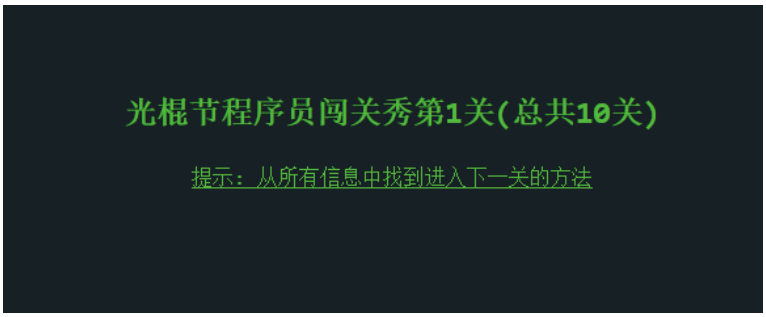
光棍节程序员闯关秀writeup

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

答题链接https://1111.segmentfault.com/

第一关



首先当然是右键查看源码啊

```
<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

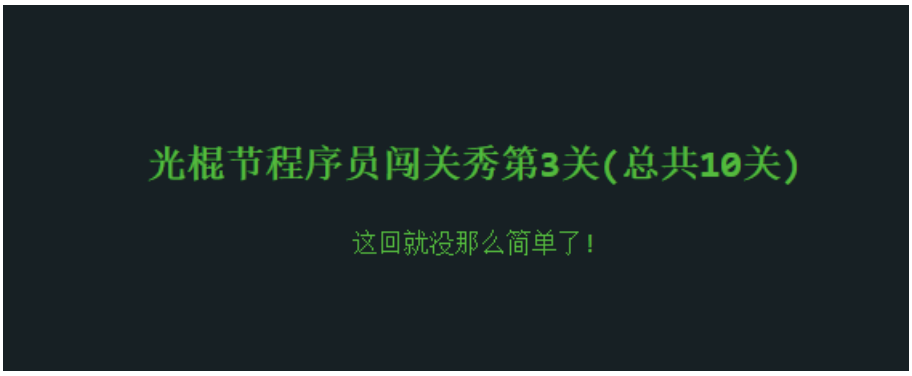
还是老样子，右键查看源码

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

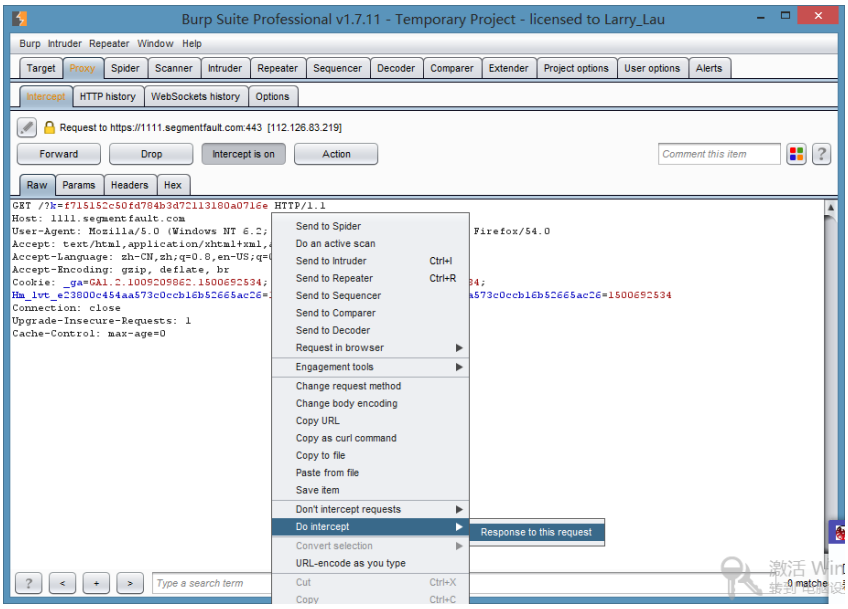
这个key是要放在URL链接里敲回车的

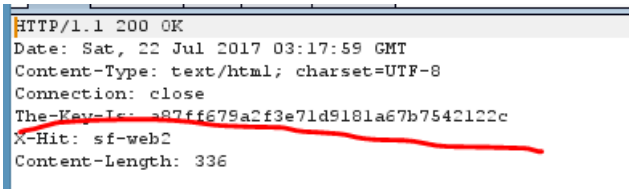
第三关

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

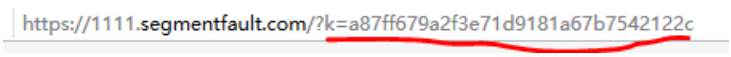




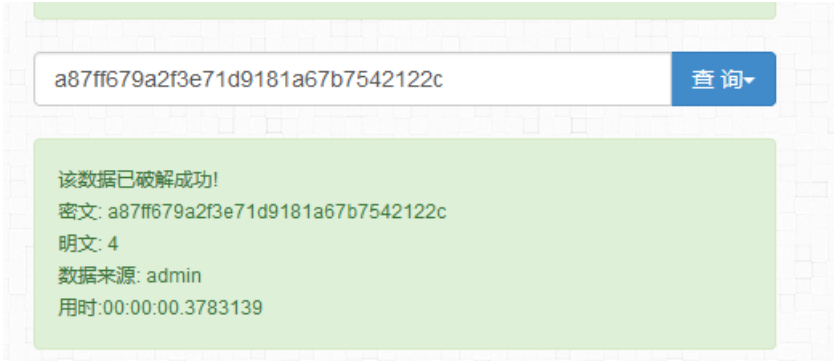
拿到flag

第四关

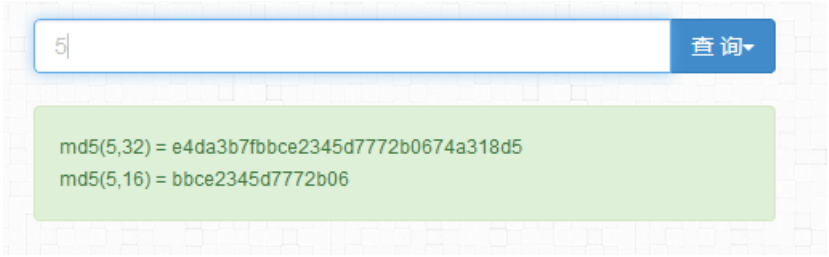
根据前几次规律，都是在改k的参数



对他进行MD5解码



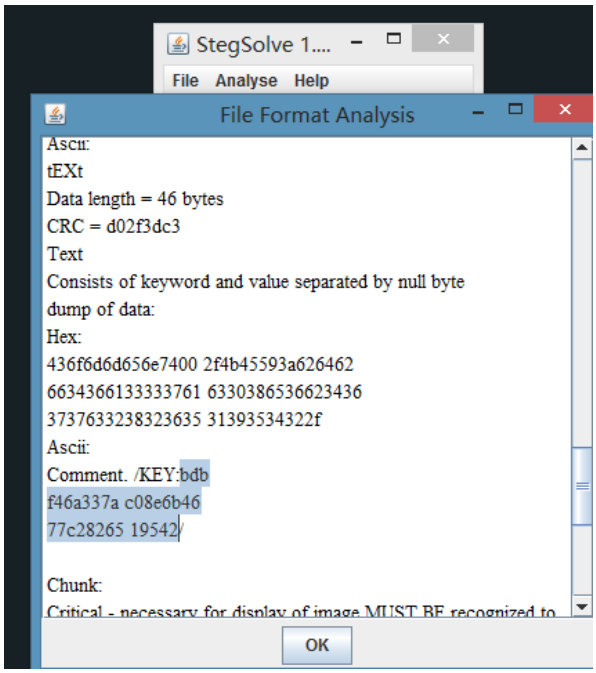
明文是4，这又是第4关，猜测第五关是5的MD5



第五关

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

给我的感觉是MD5，但是MD5已经玩过了，扔到百度搜一下

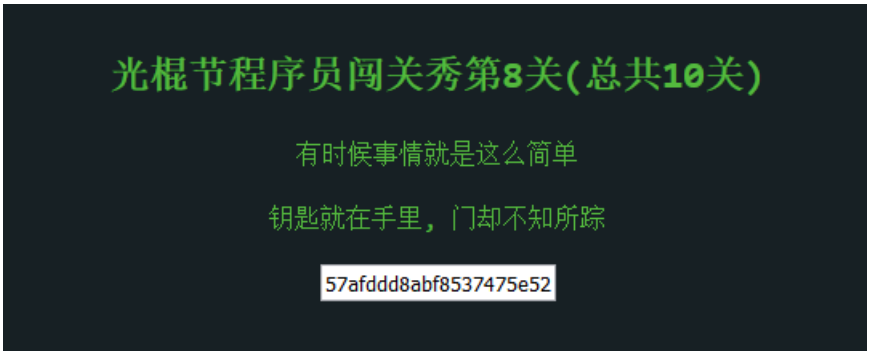
哇，还排在第一个

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: f4de502e58723e6252e8856d4d c8fc3b key: 1573402aa6086d9ce42cfd5991027022腾讯微博,与其在别处仰望 不...
t.qq.com/p/t/169307017... V1 - 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

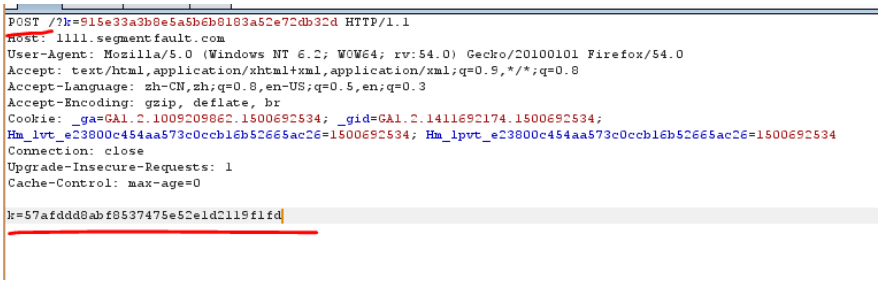


审查元素

```
<body style="background: #172024; color: #54BA3E; font: 100%/1.5 Menlo, C…, Courier, mono
  <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">
    <input name="k" value="57afddd8abf8537475e52e1d2119f1fd" type="text">
  </form>
</body>
```

没有提交按钮

手动帮忙post



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