BUGKU_CTF WEB(10-19)writeUP

原创

程序小黑 于 2018-10-20 08:41:36 发布 45739 收藏 8

分类专栏： 网络安全 WEB 网络空间安全 文章标签： 网络安全 WEB

本文链接：https://blog.csdn.net/qq_27180763/article/details/83210556

网络安全 同时被 3 个专栏收录

77 篇文章 3 订阅

订阅专栏

WEB

12 篇文章 1 订阅

订阅专栏

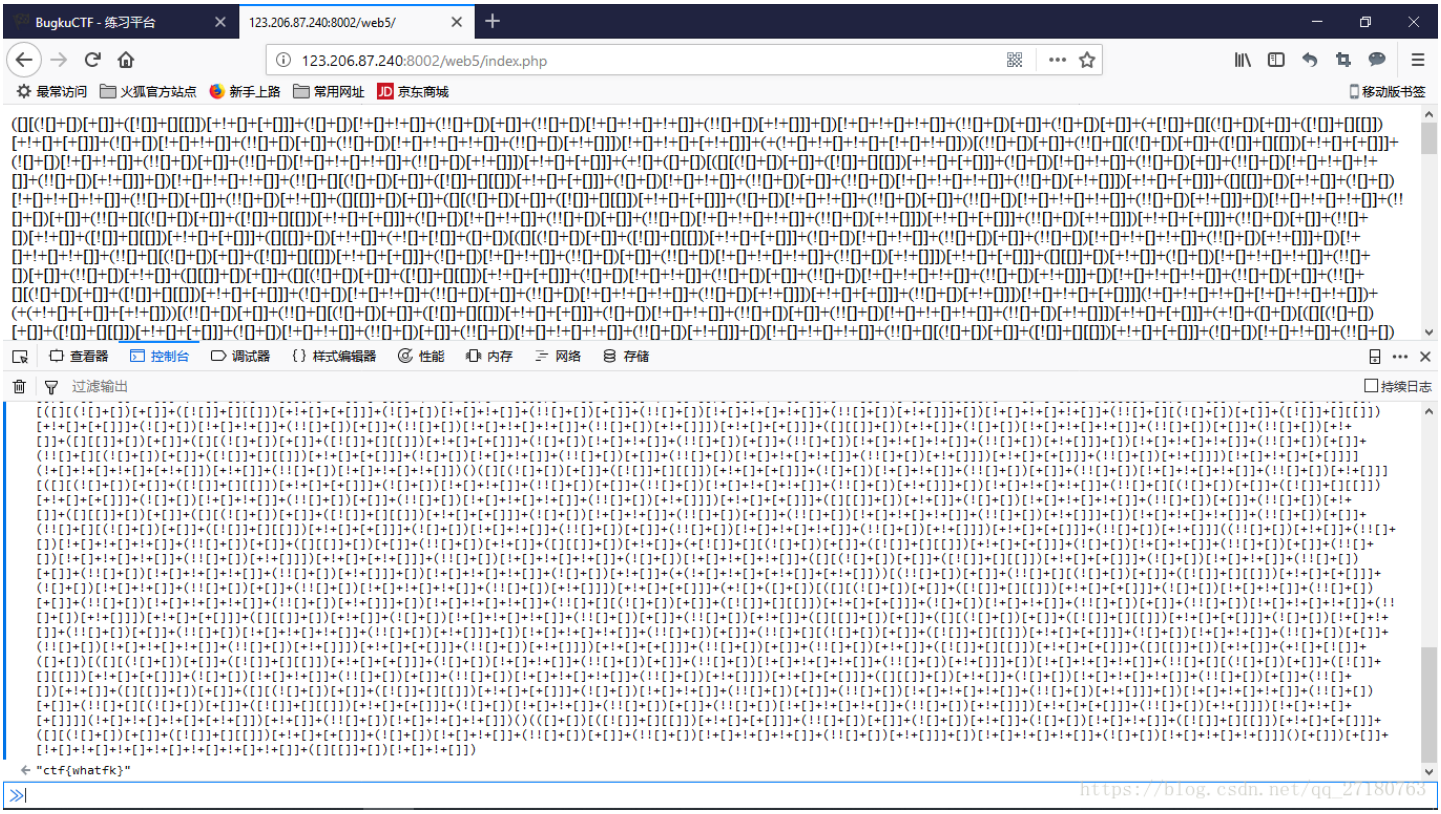
网络空间安全

41 篇文章 8 订阅

订阅专栏

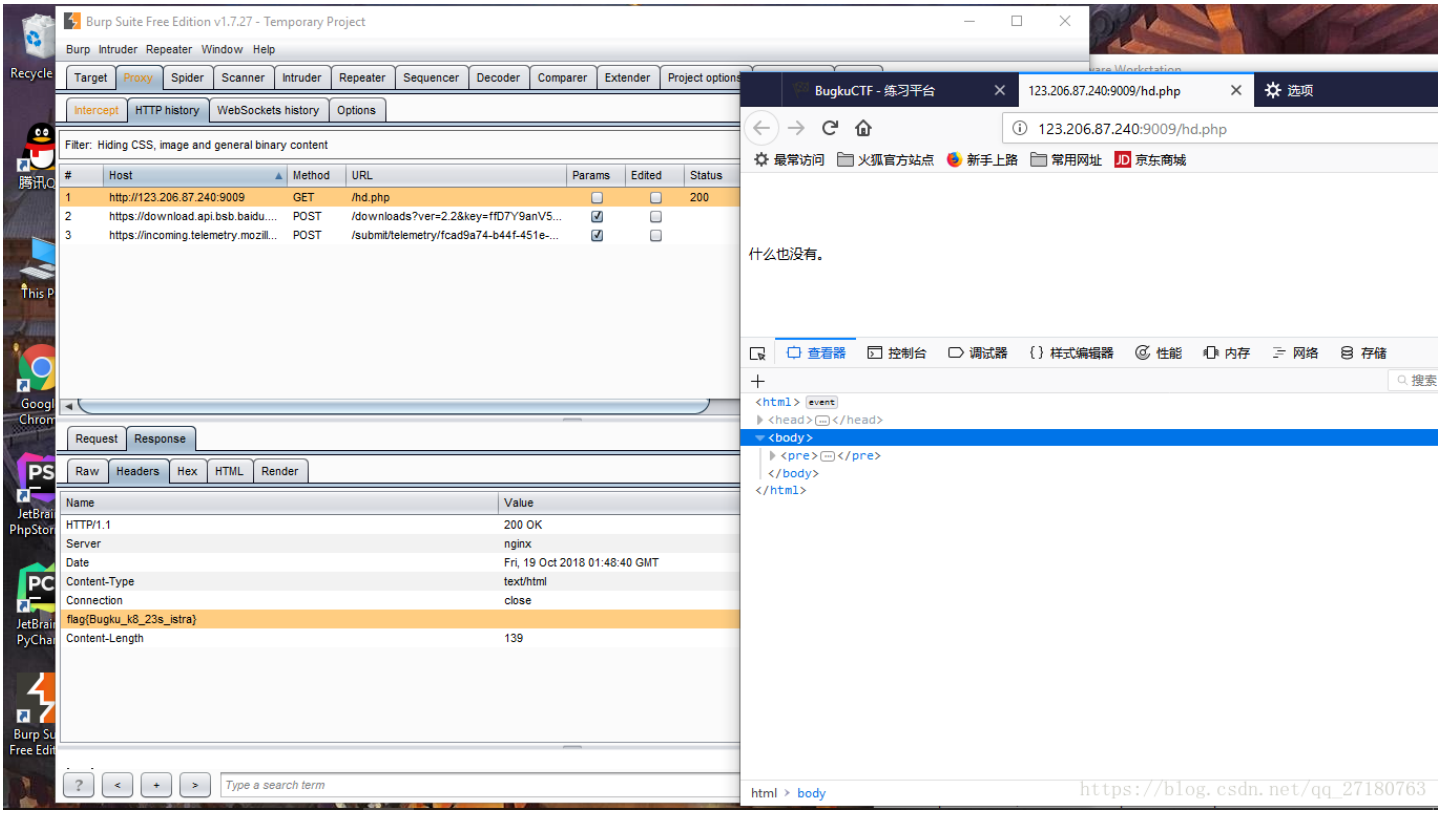
第11题：web5

查看页面源代码，发现被隐藏掉的代码。怀疑是javascript代码。网上试了各种解密和解压缩方法都不行。试了试直接在console控制台运行。成功运行并拿到flag。



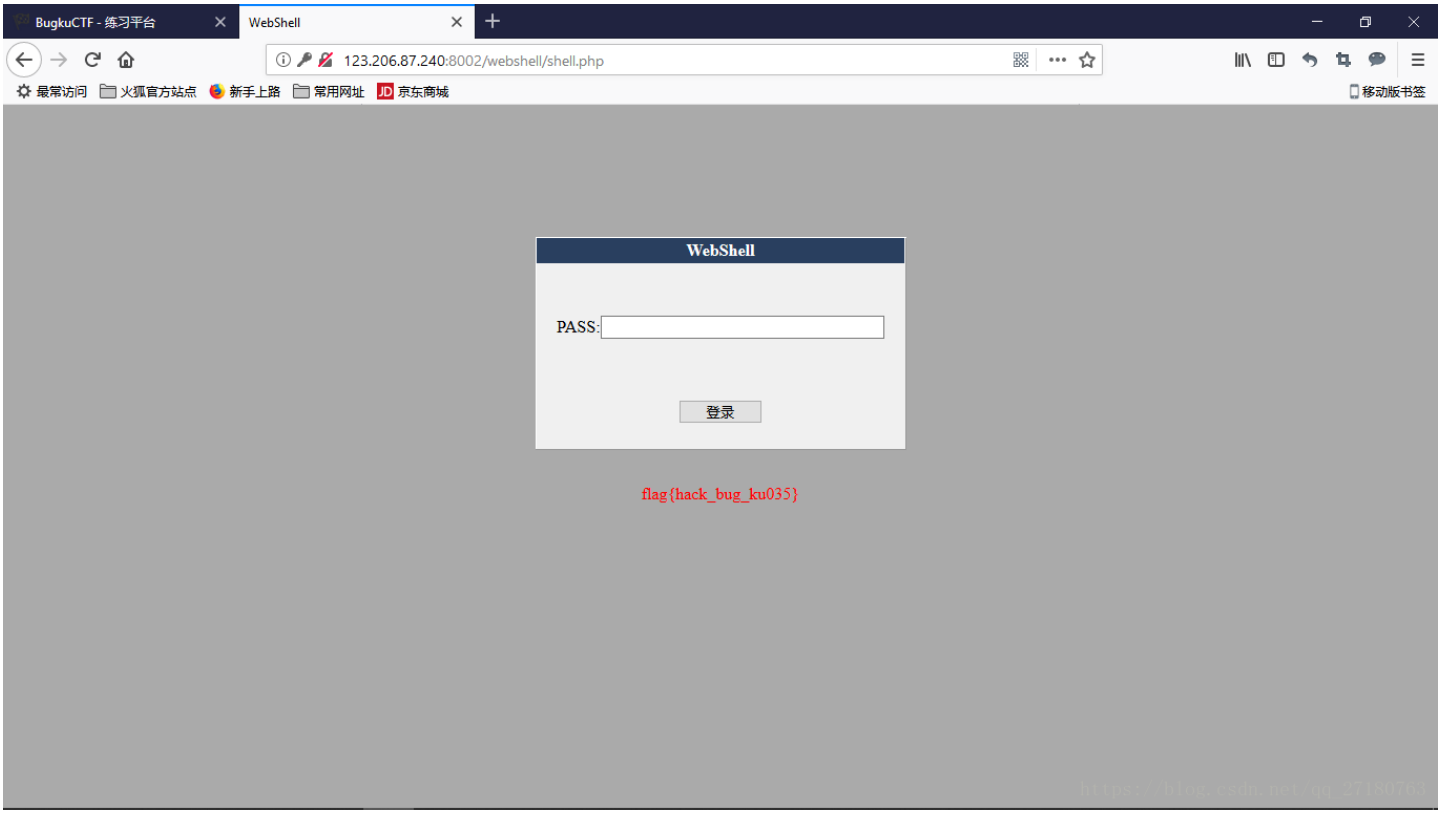
第12题：头等舱。

查看页面源代码和web请求。发现什么都没有，空空如也。于是开了bt抓包。通过网页的response发现了headers中藏有flag值



第13题：网站被黑

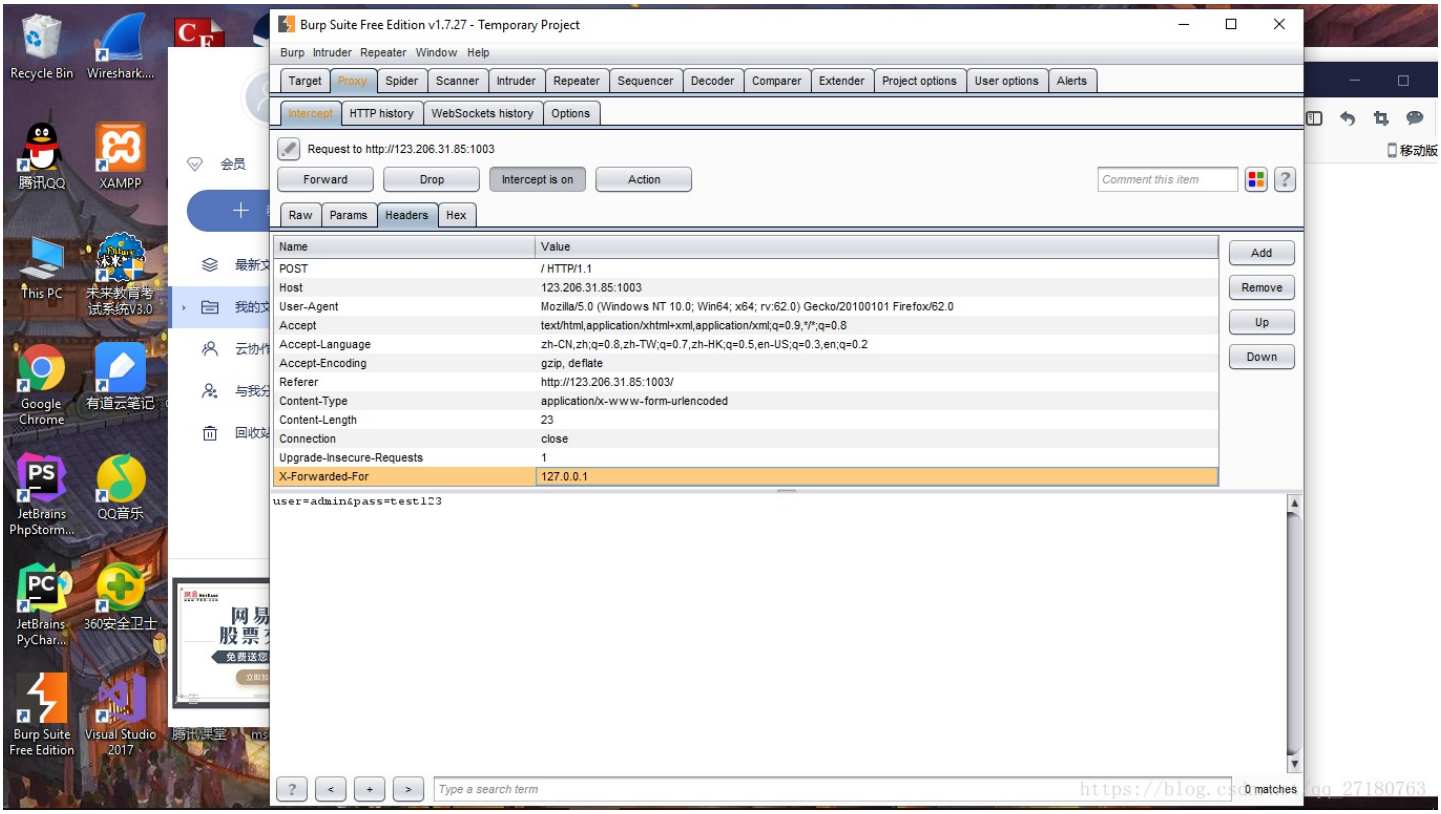
首先查看网站源代码。发现网站没有什么问题。
想到webshell被隐藏的可能，于是使用御剑后台扫描工具，发现网站shell.php。
打开后发现需要登录。使用bt爆破。发现密码是：hack。拿到flag。

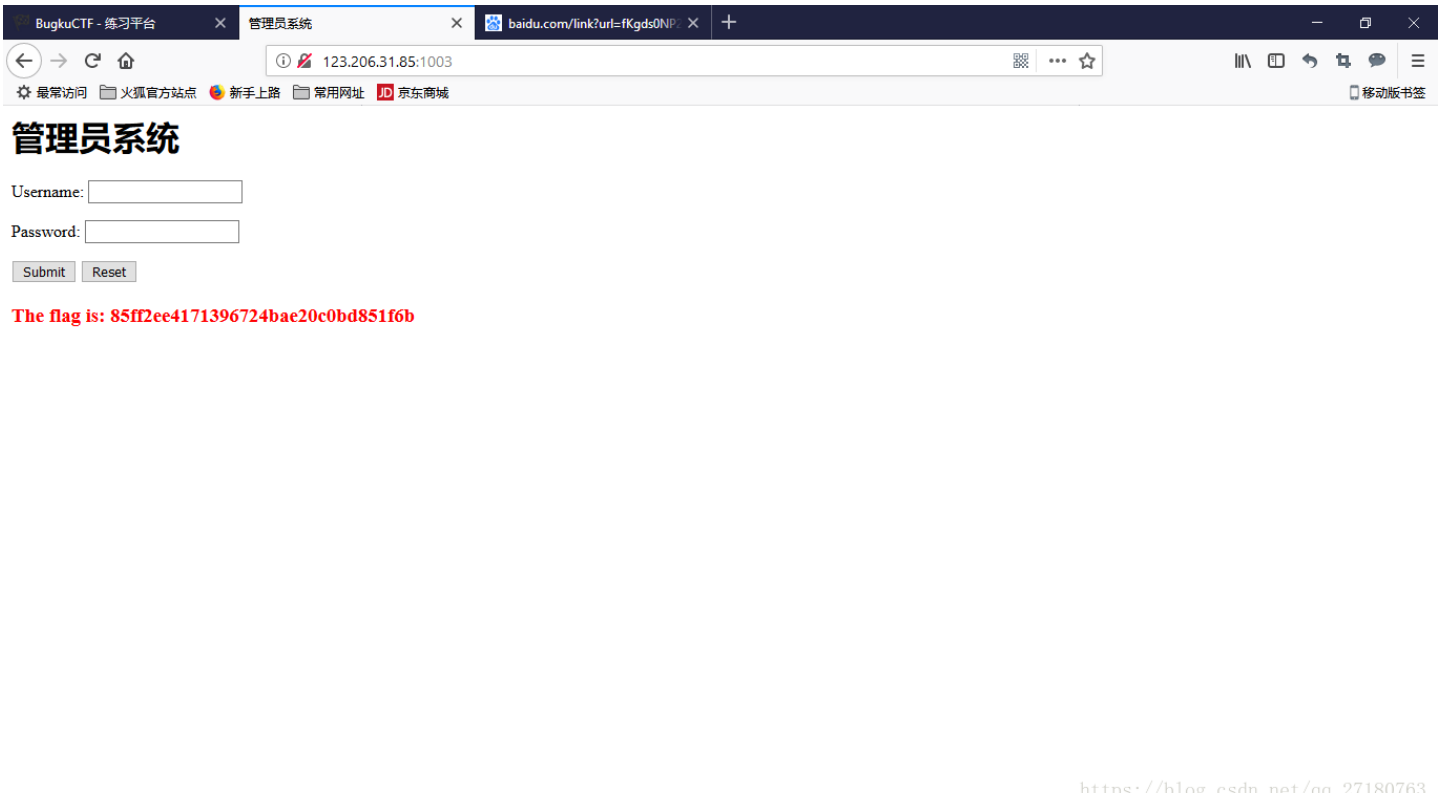


第14题：管理员系统

查看页面源代码。发现base64加密算法。解密后拿到值test123.推断该值为密码。输入账号为admin，密码为test123.提交后发现提示“IP禁止访问，请联系本地管理员登陆，IP已被记录.”

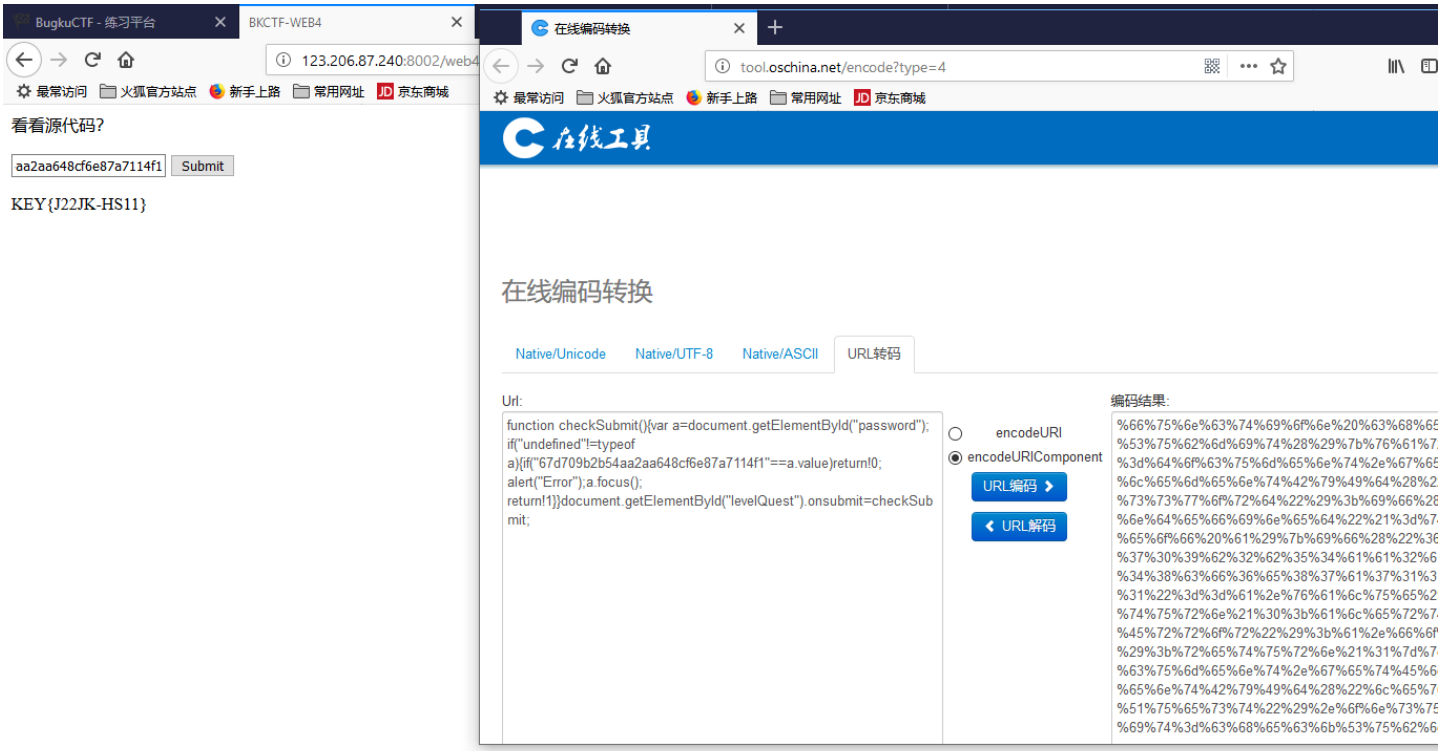
burp抓包。添加键值对：X-Forworded-For=127.0.0.1,转发后拿到flag值。





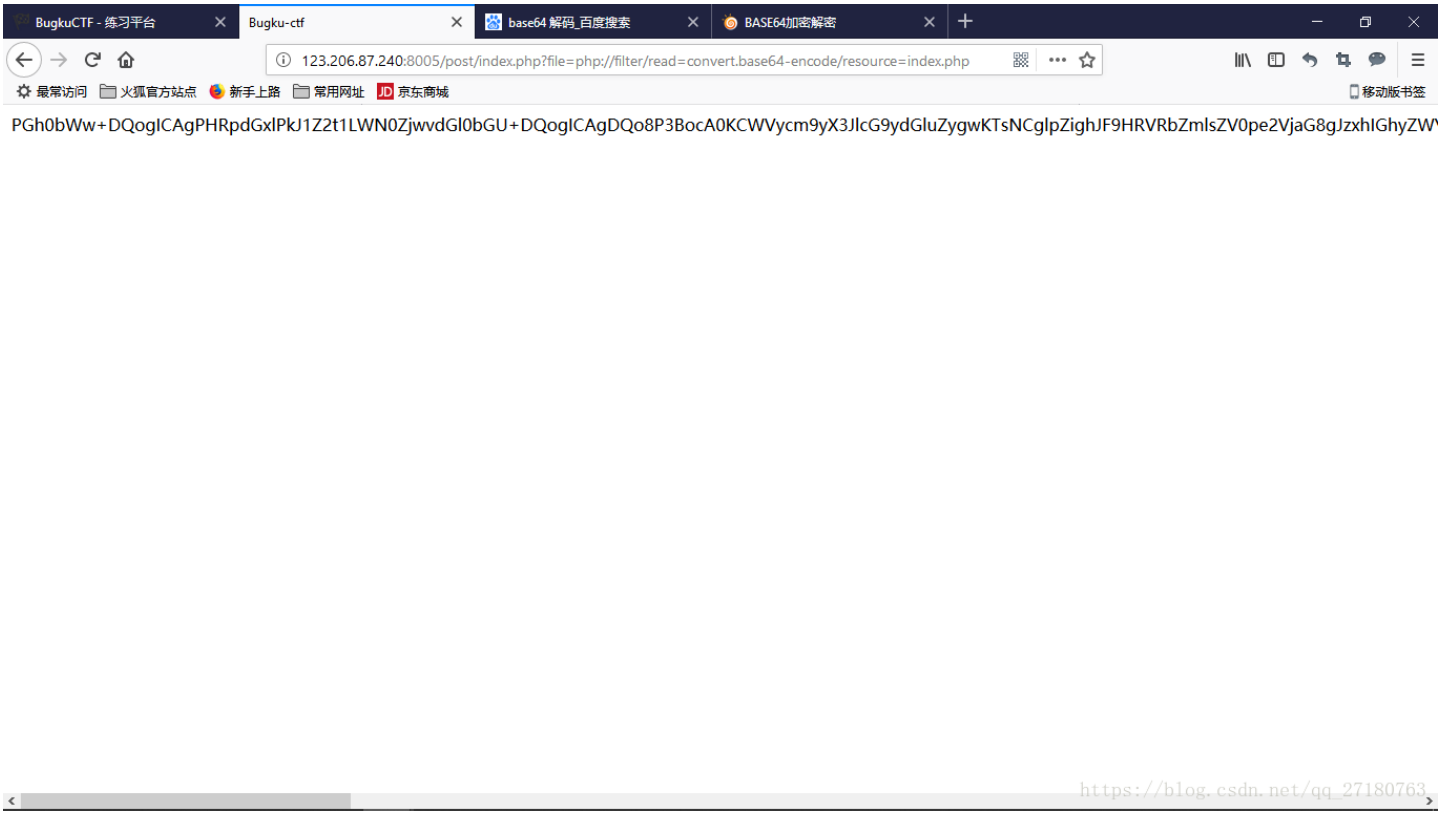
第15题： WEB4

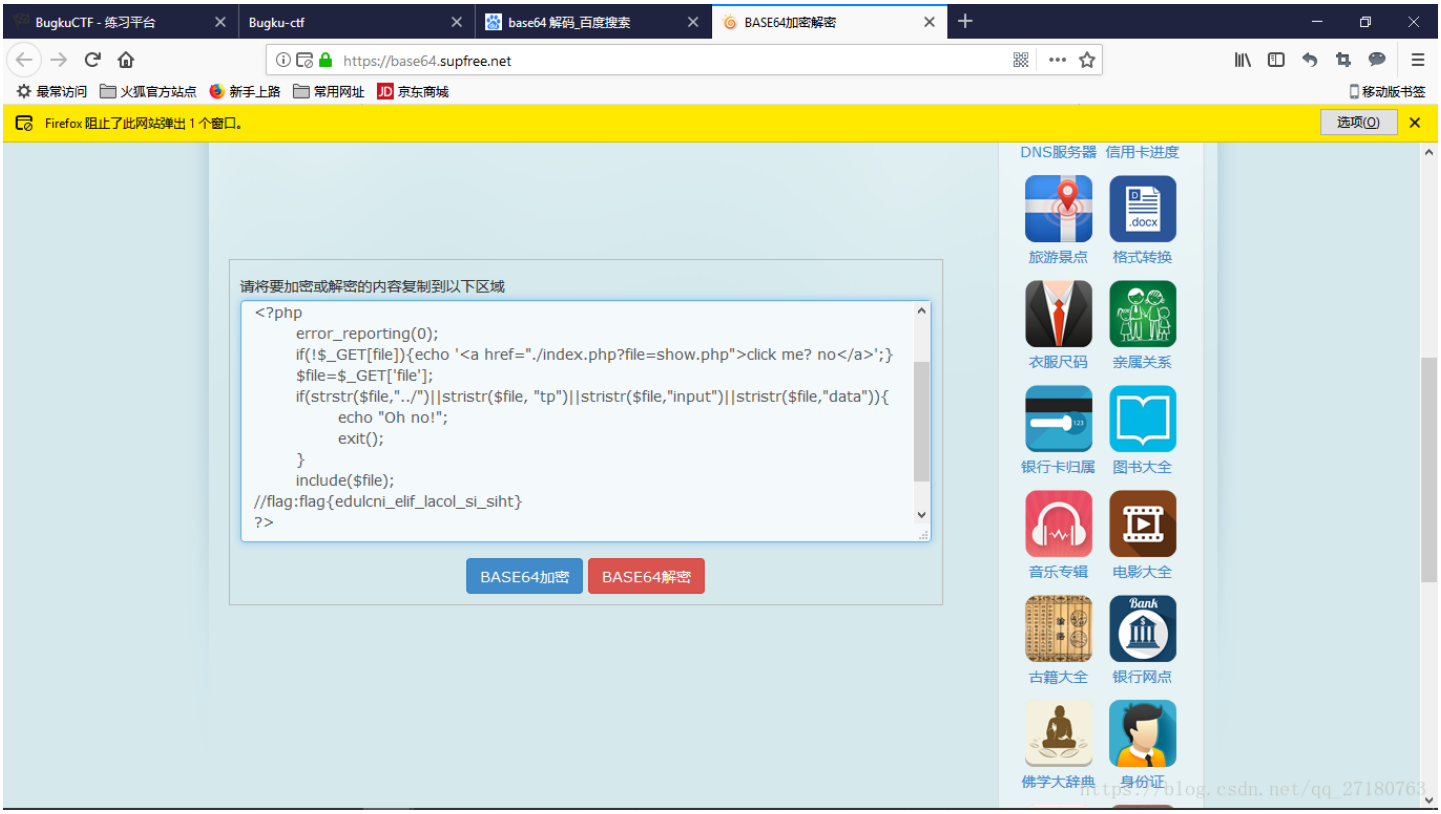
查看页面源代码。发现url编码。进行编码转换发现javascript代码。通过源代码分析传入值：
67d709b2b54aa2aa648cf6e87a7114f1
传入后拿到flag。



第16题： flag在index里

首先猜测是php://filter读文件的问题。
使用php://filter/read=convert.base64-encode/resource=index.php
拿到了加密的源文件。经过base64解密后成功拿到index.php的文件内容。
顺利拿到flag。

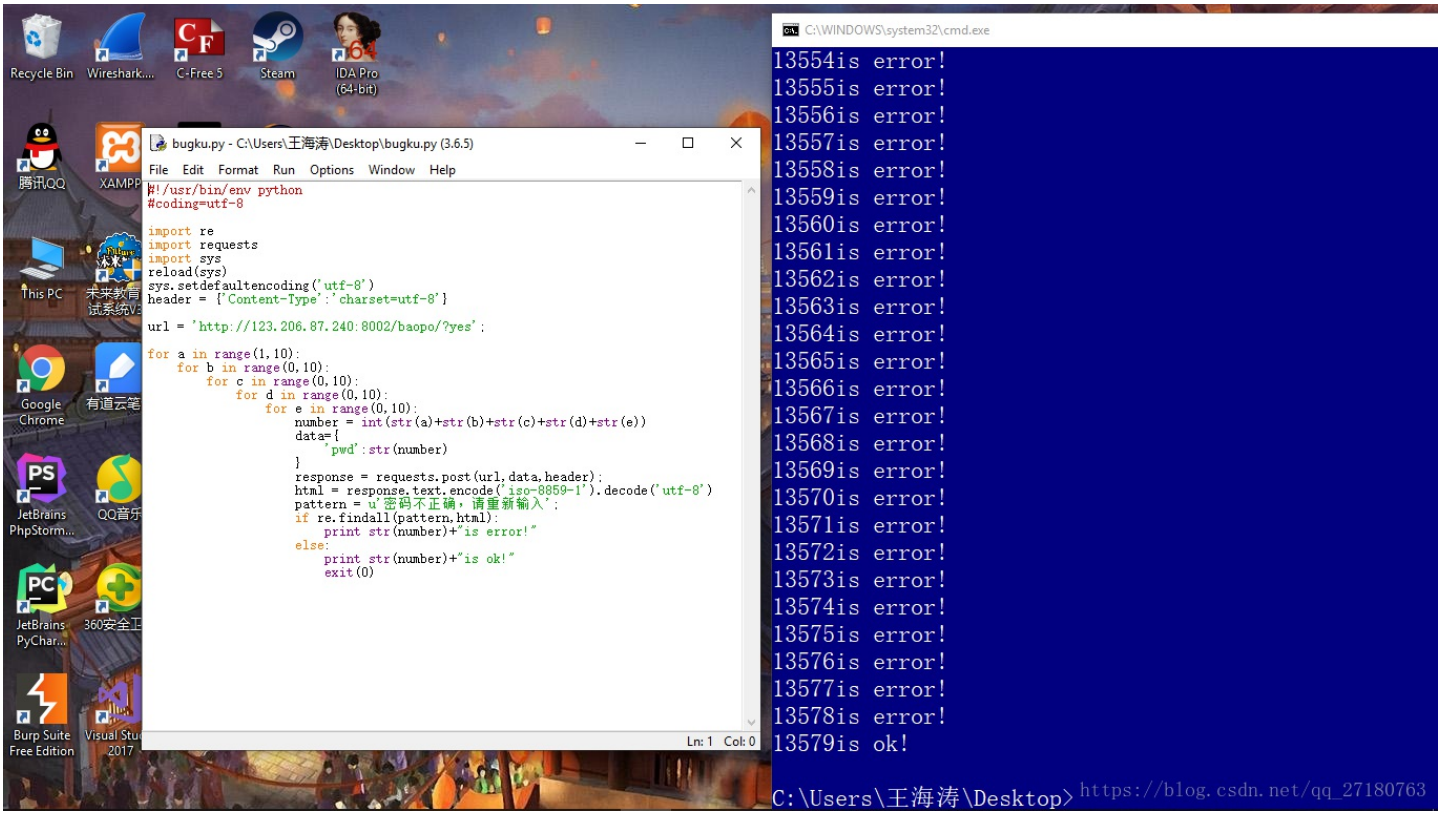




第17题：输入密码查看flag

首先查看源代码。没有任何提示信息。表单是POST提交的。再观察url，发现baopo一词。所以考虑到弱密码爆破。那我们就编写脚本进行爆破。

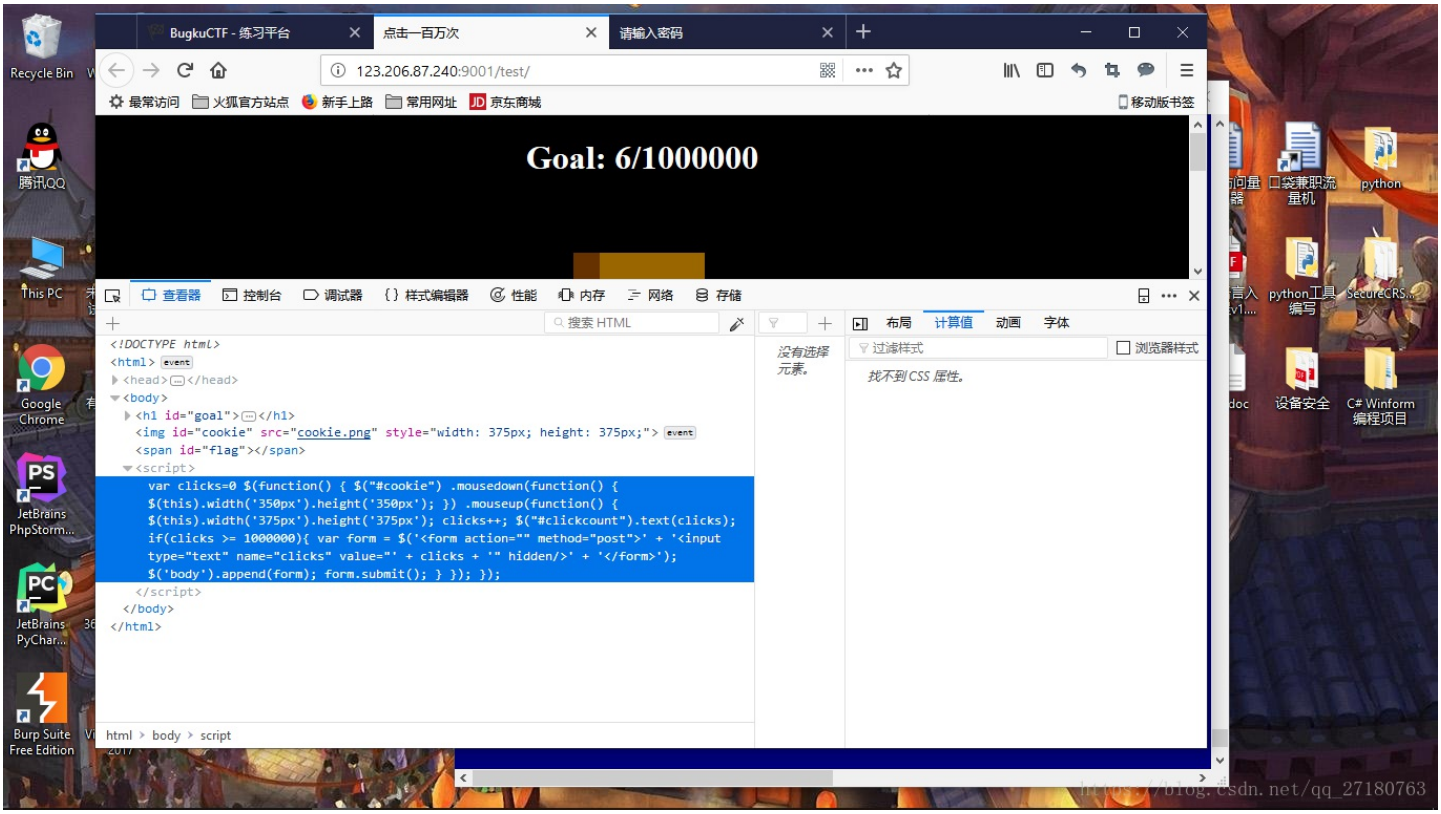
注意这个python的字符编码问题。首先是encode转换成页面源码的字符编码格式，然后通过decode转换成utf-8格式。



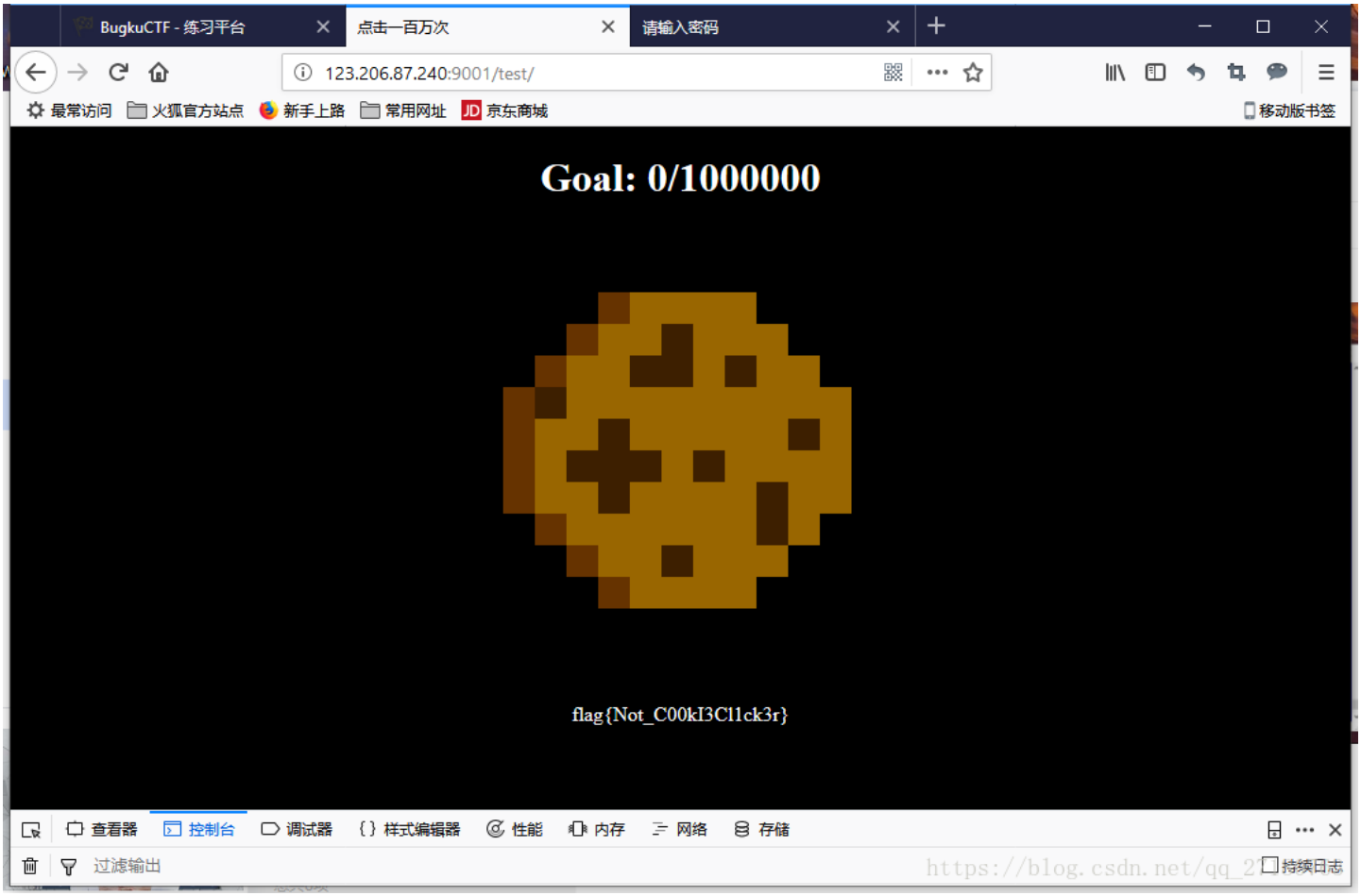
成功爆破拿到密码：“13579”，并拿到flag值“flag{bugku-baopo-hah}”

第18题：点击一百万次

右击查看源代码。发现了一段javascript代码。



分析代码，发现clicks参数。直接通过console赋值拿到flag。



第19题：备份是个好习惯

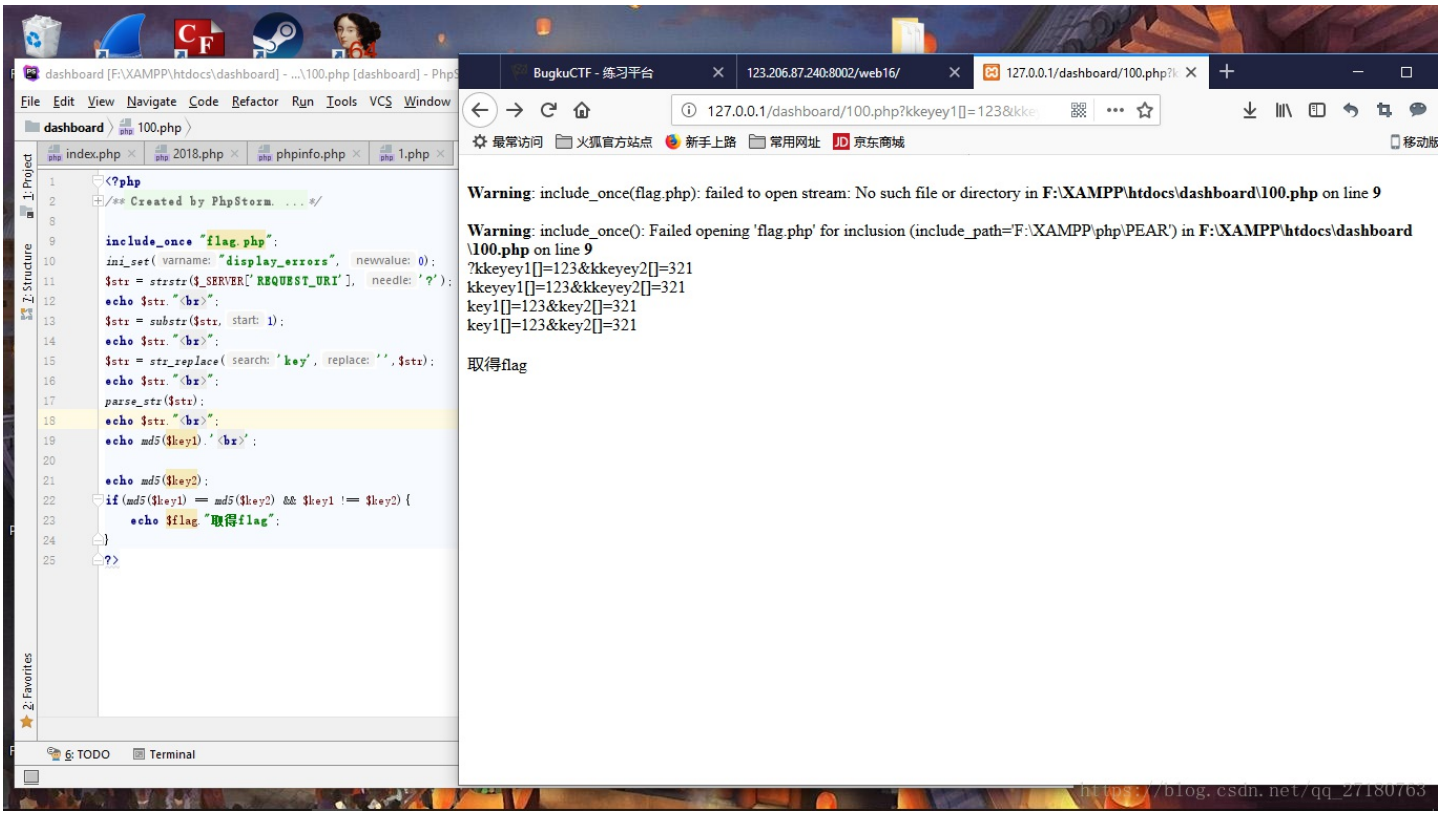
这道题一打开，映入眼帘的是一串字符串。估计是加密过的。但是怎么解密都没什么用。通过题目，考虑到可能有备份。于是访问index.php.bak,下载后拿到源代码，发现是一道md5的题。

index.php.bak - Notepad

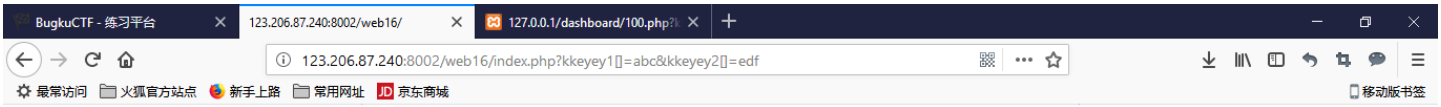
File Edit Format View Help

```
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
*/

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."取得flag";
}
?>
```


代码比较绕，所以自己搭建了一个web服务器运行程序。



发现代码将key过滤成了空，所以我们构建变量key1和key2，拿到flag值。



Bugku{OH_YOU_FIND_MY_MOMY}鍙栬緱flag