

这船晨了战队

1. 解题过程中，关键步骤不可省略，不可含糊其辞、一笔带过。
2. 解题过程中如是自己编写的脚本，不可省略，不可截图（代码字体可以调小；而如果代码太长，则贴关键代码函数）。
3. 您队伍所有解出的题目都必须书写WRITEUP，缺少一个则视该WRITEUP无效，队伍成绩将无效。
4. WRITEUP如过于简略和敷衍，导致无法形成逻辑链条推断出战队对题目有分析和解决的能力，该WRITEUP可能被视为无效，队伍成绩将无效。
5. 提交PDF版本即可

一、战队信息

- 名称：这船晨了
- 排名：100

二、解题情况

粘贴解题图片

三、解题过程

题目按照顺序填写

Web

nisc_easyweb

进去之后是一个 `phpinfo()`

看了很久没什么东西，拿 xray 扫，扫出来 `/DS_Store` 泄露，
下载了之后看一下

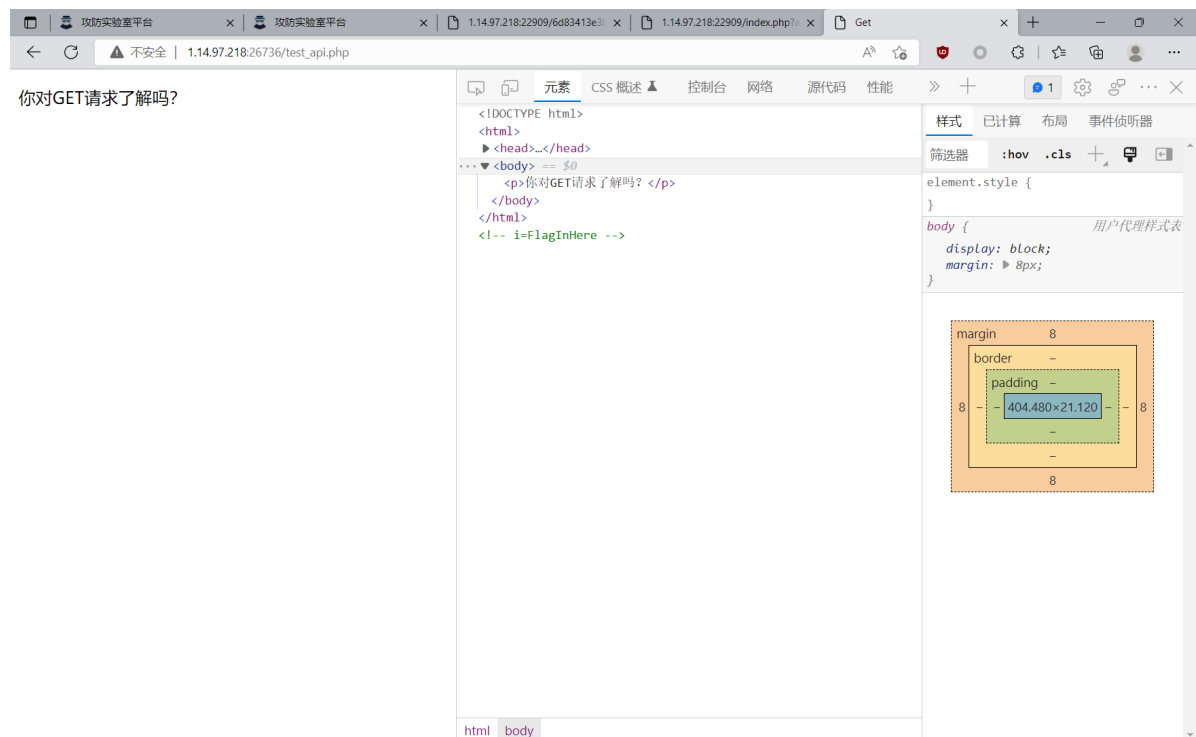
```

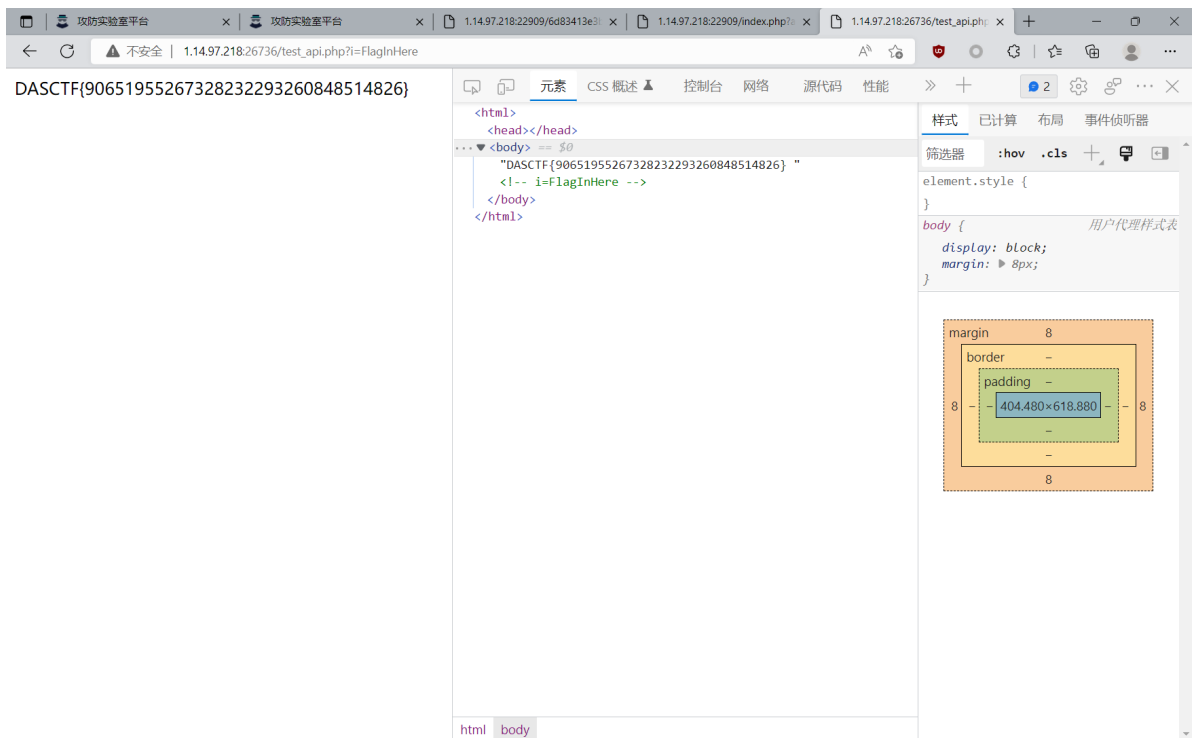
    Bud1
        ocblob
    ocblob
        a p ibwspblob
        plist00?
        ShowStatusBar[ShowToolbar[ShowTabView
        ?
        a p ivSrnlng
    FlagInHere
    ocblob
    A
    robots.txt
    ocblob
    ?
    include.php
    ocblob
    ?
    index
    test_api.php
    ocblob
    ?

```

访问 `include.php` 感觉没什么东西(也可能是我忽略了)

访问 `test_api.php` 要我们传参






DASCTF{90651955267328232293260848514826}

CTF-WEB-nisc_学校门户网站

根据密码规则，注册一个账号，注册之后登录即可

学生系统





☐ 保持登录状态

登录

注册

BITESERVER

备忘录

备忘录

欢迎 ×

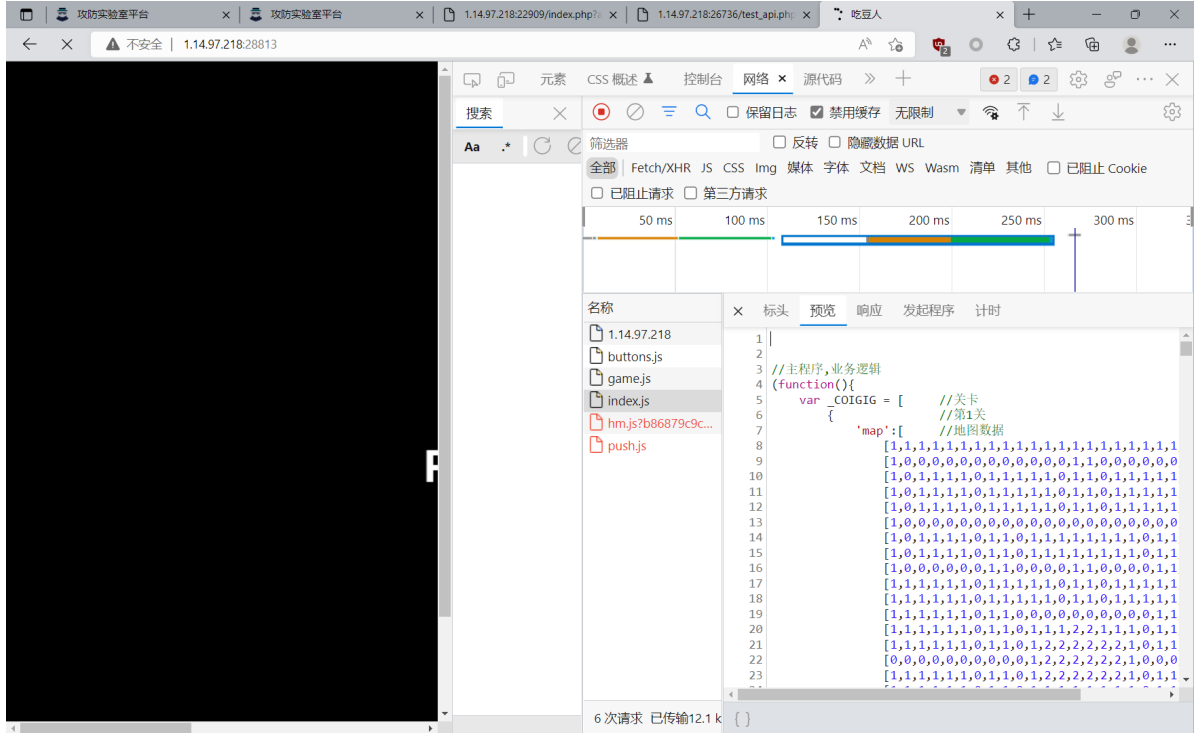
系统的密码

DASCTF{36851892360857182624584638897059}

DASCTF{36851892360857182624584638897059}

吃豆人吃豆魂

js 题目，直接 f12，发现 f12 是被禁用的，所以需要手动打开开发者工具

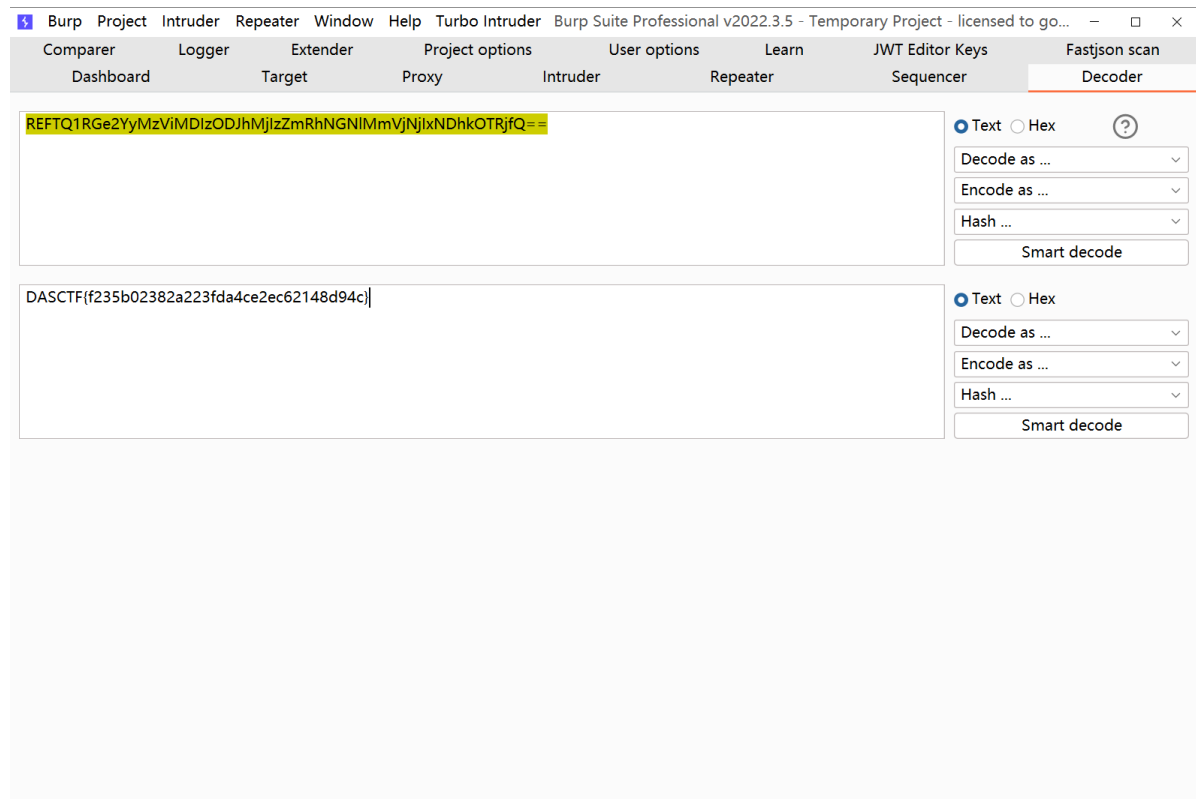


index.js 里面是有东西的，其他都没有

运气很好，一眼就看到了 `base64` 编码的东西

```
ask.py JS temp.js x web4.php web5.php 1
Users > VanHurts > Desktop > JS temp.js > ...
014 var stage = game.createStage();
015 // 游戏结束
016 stage.createItem({
017   x:game.width/2,
018   y:game.height*.35,
019   draw:function(context){
020     context.fillStyle = '#FFF';
021     context.font = 'bold 32px Helvetica';
022     context.textAlign = 'center';
023     context.textBaseline = 'middle';
024     contextthh = window.atob('REFtQ1RGe2YyMzViMDIzODJhMjIzMmRhNGNlMmVjNjIxNDhkOTRjfQ==');
025     context.fillText(_LIFE?'win^^'+alert(contextthh):'OVER!',this.x,this.y);
026   }
027 });
028 // 记分
029 stage.createItem({
030   x:game.width/2,
031   y:game.height*.5,
032   draw:function(context){
033     context.fillStyle = '#FFF';
034     context.font = '20px Helvetica';
035     context.textAlign = 'center';
036     context.textBaseline = 'middle';
037     context.fillText('FINAL SCORE: '+(_SCORE+50*Math.max(_LIFE-1,0)),this.x,this.y);
038   }
039 });
040 // 事件绑定
041 stage.bind('keydown',function(e){
042   switch(e.keyCode){
```

base64 解码



DASCTF{f235b02382a223fda4ce2ec62148d94c}

re

ManyCheck

通过更改跳转过第一关

```
call sub_4013BC
add esp, 4
lea eax, [ebp+var_4]
push eax
push offset Format ; "%d"
call _scanf
add esp, 8
mov ecx, [ebp+var_4]
cmp ecx, [ebp+var_8]
jnz short loc_4010BF ; 改跳转

push offset aBingo ; "Bingo!\n"
call sub_4013BC
add esp, 4
mov dl, byte ptr [ebp+var_8]
mov byte_40CA37, dl
mov eax, [ebp+var_8]
sub eax, 1
mov byte_40CA42, al
call sub_401014 ; 第二关
jmp short loc_4010CC

loc_4010BF:
push offset aWhat
call sub_4013BC
add esp, 4

char v3; // [esp+0h] [ebp-8h]
int v4; // [esp+4h] [ebp-4h] BYREF

v4 = 0;
sub_4013BC((int)aFirstCheck, 77);
sub_4013BC((int)aGuessMyLuckyNu, v1);
scanf("%d", &v4);
if ( v4 != v2 )
    return sub_4013BC((int)aWhatAPity, v1);
sub_4013BC((int)aBingo, v2);
byte_40CA37 = v3;
byte_40CA42 = v3 - 1;
return sub_401014();
}
```

第二关算一下开方

```
sub_4013BC((int)aSecondCheck, v1);
sub_4013BC((int)aLetSDoSomeMath, v1);
sub_4013BC((int)aNN57596388N, v1);
scanf("%d", &v1);
sub_4013BC((int)aMM9812500M, v1);
scanf("%d", &v2);
if ( v1 * v1 != 3025 || v2 * v2 != 2401 )
    return sub_4013BC((int)aWrong, v1);
sub_4013BC((int)aGoodMath, v1);
byte_40CA38 = v1; // v1=55, v2=49
byte_40CA39 = v2;
byte_40CA40 = v2 - 1;
byte_40CA41 = v1 + 1;
return sub_401019();
}
```

第三关位移16位后进行或运算

得到输入数位移方式以及目标数字

```
xt:00401207 call sub_40130C
xt:00401214 add esp, 4
xt:00401217 push offset aGiveMeThisInte ;
xt:0040121C call sub_4013BC
xt:00401221 add esp, 4
xt:00401224 lea eax, [ebp+var_4]
xt:00401227 push eax
xt:00401228 push offset aD_2 ; "%d"
xt:0040122D call _scanf
xt:00401232 add esp, 8
xt:00401235 push 10h
xt:00401237 mov ecx, [ebp+var_4]
xt:0040123A push ecx
xt:0040123B call sub_40100A
xt:00401240 add esp, 8
xt:00401243 cmp eax, 66744769h
xt:00401248 jnz short loc_4012B7

1 int __cdecl sub_4011A0(int a1, char num16)
2 {
3     return (a1 >> (32 - num16)) | (a1 << num16);
4 }
```

计算输入数字

```
a=1718896489
print(a<<16|a>>16)
```

输出 调试控制台 终端 JUPYTER

得到数字：112649600329332

输入后继续运行得到flag


```

0CA30 unk_40CA30 db 44h ; D
0CA31 db 41h ; A
0CA32 db 53h ; S
0CA33 db 43h ; C
0CA34 db 54h ; T
0CA35 db 46h ; F
0CA36 db 7Bh ; {
0CA37 byte_40CA37 db 'M'
0CA38 byte_40CA38 db '7'
0CA39 byte_40CA39 db '1'
0CA3A byte_40CA3A db '_'
0CA3B byte_40CA3B db 'G'
0CA3C byte_40CA3C db 'i'
0CA3D byte_40CA3D db 'f'
0CA3E byte_40CA3E db 't'
0CA3F byte_40CA3F db '_'
0CA40 byte_40CA40 db '0'
0CA41 byte_40CA41 db '8'
0CA42 byte_40CA42 db 'L'
0CA43 byte_40CA43 db '}'
0CA44 byte_40CA44 db 0
0CA45 align 10h

```

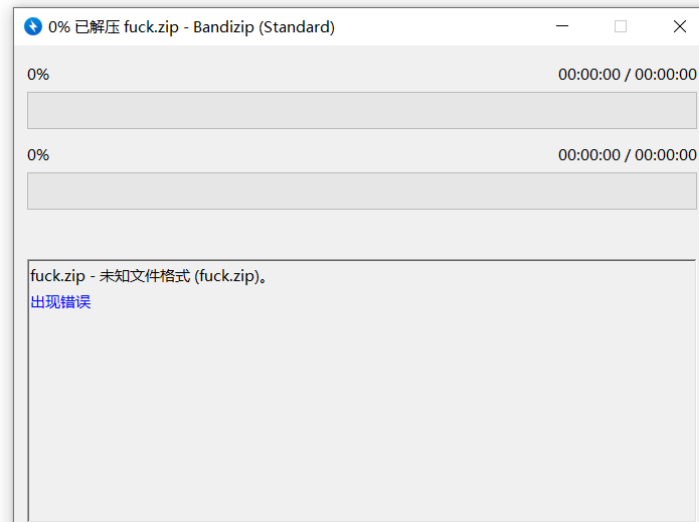
Flag 为: DASCTF{M71_Gift_08L}

misc

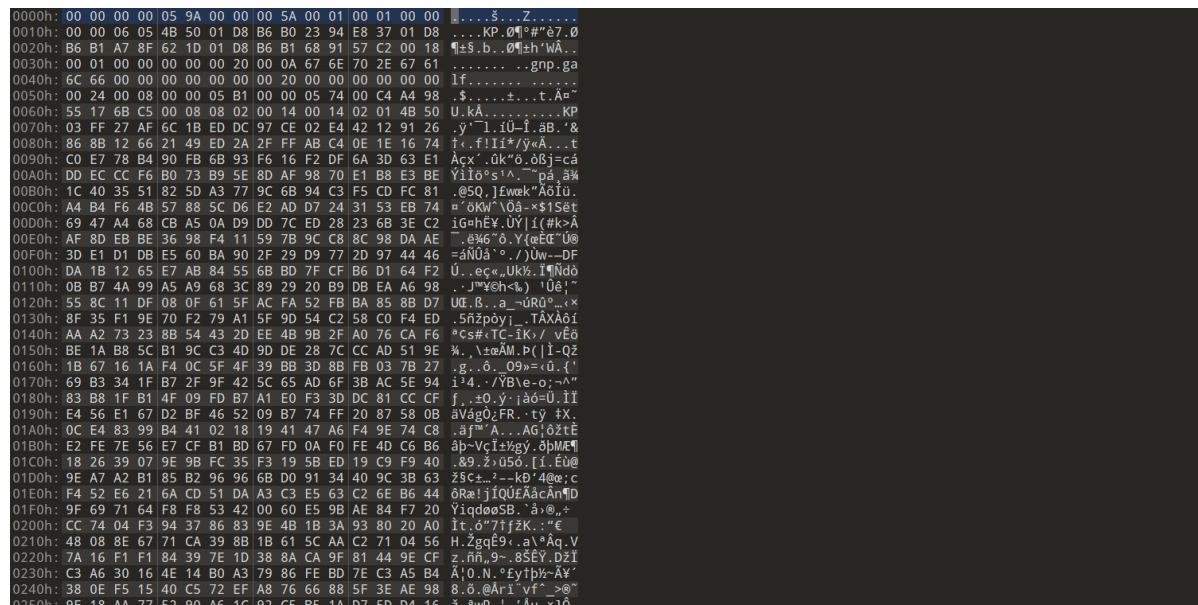
好怪哦

打开文件之后发现打不开

名称	修改日期	类型	大小
 fuck.zip	2022/9/5 14:12	ZIP 压缩文件	2 KB
 segmentFlow.zip	2022/4/19 9:19	ZIP 压缩文件	154 KB



拖进 010 发现文件16进制逆置



编写脚本转为正向

```
with open('fuck.zip','rb') as m:
    list1 = ("{:02X}".format(int(a)) for a in m.read())
    mlist = list(list1)
    print(mlist)
    list2 = mlist[::-1]
    print(list2)
    flag = ''
    for i in list2:
        flag+=i
    print(flag)
```

解压缩之后发现缺少文件头，是一个 png 图片。

添加头 得到 flag

DASCTF{f8b275b06baf4204fa62743eab5eca98}