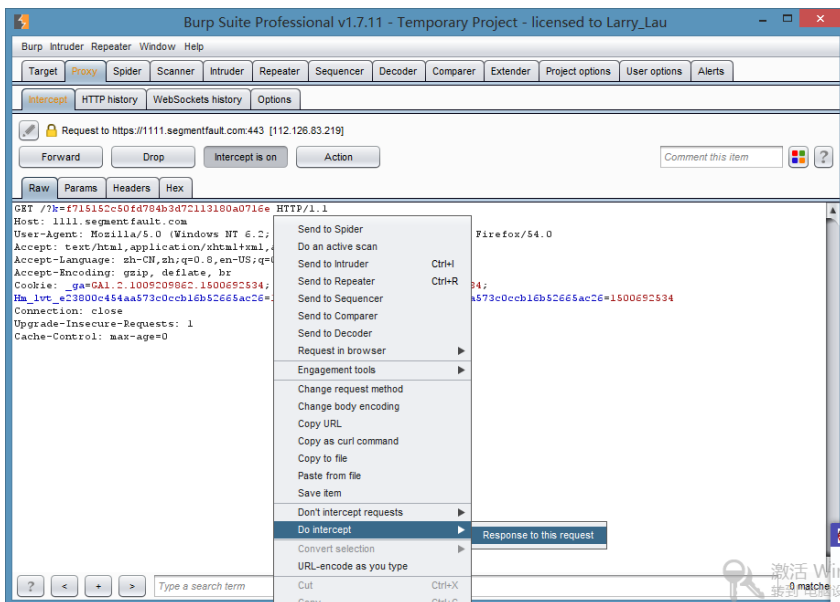
这个key是要放在URL链接里敲回车的

第三关

根据前两关这个难度，第三关估计在请求头或者响应头里，先开burp



刷新，拦截返回包



```
HTTP/1.1 200 OK
Date: Sat, 22 Jul 2017 03:17:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
The-Key-Is: 87ff679a2f3e71d9181a67b7542122c
X-Hit: sf-web2
Content-Length: 336
```

拿到flag

第四关

光棍程序员闯关秀第4关(总共10关)

观察你密码的规律

根据前几次规律，都是在改k的参数

<https://1111.segmentfault.com/?k=a87ff679a2f3e71d9181a67b7542122c>

对他进行MD5解码

a87ff679a2f3e71d9181a67b7542122c 查询

该数据已破解成功!
密文: a87ff679a2f3e71d9181a67b7542122c
明文: 4
数据来源: admin
用时: 00:00:00.3783139

明文是4，这又是第4关，猜测第五关是5的MD5

5 查询

md5(5,32) = e4da3b7fbbce2345d7772b0674a318d5
md5(5,16) = bbce2345d7772b06

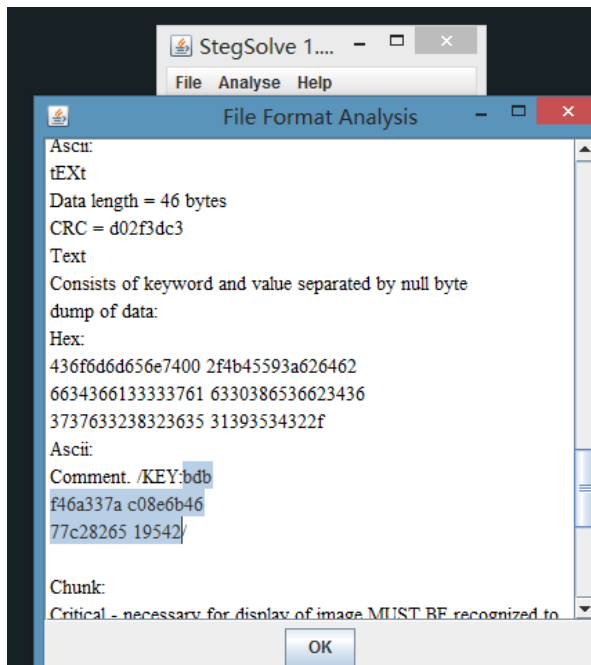
第五关

光棍节程序员闯关秀第5关(总共10关)



扫码，发现什么都没有

难倒是图片隐写术？上工具



得到key

第六关

光棍节程序员闯关秀第6关(总共10关)

f4de502e58723e6252e8856d4dc8fc3b, 只能告诉你这么多

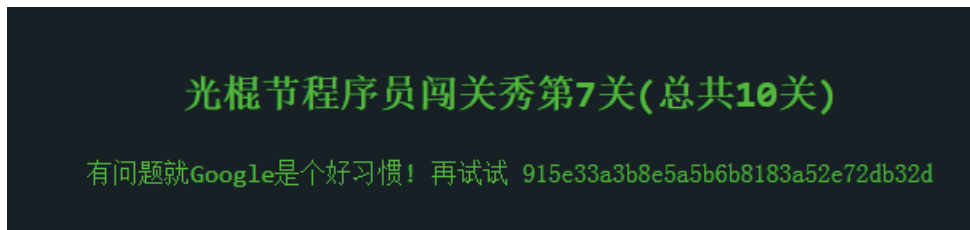
给我的感觉是MD5，但是MD5已经玩过了，扔到百度搜一下

哇，还排在第一个

[高阳Sunny:google 你丫什么时候...](#)

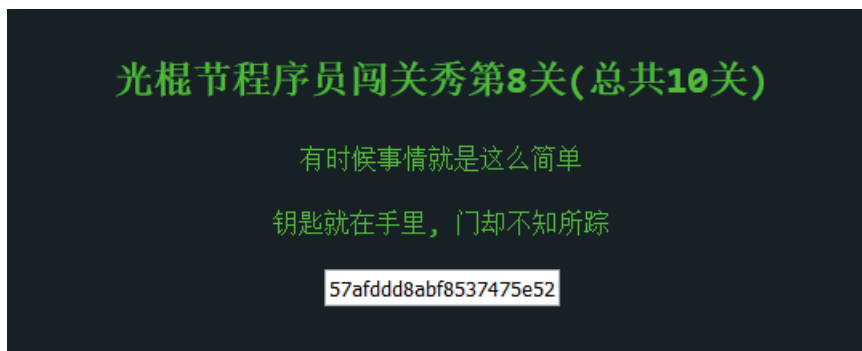
2012年11月8日 - 高阳Sunny:google 你丫什么时候能收录,title: f4de502e58723e6252e8856d4dc8fc3b key: 1573402aa6086d9ce42cfd5991027022腾讯微博,与其在别处仰望不...
t.qq.com/p/t/169307017... ▾ Vi - 百度快照

第七关



放到google没结果，放到url里直接过了，这个题是没处理好？

第八关



审查元素

```
<body style="background: #172024; color: #548A3E; font: 100%/1.5 Menlo, C..., Courier, mono" data-bbox="52 563 685 660">
  <h2>光棍节程序员闯关秀第8关(总共10关)</h2>
  <p>有时候事情就是这么简单</p>
  <p>钥匙就在手里，门却不知所踪</p>
  <form method="GET" data-bbox="52 613 685 660">
    <input name="k" value="57afddd8abf8537475e52e1d2119f1fd" type="text" data-bbox="52 625 685 645"/>
  </form>
</body>
```

没有提交按钮

手动帮忙post

```
POST /?k=915e33a3b8e5a5b6b8183a52e72db32d HTTP/1.1
Host: 1111.segmentfault.com
User-Agent: Mozilla/5.0 (Windows NT 6.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Cookie: __ga=GAI.2.1008209862.1500692534; __gid=GAI.2.1411692174.1500692534;
Hm_lvt_e23800c454aa573c0ccb16b52665ac26=1500692534; Hm_lpv_e23800c454aa573c0ccb16b52665ac26=1500692534
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

k=57afddd8abf8537475e52e1d2119f1fd
```

第九关

好吧我承认这一关我看了writeup

因为是光棍节，所以要把_都替换成1，然后转为byte然后转为ASCII码，是base64加密的，再解密为tar.gz文件，解压出来一张老师的图片。

然后通关

转载于:<https://www.cnblogs.com/hongren/p/7220829.html>