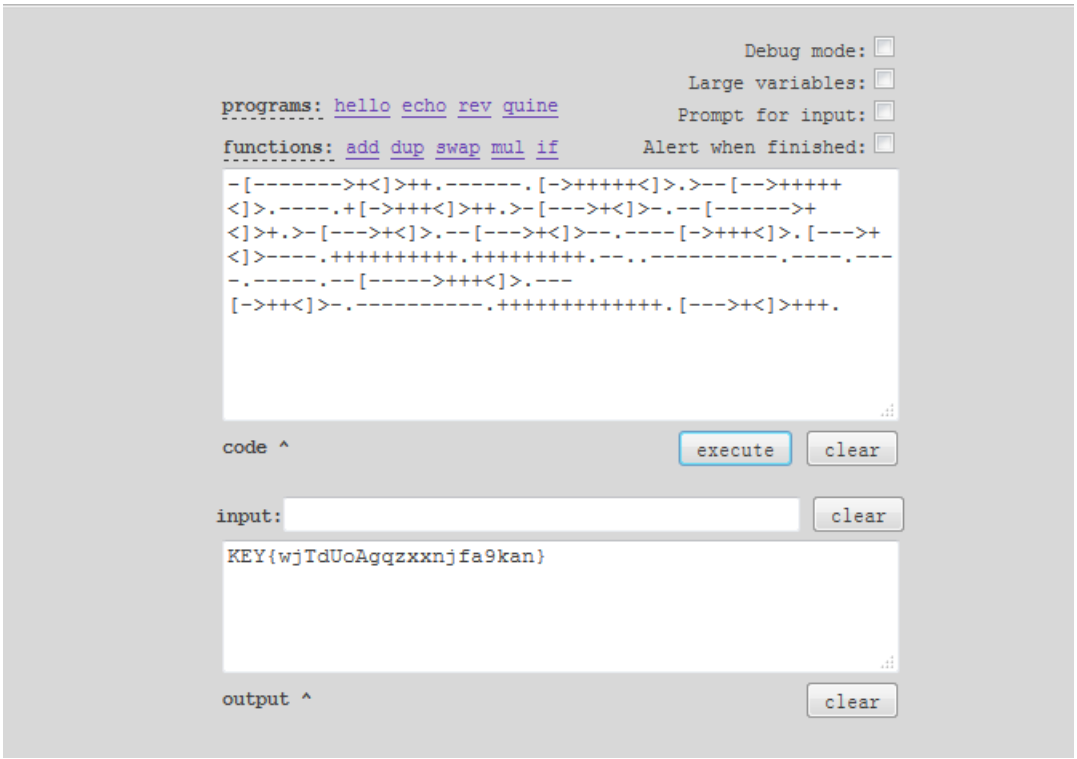
UCTF WriteUp

原创

起个名字被占了 于 2015-06-01 22:44:35 发布 1122 收藏

1. 第一题是关于BrainFuck语言的，没啥说的，直接编译就行了。



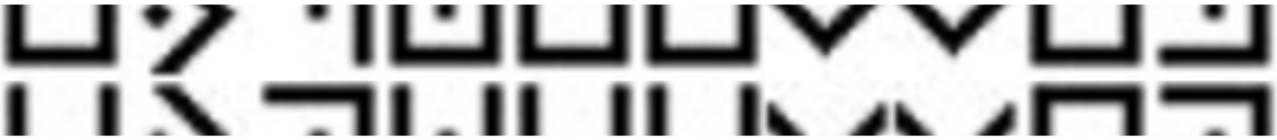
看到没有，Key直接出来了。

KEY{wjTdUoAgqzxxnjfa9kan}

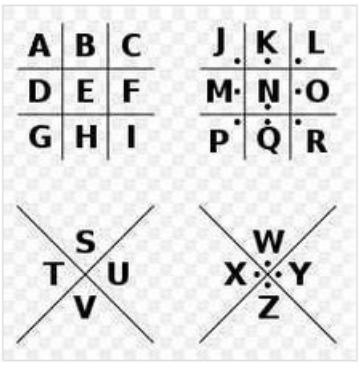
推荐给大家一个比较好的网站：http://esoteric.sange.fi/brainfuck/impl/interp/i.html

---

2.



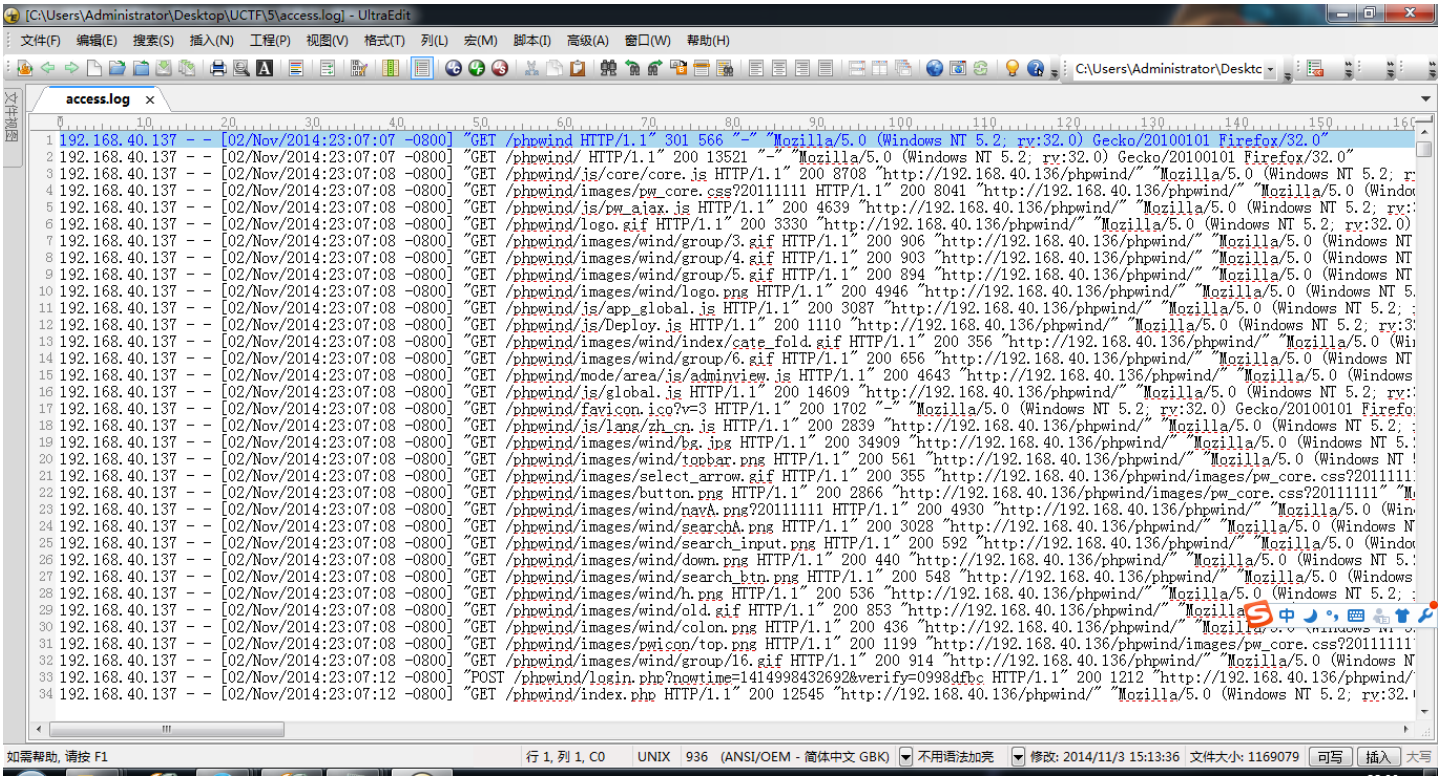
首先看到第二张图片是著名的“猪圈密码”，这个可能对于没有接触过CTF的同学来说比较陌生，不过没关系，告诉大家一个好的办法，当你看到一张图骗不知道啥意思或者想得到更多关于这张图片更多信息的时候，你可以直接去百度传图，一般都会给出你比较准确的信息。这种方法也是社工的好方法。好了，废话不多说了。直接解密就是了。
找到猪圈密码表：



通过题目中图片你会发现，给出的密文被中间翻转移位了，所以呢，翻转回来，按照密码表解密就是了：
KEY{BXPKBBSSEM}

5.日志分析* 网站被入侵了，管理员使用phpwind8.7制作的网站，通过入侵日志，你能分析出哪个最有可能是黑客留下的webshell么？KEY填入webshell的名称即可，不需要填入路径，比如：webshell是xxx.php，KEY就是KEY{xxxx.php}

把附件下载下来之后，是一个日志文件：access.log，没啥思路，先打开看看。



一大坨请求包，然后写了一个脚本，把里面所有.php的请求抓取出来，

```
#coding:utf-8
import re
f = open('out.txt','w+')
for line in open('access.log'):
    # print line
    out = re.findall(r'POST .*php',line)
    if out:
        f.write(str(out)+'\r\n')
f.close()
```

看到有个common.php，常用的php内置函数。试了一下，果真是这个...

KEY{common.php}

8

第8题,（10分）

大神们，1+2+3+4+5+.....7890结果是多少？结果提交形式KEY{结果}

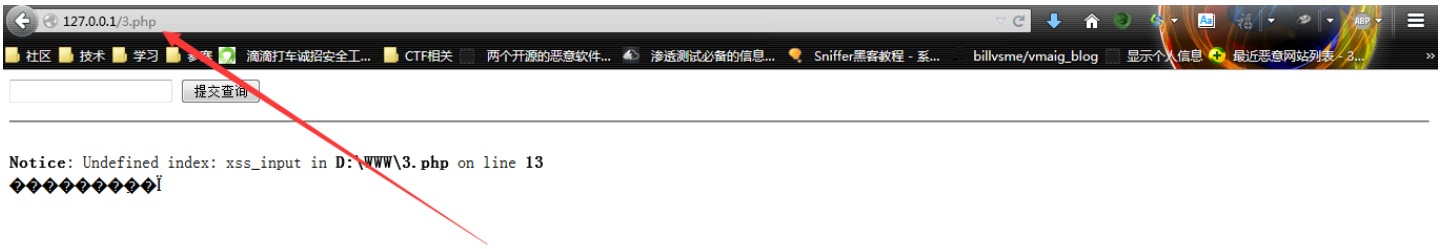
直接写个脚本就行了，我用Python写了两行代码：

```
__author__ = 'Administrator'
#coding:utf-8
sum = 0
for i in range(1,7891):
    sum = sum +i
print  sum


#31129995
```

KEY{31129995}

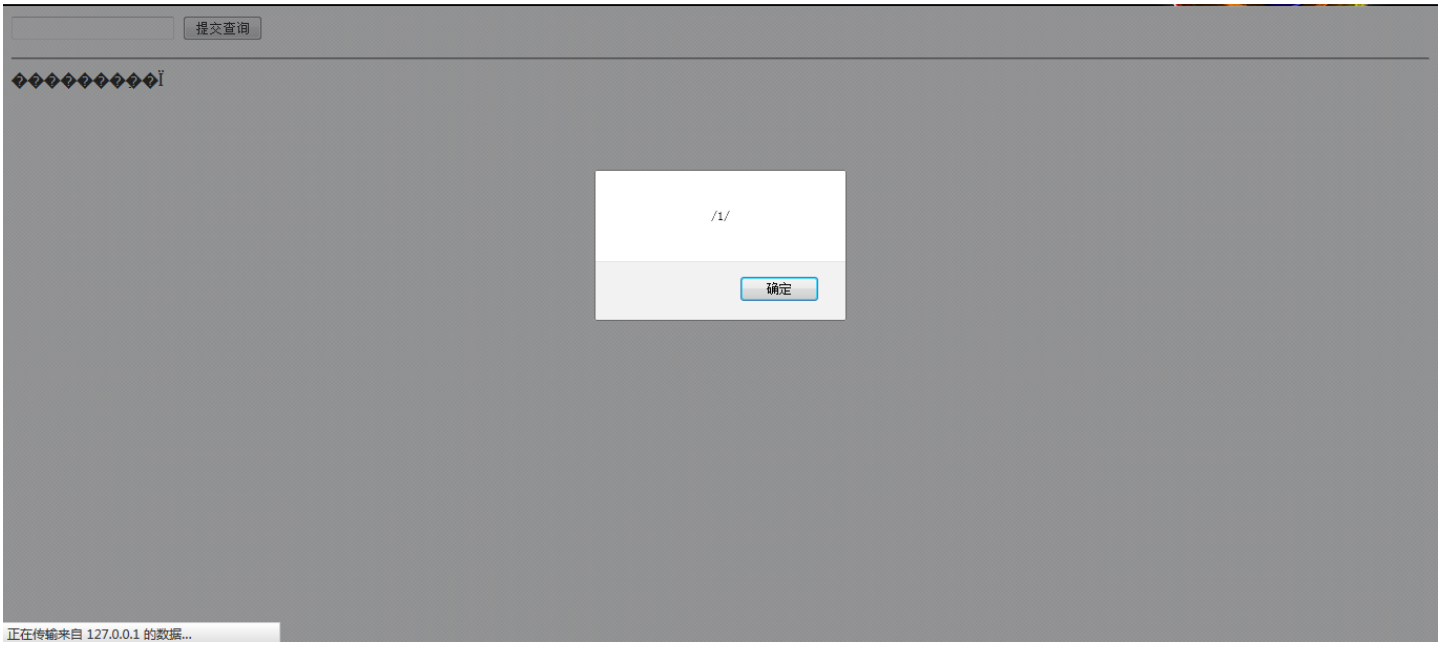
9 、附件为某网站重要文件，请分析并查找KEY，提交格式”KEY{XXXXXX}”.
附件是一个.asp的文件，开始还以为是KEY被加密写在文件中的，用Winhex打开看了一下，并没有发现什么，是一个标准的asp文件。那就编译一下呗。因为我搭建的是php的运行环境，所以asp的文件不能解析，我就改成了.php的了



可以看到，文件已经编译了，邮件看一下源码：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>XSS□□□□□□</title>
</head>
<body>
<form action="" method="get">
<input type="text" name="xss_input">
<input type="submit">
</form>
<hr>
<?php
$xss = $_GET['xss_input'];
echo '□□□□□□□□□□Ï<br>'.$xss;
?>
</body>
</html>
```

有些乱码，不过能看出来应该是考察XSS的东西，输入测试代码：`<script>alert(/1/)</script>`。ok，弹出了可爱的窗了：



那题目说的重要文件是不是cookie呢？试一下吧

再次输入：`<script>alert(document.cookie)</script>`

得到KEY{E4cY5uRf8r7wIAIkoFfuGpEfn8k1JOuu}