2019年CTF4月比赛记录（二）：“掘安杯”、TJCTF部分Web题目writeup与重解

原创

極品一═☆宏 于 2019-04-14 14:03:44 发布 1868 收藏 5

分类专栏： CTF_web 2019年CTF比赛—4月赛

本文链接：https://blog.csdn.net/qq_43214809/article/details/89087085

CTF_web 同时被 2 个专栏收录

13 篇文章 0 订阅

订阅专栏

2019年CTF比赛—4月赛

3 篇文章 0 订阅

订阅专栏

写在前面的：

这次比赛总体上还好吧，虽然并没有做出特别多的题目，只有8道，但是经过这个比赛，包括后面的复现，还是能学到点东西的，对自己而言也算是一种提升吧。起码相较于两个月前还是能感觉到自己的进步的。

具体的writeup官方也给出来了，我只在这里写出自己的做题记录，可能有的比较复杂，复现的过程也比较繁琐，还望见谅。

这一阵子事情挺多的，掘安和TJ的时间有点久了

比赛时间：2019年4月6日

复现时间：2019年4月10日至4月14日

一、Writeup：（基本上是密码、MISC、Web，具体的分类我记不太清了）

（一）、MISC：

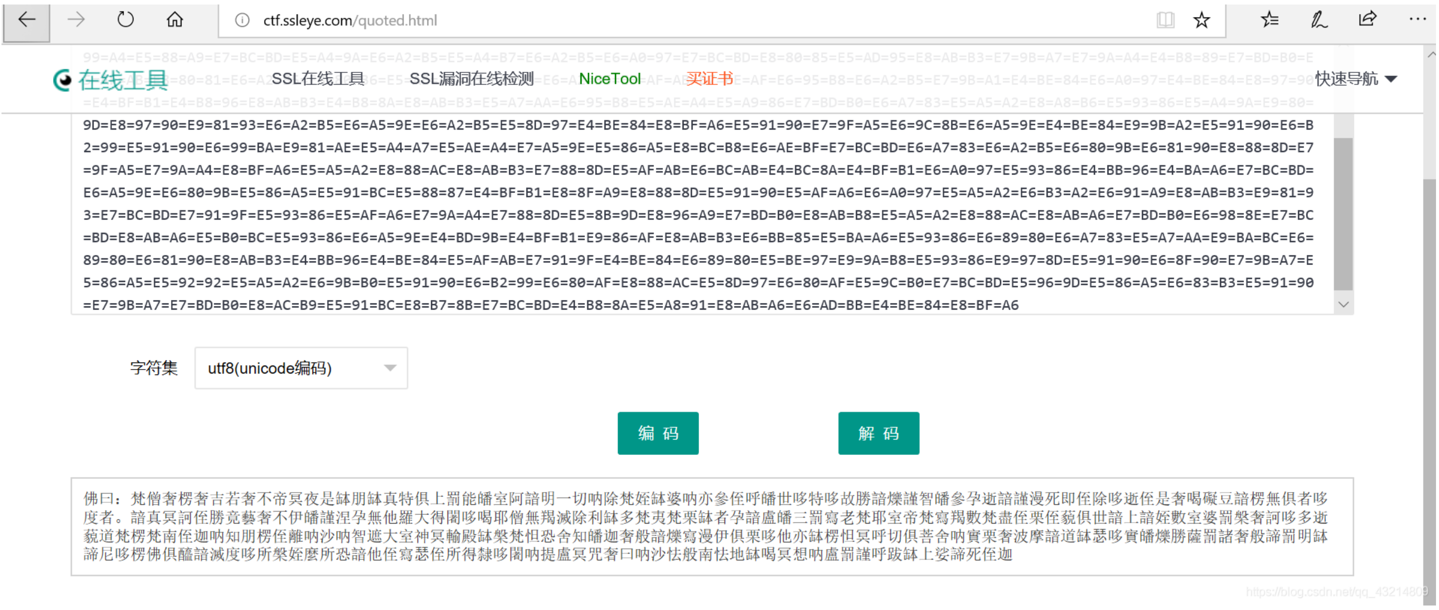
首先一个文本文档：

what_cd6cb314e80750cd76607dfd7d22594e.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

=E4=BD=9B=E6=9B=B0=EF=BC=9A=E6=A2=B5=E5=83=A7=E5=A5=A2=E6=A5=9E=E5=A5=A2=E5=90=89=E8=8B=A5=E5=A5=A2=E4=B8=8D=E5=B8=9D=E5
=86=A5=E5=A4=9C=E6=98=AF=E7=BC=BD=E6=9C=8B=E7=BC=BD=E7=9C=9F=E7=89=B9=E4=BF=B1=E4=B8=8A=E7=BD=B0=E8=83=BD=E7=9A=A4=E5=AE
=A4=E9=98=BF=E8=AB=B3=E6=98=8E=E4=B8=80=E5=88=87=E5=91=90=E9=99=A4=E6=A2=B5=E5=A7=AA=E7=BC=BD=E5=A9=86=E5=91=90=E4=BA=A6
=E5=8F=83=E4=BE=84=E5=91=BC=E7=9A=A4=E4=B8=96=E5=93=86=E7=89=B9=E5=93=86=E6=95=85=E5=8B=9D=E8=AB=B3=E7=88=8D=E8=AC=B9=E6=
99=BA=E7=9A=A4=E5=8F=83=E5=AD=95=E9=80=9D=E8=AB=B3=E8=AC=B9=E6=BC=AB=E6=AD=BB=E5=8D=B3=E4=BE=84=E9=99=A4=E5=93=86=E9=80=
9D=E4=BE=84=E6=98=AF=E5=A5=A2=E5=96=9D=E7=A4=99=E8=B1=86=E8=AB=B3=E6=A5=9E=E7=84=A1=E4=BF=B1=E8=80=85=E5=93=86=E5=BA=A6=E
8=80=85=E3=80=82=E8=AB=B3=E7=9C=9F=E5=86=A5=E8=A8=B6=E4=BE=84=E5=8B=9D=E7=AB=9F=E8=97=9D=E5=A5=A2=E4=B8=8D=E4=BC=8A=E7=9
A=A4=E8=AC=B9=E6=B6=85=E5=AD=95=E7=84=A1=E4=BB=96=E7=BE=85=E5=A4=A7=E5=BE=97=E9=97=8D=E5=93=86=E5=96=9D=E8=80=B6=E5=83=A
7=E7=84=A1=E7=BE=AF=E6=BB=85=E9=99=A4=E5=88=A9=E7=BC=BD=E5=A4=9A=E6=A2=B5=E5=A4=B7=E6=A2=B5=E6=A0=97=E7=BC=BD=E8=80=85=E
5=AD=95=E8=AB=B3=E7=9B=A7=E7=9A=A4=E4=B8=89=E7=BD=B0=E5=AF=AB=E8=80=81=E6=A2=B5=E8=80=B6=E5=AE=A4=E5=B8=9D=E6=A2=B5=E5=
AF=AB=E7=BE=AF=E6=95=B8=E6=A2=B5=E7=9B=A1=E4=BE=84=E6=A0=97=E4=BE=84=E8=97=90=E4=BF=B1=E4=B8=96=E8=AB=B3=E4=B8=8A=E8=AB=B
3=E5=A7=AA=E6=95=B8=E5=AE=A4=E5=A9=86=E7=BD=B0=E6=A7=83=E5=A5=A2=E8=A8=B6=E5=93=86=E5=A4=9A=E9=80=9D=E8=97=90=E9=81=93=E
6=A2=B5=E6=A5=9E=E6=A2=B5=E5=8D=97=E4=BE=84=E8=BF=A6=E5=91=90=E7=9F=A5=E6=9C=8B=E6=A5=9E=E4=BE=84=E9=9B=A2=E5=91=90=E6=B2
=99=E5=91=90=E6=99=BA=E9=81=AE=E5=A4=A7=E5=AE=A4=E7=A5=9E=E5=86=A5=E8=BC=B8=E6=AE=BF=E7=BC=BD=E6=A7=83=E6=A2=B5=E6=80=9B
=E6=81=90=E8=88=8D=E7=9F=A5=E7=9A=A4=E8=BF=A6=E5=A5=A2=E8=88=AC=E8=AB=B3=E7=88=8D=E5=AF=AB=E6=BC=AB=E4=BC=8A=E4=BF=B1=E6
=A0=97=E5=93=86=E4=BB=96=E4=BA=A6=E7=BC=BD=E6=A5=9E=E6=80=9B=E5=86=A5=E5=91=BC=E5=88=87=E4=BF=B1=E8=8F=A9=E8=88=8D=E5=91=
90=E5=AF=A6=E6=A0=97=E5=A5=A2=E6=B3=A2=E6=91=A9=E8=AB=B3=E9=81=93=E7=BC=BD=E7=91=9F=E5=93=86=E5=AF=A6=E7=9A=A4=E7=88=8D=
E5=8B=9D=E8=96=A9=E7=BD=B0=E8=AB=B8=E5=A5=A2=E8=88=AC=E8=AB=A6=E7=BD=B0=E6=98=8E=E7=BC=BD=E8=AB=A6=E5=B0=BC=E5=93=86=E6
=A5=9E=E4=BD=9B=E4=BF=B1=E9=86=AF=E8=AB=B3=E6=BB=85=E5=BA=A6=E5=93=86=E6=89=80=E6=A7=83=E5=A7=AA=E9=BA=BC=E6=89=80=E6=81
=90=E8=AB=B3=E4=BB=96=E4=BE=84=E5=AF=AB=E7=91=9F=E4=BE=84=E6=89=80=E5=BE=97=E9=9A=B8=E5=93=86=E9=97=8D=E5=91=90=E6=8F=90=E
7=9B=A7=E5=86=A5=E5=92=92=E5=A5=A2=E6=9B=B0=E5=91=90=E6=B2=99=E6=80=AF=E8=88=AC=E5=8D=97=E6=80=AF=E5=9C=B0=E7=BC=BD=E5=96
=9D=E5=86=A5=E6=83=B3=E5=91=90=E7=9B=A7=E7=BD=B0=E8=AC=B9=E5=91=BC=E8=B7=8B=E7=BC=BD=E4=B8=8A=E5=A8=91=E8=AB=A6=E6=AD=B
B=E4=BE=84=E8=BF=A6

一看就知道Quoted-printable编码，解码：



很简单，与佛论禅：

到了这一步后，一开始我是懵逼的，我一开始还以为汉字编码，整了半天，后来才想起来有个社会主义核心价值观编码，不得不说，这思想觉悟真不错：

编码 解码

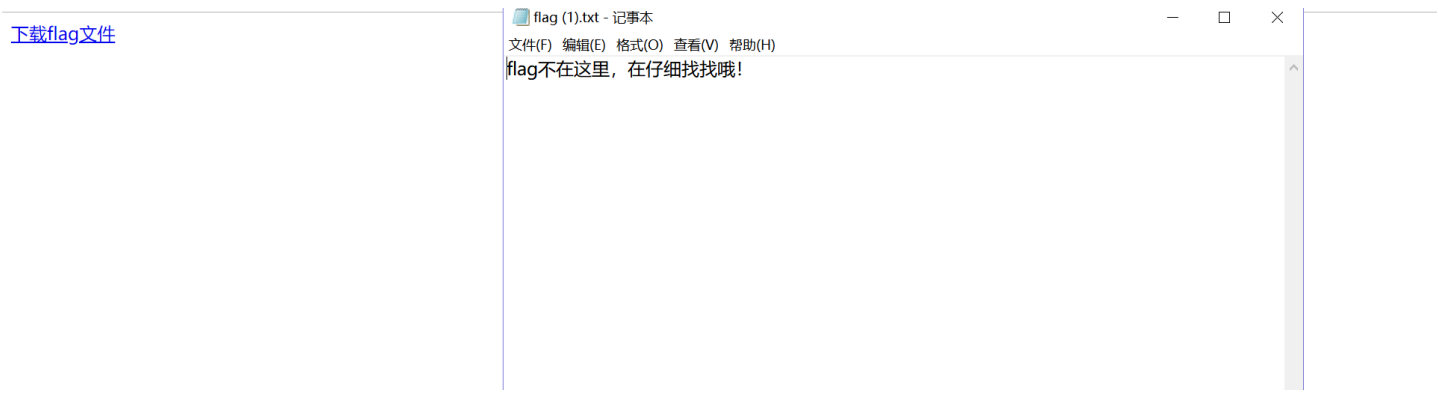
公正友善自由公正民主公正和谐法治自由公正公正法治友善平等公正爱国公正平等法治爱国公正敬业公正友善爱国平等诚信平等法治敬业法治平等公正公正公正诚信平等平等友善敬业法治民主法治富强法治友善法治

（二）、MISC：

签到水题，直接关注公众号拿flag：

（三）、Web：

这是道web题，打开题目后出现一个链接，让我们下载：



唔，不在这里，那就view-source看一下：

不安全 | view-source:120.79.1.69:8887/web2/

```
<html>
<head>
<title>下载下载</title>
</head>
<body>
<a href="?file=flag.txt">下载flag文件</a>
<!--
<a href="flag.php">flag</a>
-->
</body>
</html>
```


提示来了，flag.php，那就直接放到地址栏里，然后出来了一个文件：

flag (1).php

```
        }
        $char .= $key {$x};
        $x ++;
    }
    for($i = 0; $i < $len; $i ++) {
        $str .= chr ( ord ( $data {$i} ) + (ord ( $char {$i} )) % 256 );
    }
    return base64_encode ( $str );
}

function decrypt($data, $key) {
    $key = md5 ( $key );
    $x = 0;
    $data = base64_decode ( $data );
    $len = strlen ( $data );
    $l = strlen ( $key );
    for($i = 0; $i < $len; $i ++) {
        if ($x == $l) {
            $x = 0;
        }
        $char .= substr ( $key, $x, 1 );
        $x ++;
    }
    for($i = 0; $i < $len; $i ++) {
        if (ord ( substr ( $data, $i, 1 ) ) < ord ( substr ( $char, $i, 1 ) )) {
            $str .= chr ( (ord ( substr ( $data, $i, 1 ) ) + 256) - ord ( substr ( $char, $i, 1 ) ) );
        } else {
            $str .= chr ( ord ( substr ( $data, $i, 1 ) ) - ord ( substr ( $char, $i, 1 ) ) );
        }
    }
    return $str;
}

$key="MyCTF";
$flag="o6lziae0xtaqoqCtmWqcaZuZfrd5pbI=";//encrypt($flag,$key)
?>
```


两个值在最后面已经给出来了，而且程序也给了，直接跑一下就可以了：

```
<?php
```

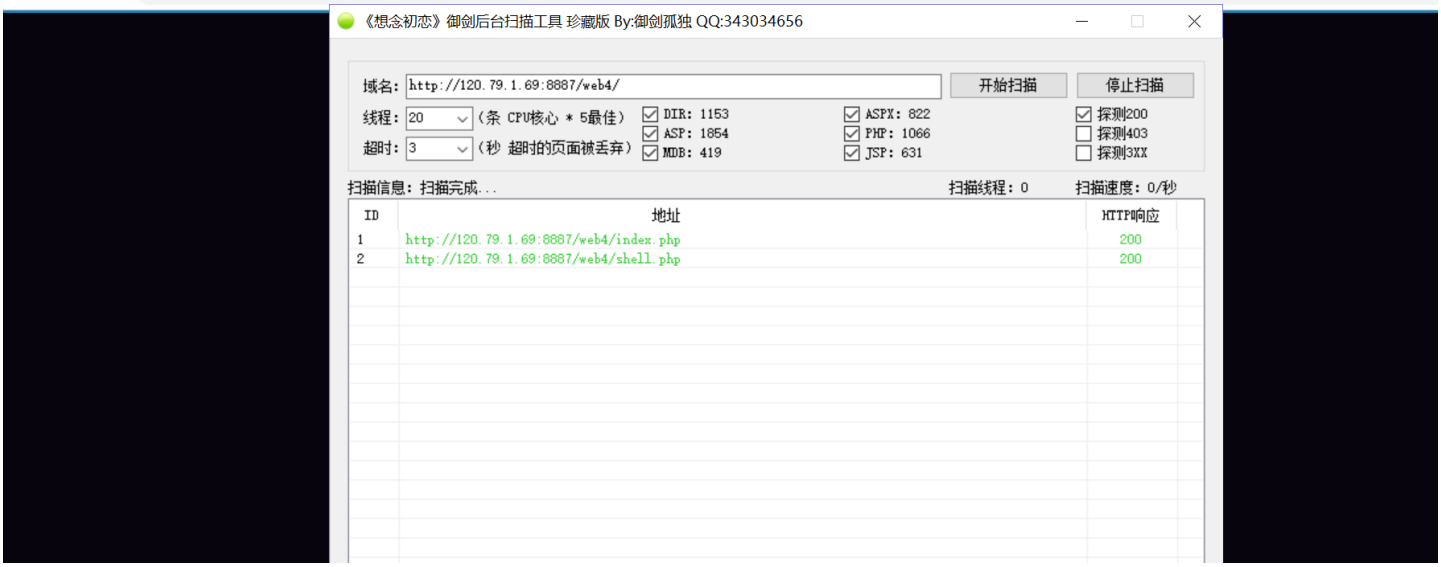
```php
<?php
$key="MyCTF";
$flag="o6lziae0xtaqoqCtmWqcaZuZfrd5pbI=";
echo encrypt($flag, $key);
echo "<br />";
echo decrypt($flag, $key);
echo "<br />";
function encrypt($data, $key) {
    $key = md5 ( $key );
    $x = 0;
    $len = strlen ( $data );
    $l = strlen ( $key );
    for($i = 0; $i < $len; $i ++) {
        if ($x == $l) {
            $x = 0;
        }
        $char .= $key {$x};
        $x ++;
    }
    for($i = 0; $i < $len; $i ++) {
        $str .= chr ( ord ( $data {$i} ) + (ord ( $char {$i} )) % 256 );
    }
    return base64_encode ( $str );
}


function decrypt($data, $key) {
    $key = md5 ( $key );
    $x = 0;
    $data = base64_decode ( $data );
    $len = strlen ( $data );
    $l = strlen ( $key );
    for($i = 0; $i < $len; $i ++) {
        if ($x == $l) {
```

```
pWacr8qayJOvp5mn1KappNO8qMWVvaqMmaLFZ6SUr6M=
myCTF{cssohw456954GUEB}
PHP Notice: Undefined variable: char in /root/soft/playground/index.php on line 17 PHP Notice: Undefined variable: str in /root/soft/playground/index.php on line 21 PHP Notice: Undefined variable: char in /root/soft/playground/index.php on line 37 PHP Notice: Undefined variable: str in /root/soft/playground/index.php on line 44
```

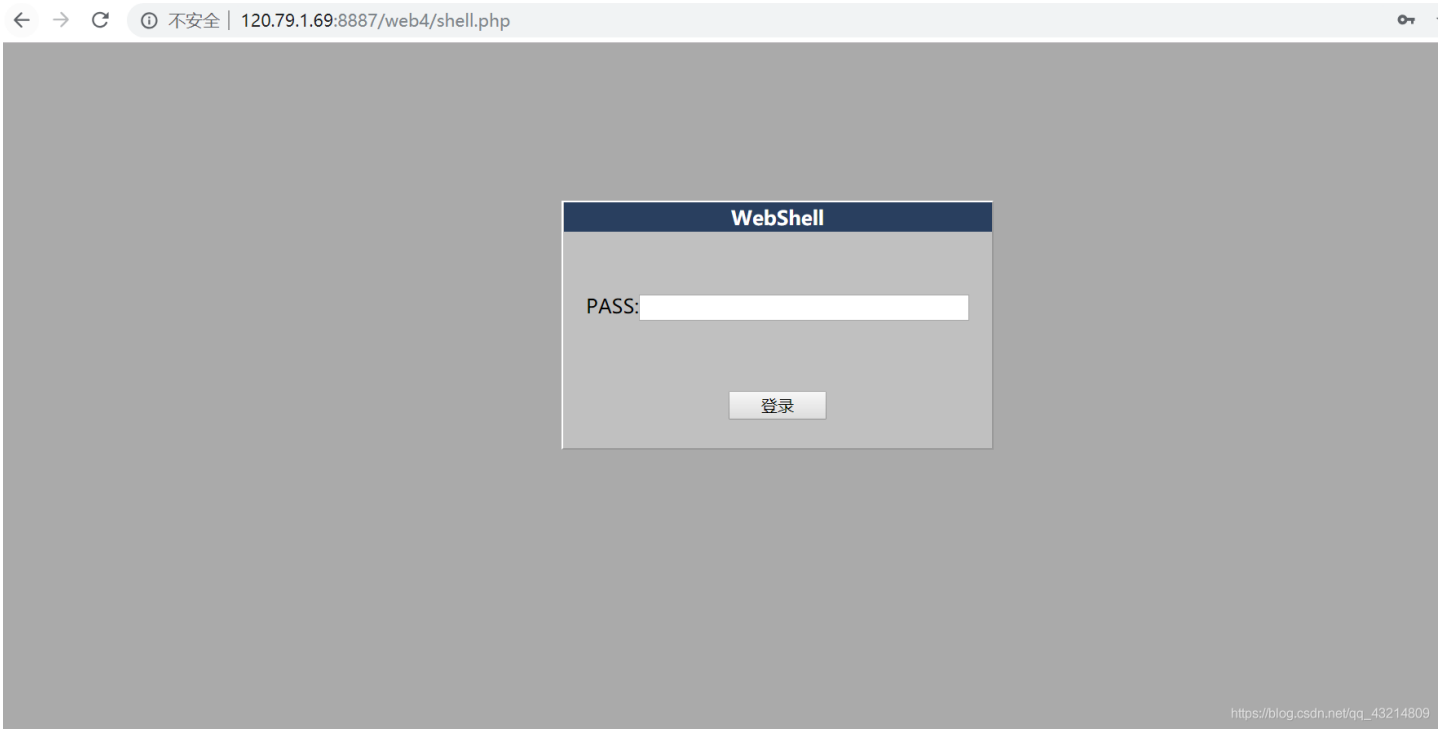

（四）、Web：

这也是道web题，题目描述是网站被黑了，打开链接看一下：

说实话，当看到这个页面后，还是比较失（欣）望（喜）的，这是道原题，直接御剑后台扫一波：



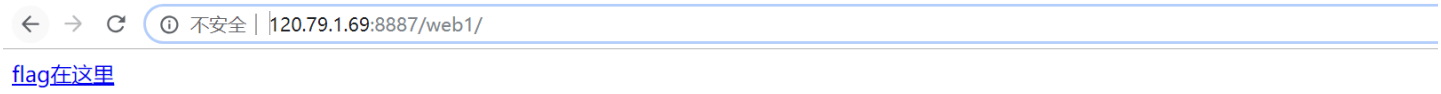
找到第二个网址，shell.php：



需要提交才能获得flag，直接抓包爆破，最后的密码连改都没改，还是hack，提交直接得到flag。

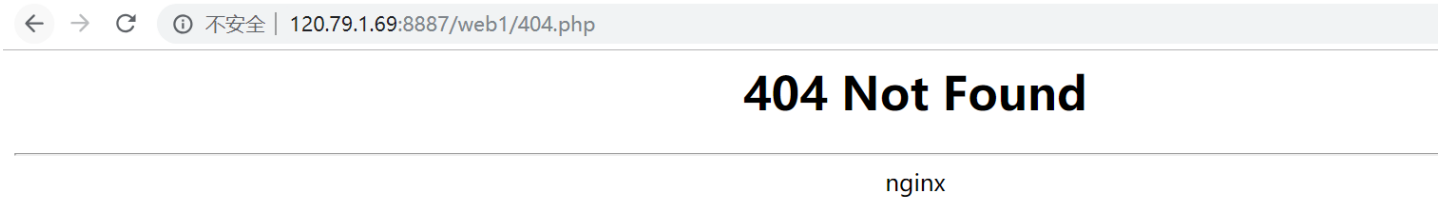
（五）、Web：

这也是web题：



flag在这里

但是直接点击后，出现如下界面：



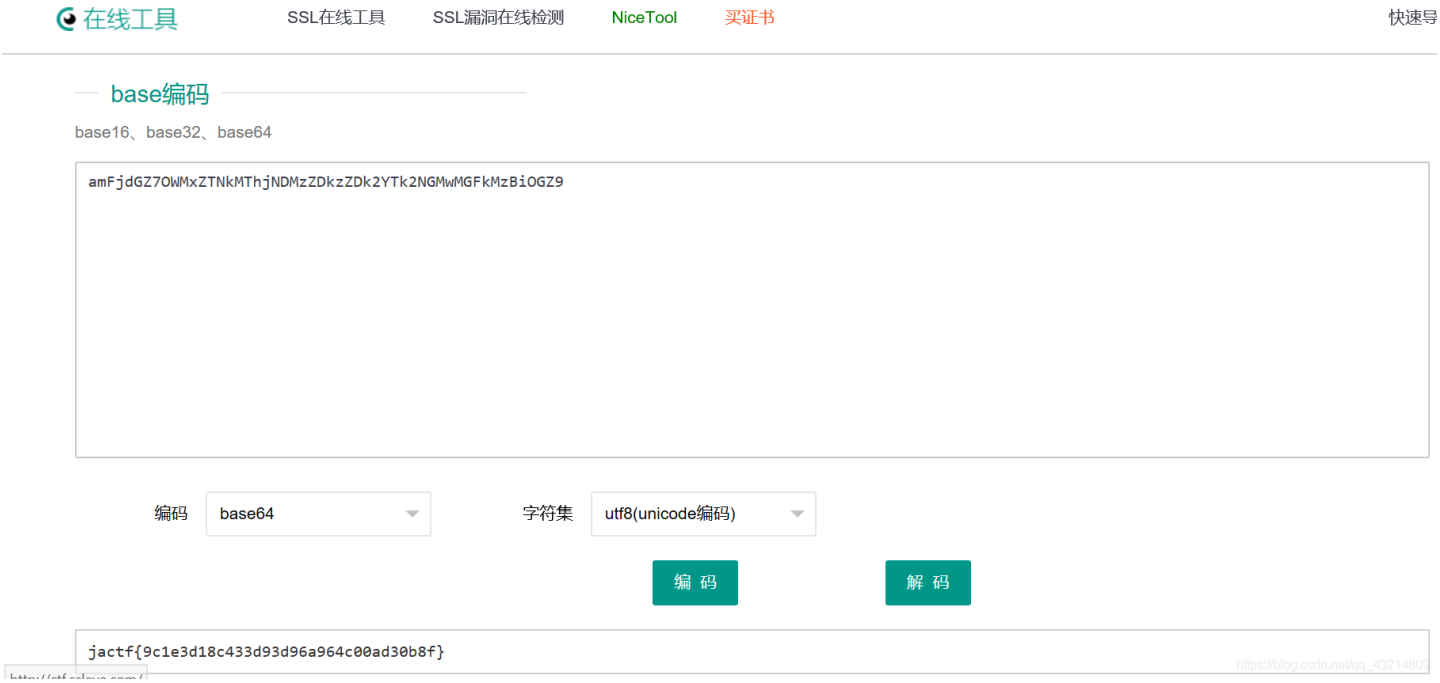
咦，这是什么情况，view-source走一下：

```
<html>
<head>
<title></title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<a href="flag.php">flag在这里</a>
</body>
</html>
```


我们可以看到，链接是flag.php但是当我们点击后，重定向到了404.php，我一开始也是不知道该怎么整，后来curl看了一下：

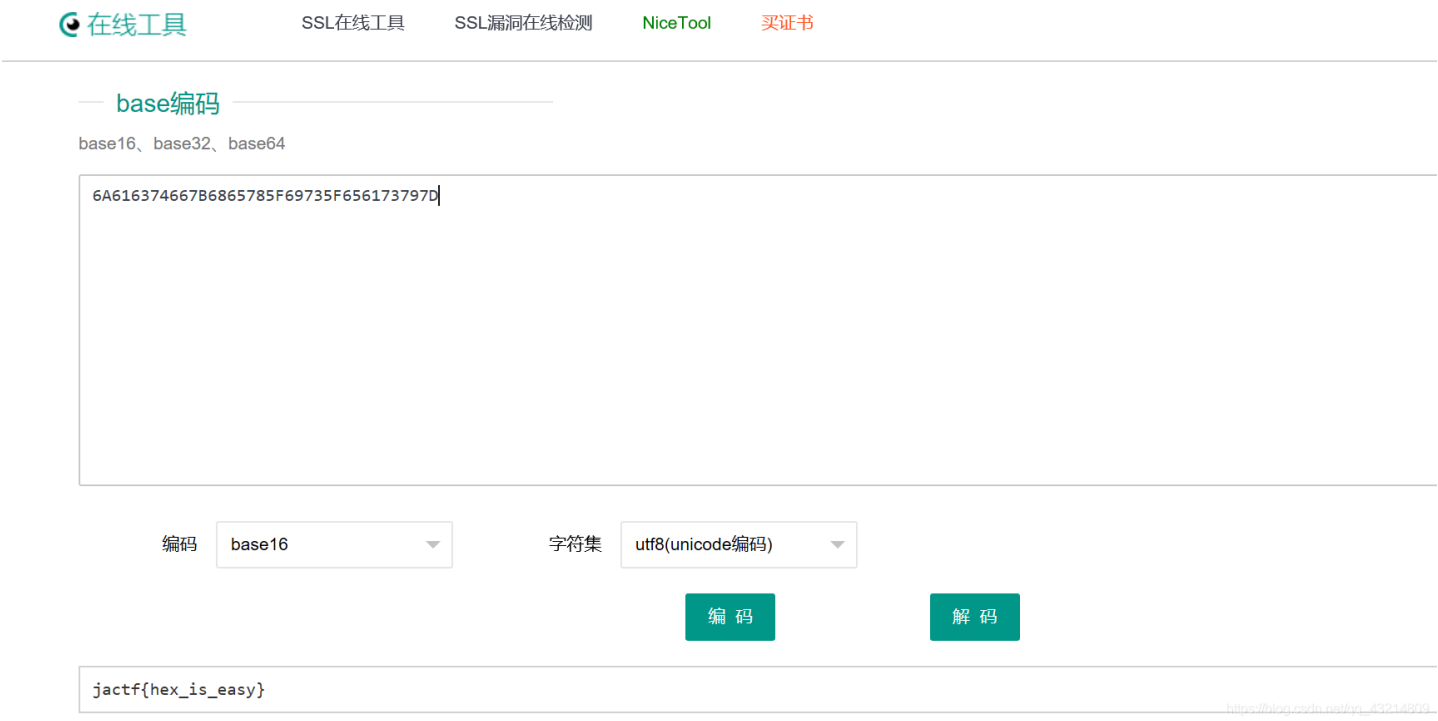
```
C:\Users\12041>curl -v http://120.79.1.69:8887/web1/flag.php
*   Trying 120.79.1.69...
* TCP_NODELAY set
* Connected to 120.79.1.69 (120.79.1.69) port 8887 (#0)
> GET /web1/flag.php HTTP/1.1
> Host: 120.79.1.69:8887
> User-Agent: curl/7.55.1
> Accept: */*
>
< HTTP/1.1 302 Moved Temporarily
< Server: nginx
< Date: Sat, 06 Apr 2019 02:57:39 GMT
< Content-Type: text/html
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-Powered-By: PHP/5.4.45
< Flag: amFjdGZ7OWMxZTNkMThjNDMzZDkzZDk2YTk2NGMwMGFkMzBiOGZ9
< location: 404.php
<
* Connection #0 to host 120.79.1.69 left intact
```


发现Flag，解码走一下：



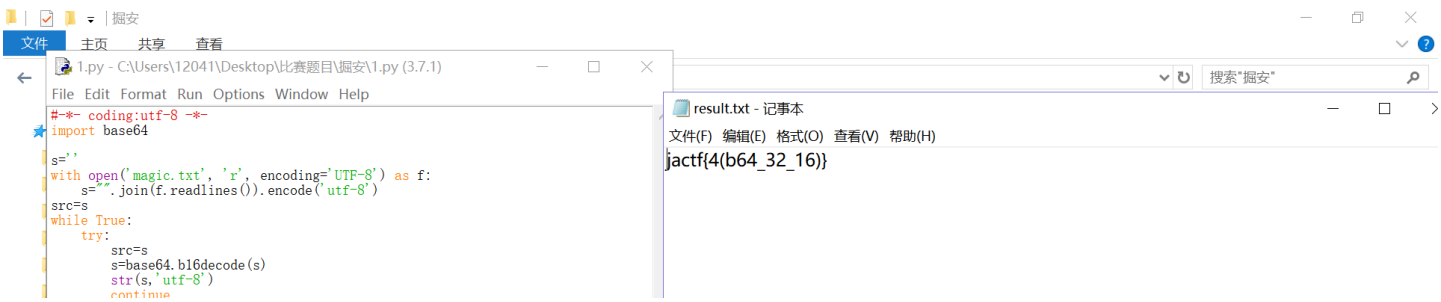
（六）、Crypto：

密码学签到水题，直接base16走一下：



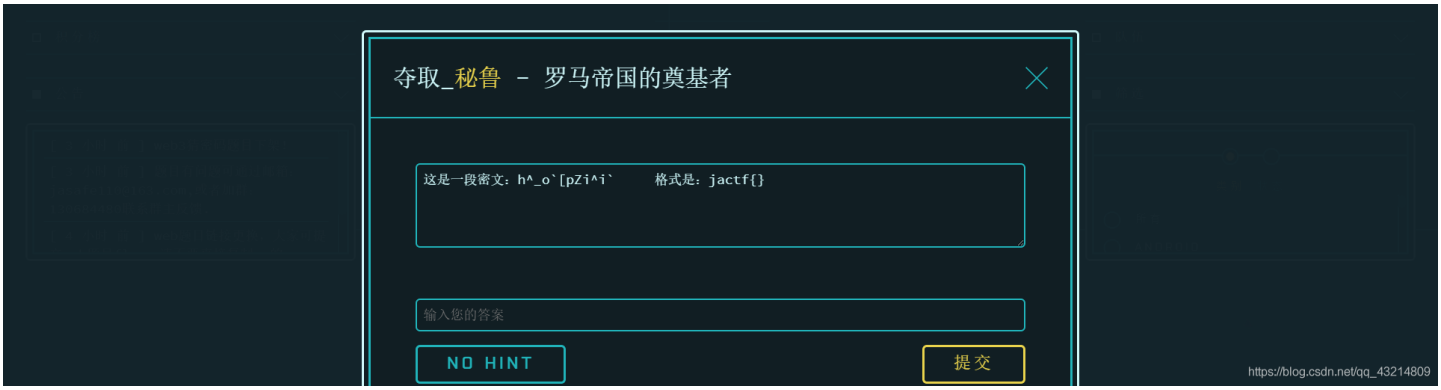
（七）、Crypto：

题目给的很明确，base16、base32、base64全部都参与编码，既然这样的话，普通的解码是得不到flag的，因为是循环的，那就只能python脚本爆破，从网上找了一个，直接用：

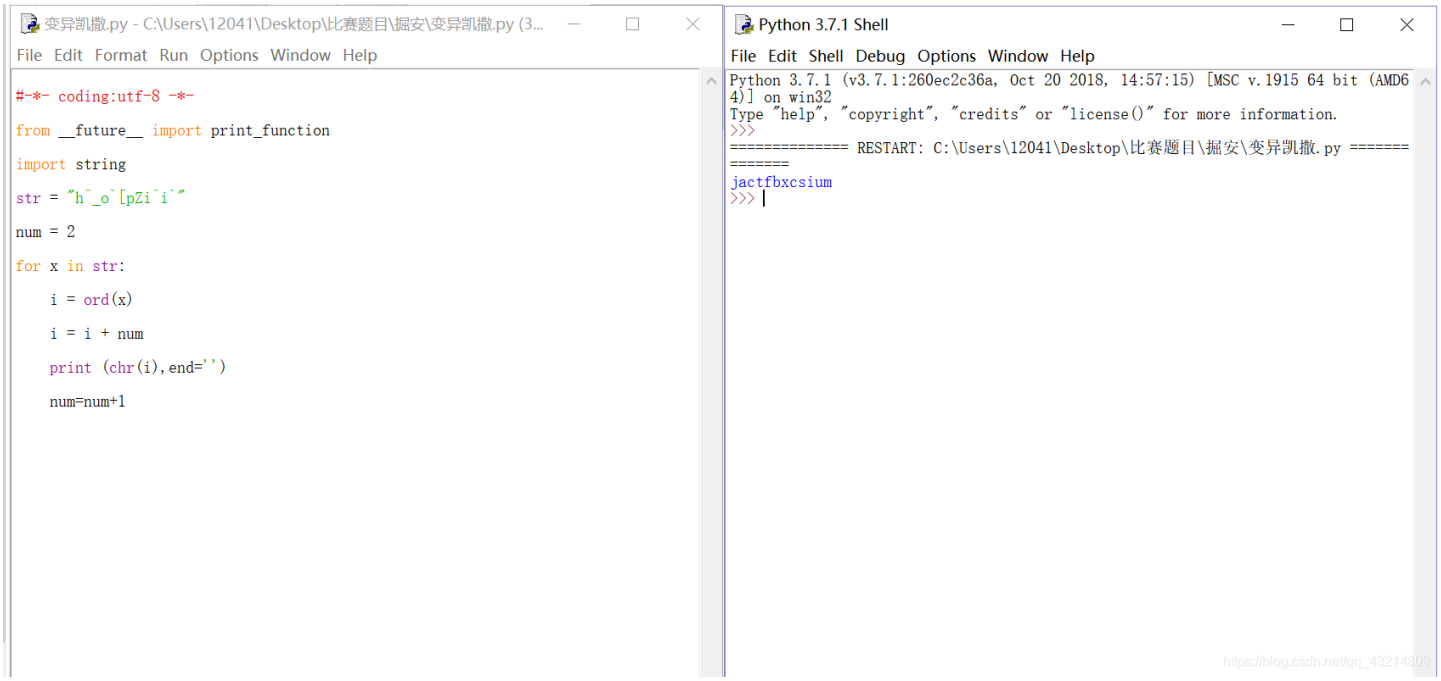


```
    except:
        pass
    try:
        src=s
        s=base64.b32decode(s)
        str(s,'utf-8')
        continue
    except:
        pass
    try:
        src=s
        s=base64.b64decode(s)
        str(s,'utf-8')
        continue
    except:
        pass
    break
with open('result.txt','w', encoding='utf-8') as file:
    file.write(str(src,'utf-8'))
print("ok!")
```


（八）、Crypto：



罗马帝国的奠基者，很明显，凯撒么。但是普通的凯撒加密不能解密，观察格式应该知道这是变异凯撒，通过去找相对应的ascii码，python脚本求解：



二、复现：（主要是web题目）

（一）、Web：

这道题打开后也是一段代码：

```
<?php
error_reporting(0);
if(isset($_GET['action']))  {
        $action  =  $_GET['action'];
}
```

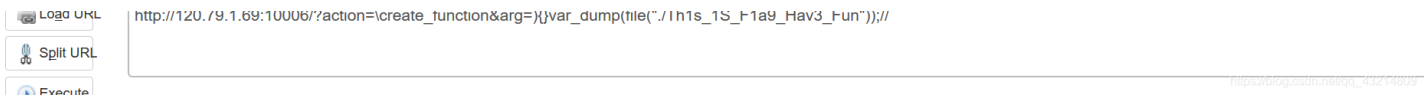
```php
/

if(isset($_GET['action'])){
        $arg  =  $_GET['arg'];
}

if(preg_match('/^[a-z0-9_]*$/isD',  $action)){
        show_source(__FILE__);
}  else  {
        $action($arg,'');
}
```


乍一看还是可以理解的，以GET的方式提交两个变量，一个是action，一个是arg。然后正则匹配，对于action匹配字母数字和下划线，然后就不知道了，后来看了看官方给的writeup，利用create_function()代码注入，绕过正则过滤。
(@_@)表示没太看懂，可能还是太菜了?。按照它说的，找到了P神当年的文章，看了一遍，大体上知道是个怎么个情况。对于正则匹配的那一部分代码，在数字字母下划线都被禁用的情况下调用函数，因为正则里面用了^$，就有可能在开头或结尾加入某个字符绕过正则且函数依旧能正常执行。利用字典fuzz，发现\可以绕过。最后构造出payload，扫描当前目录，找到以下内容：

```
array(5) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(21) "Th1s_1S_F1a9_Hav3_Fun" [3]=> string(9) "index.php" [4]=> string(6) "zx.php" }
```

直接构造payload打开文件，拿flag：

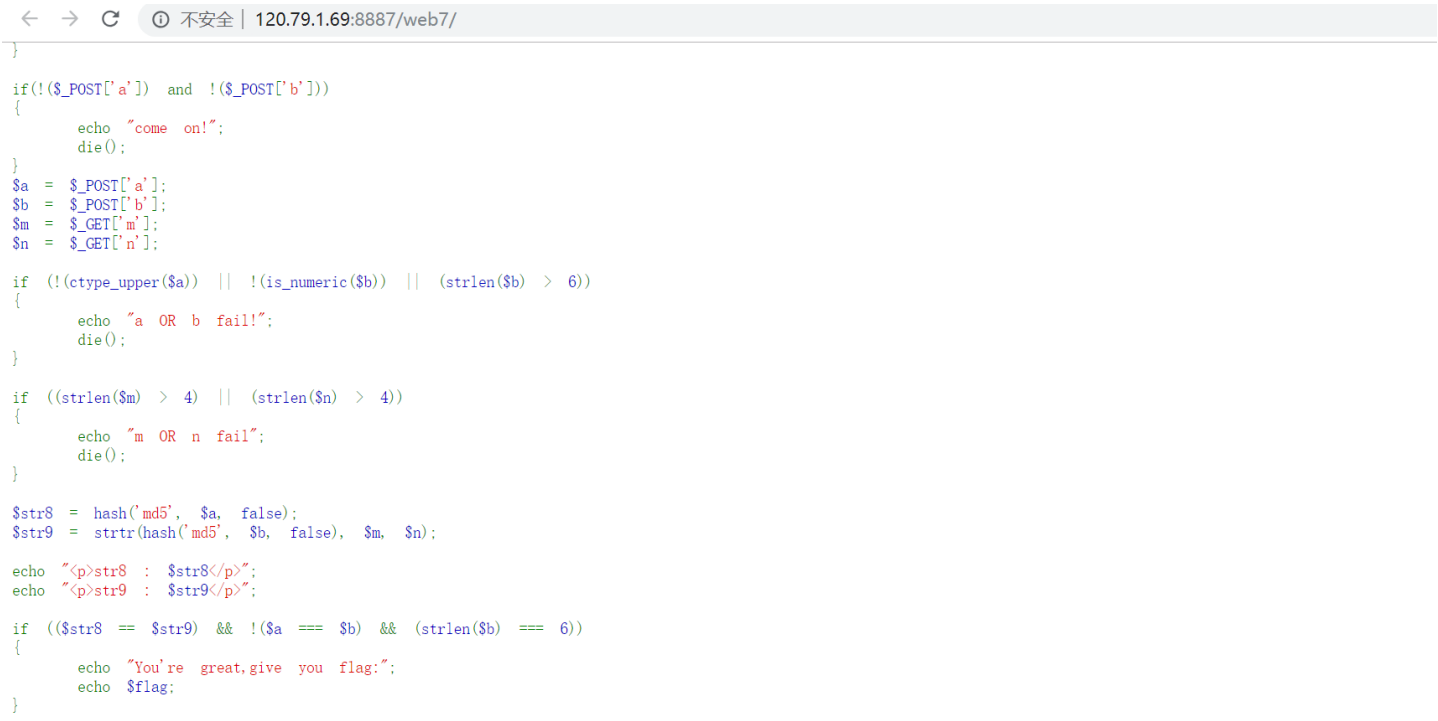
```
array(2) { [0]=> string(40) "jactf{c795359da56ae38ec9132eaad24733fc} " [1]=> string(1) " " }
```



这道题如果直接用之前那道题目的payload显然是行不通的，说实话我也不知道为什么，这一部分知识还是欠缺蛮多的，做了一段时间的代码审计也只不过知道一点皮毛，现在也才意识到自己还有许多盲区待扫。

（二）、Web：

打开后又是代码审计：



str1 OR Sstr2 no no no

前面还有一部分str1、str2、str3、str4的代码，但那部分还是比较好构造的，主要还是后面的str5、str6、str7、str8、str9。

```php
<?php
highlight_file(__FILE__);
include('flag.php');
$str1 = @$_GET['str1'];
$str2 = @$_GET['str2'];
$str3 = @$_GET['str3'];
$str4 = @$_GET['str4'];
$str5 = (string)@$_POST['str5'];
$str6 = (string)@$_POST['str6'];
$str7 = (string)@$_POST['str7'];
if( $str1 == $str2 ){
die('str1 OR Sstr2 no no no');
}
if( md5($str1) != md5($str2) ){
die('step 1 fail');
}
if( $str3 == $str4 ){
die('str3 OR str4 no no no');
}
if ( md5($str3) !== md5($str4)){
die('step 2 fail');
}
if( $str5 == $str6 || $str5 == $str7 || $str6 == $str7 ){
die('str5 OR str6 OR str7 no no no');
}
if (md5($str5) !== md5($str6) || md5($str6) !== md5($str7) || md5($str5) !== md5($str7)){
die('step 3 fail');
}

if(!($_POST['a']) and !($_POST['b']))
{
echo "come on!";
die();
}
```

首先，第一个对于str1、str2、str3、str4，之前遇到过这种题，直接利用弱类型比较，数组绕过。str[]=1&str[]2=2&str[]=3&str[]=4；那么下一步，对于str5、str6、str7，出现了强制类型转化，官方wp给出了通过传入文件使其md5相等，这一点还是当时没想到，有必要记录下来。最后对于a、b、m、n，我们可以看到a必须为大写字母，b为数字而且长

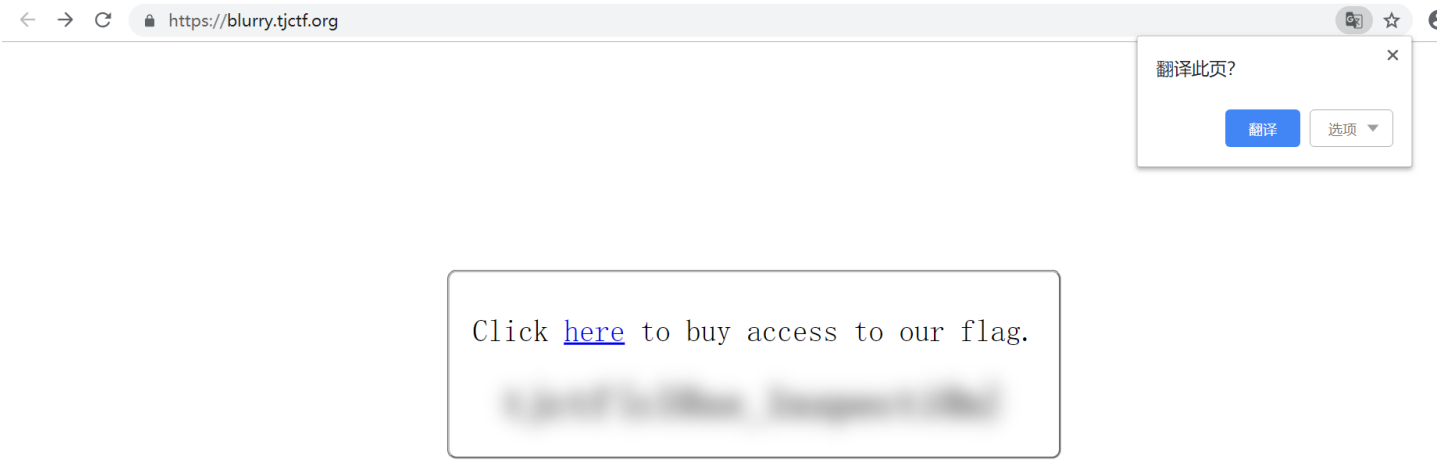
度为6，m和n长度小于4。对于str8和str9，我们可以看到str8是对a作hash加密，str9是对b作hash加密，然后把m替换为n。当然我们也能看到，str8和str9还是利用的弱类型比较。我们知道md5的弱类型比较绕过有很多种方法，官方给出的是0e，我个人感觉这也是日常做题可以想到的，因为常用的字母串也就那些，然后对于str9，b通过hash加密后可以满足0e开头，但是为了满足长度为6，就需要利用后面的替换，把0e后不是数字的替换为数字。官方wp也给出了最后的脚本，直接运行得到flag。

三、TJCTF：

（一）、签到水题：

1.blurry（web）：

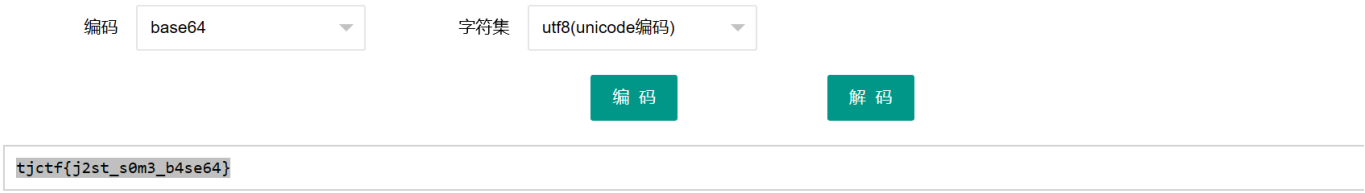
直接view-source：




```
            position: absolute;
            top: 45%;
            left: 50%;
            transform: translate(-50%, -50%);
            font-size: 26px;
        }
    </style>
</head>
<body>
    <fieldset class="cent">
        <p>Click <a href="https://youtu.be/65BrEZxZIVQ">here</a> to buy access to our flag.</p>
        <div class="blur">
            <b id="flag">tjctf{clOse_lnspectiOn}</b>
        </div>
    </fieldset>
</body>
```

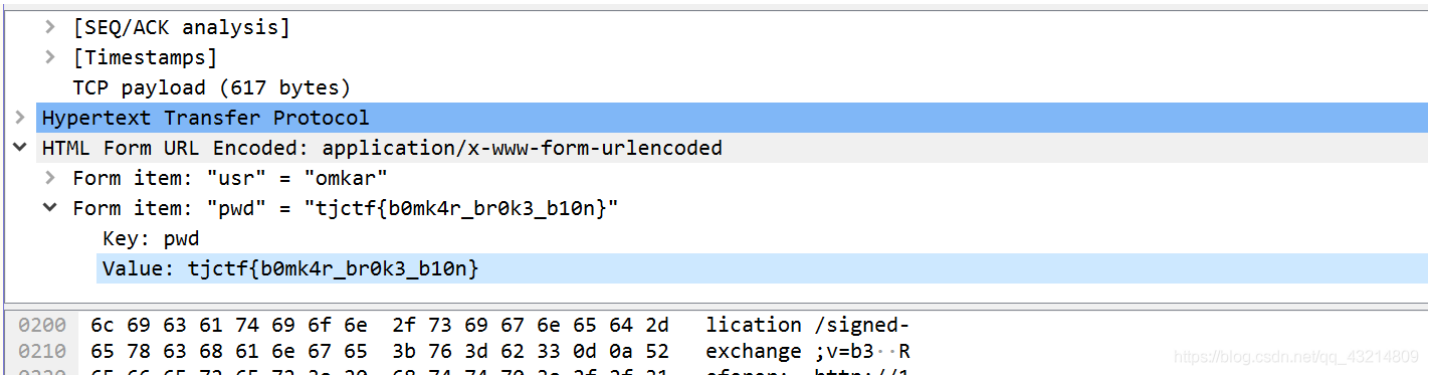

2.Touch Base（Crtpto）：

直接解码：



3.Cable（Forensics）：

直接wireshark：



TJCTF的web题目就不复现了，以我现在的能力还搞不懂，现down下来回头看看再说吧

小结

1.就一个感受，会编写一个python脚本好重要，该努力学学python了，不然以后题都没得做。
2.日常感谢wp提供者。
3.掘安杯好像又出了几道新的cyrpto、misc题目，没时间看了，当然这次比赛还是不错的。
4.前几天的西湖论剑也参加了，昨天参加了一个东南大学主办的“永信杯”，下一篇写写这两个比赛的writeup、复现和感受。