攻防世界逆向getitWriteup

原创

bin cat 于 2021-11-29 20:06:57 发布 3198 收藏

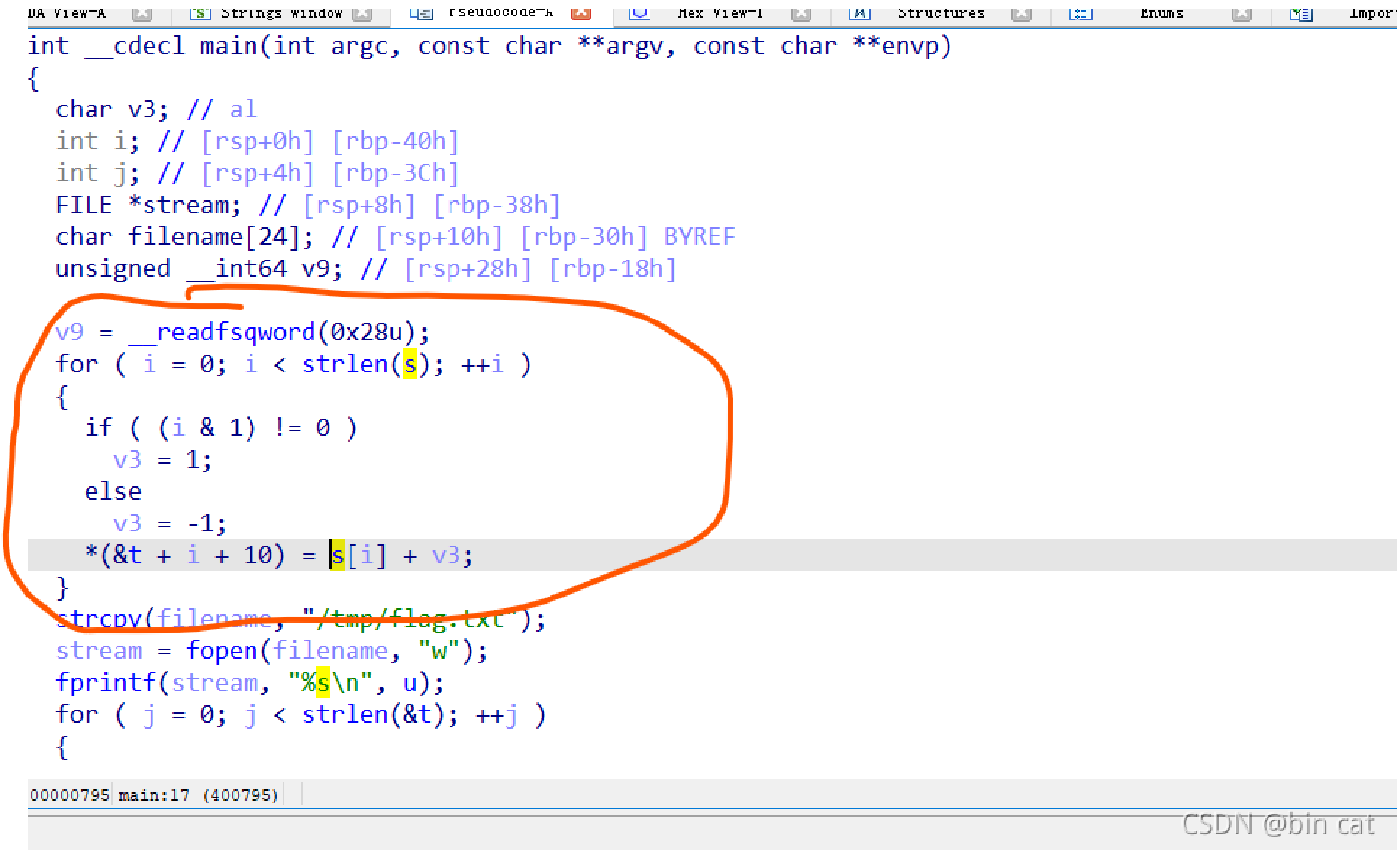
文章标签： 安全

本文链接：https://blog.csdn.net/m0_58348028/article/details/121618073

版权

忽略查壳步骤

直接进入main，转伪代码

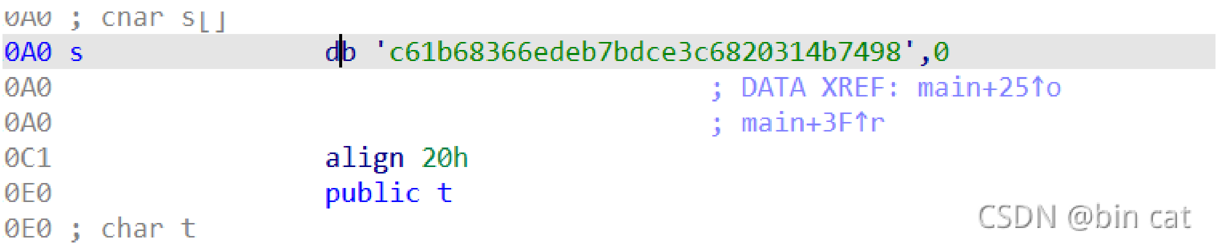


```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char v3; // al
  int i; // [rsp+0h] [rbp-40h]
  int j; // [rsp+4h] [rbp-3Ch]
  FILE *stream; // [rsp+8h] [rbp-38h]
  char filename[24]; // [rsp+10h] [rbp-30h] BYREF
  unsigned __int64 v9; // [rsp+28h] [rbp-18h]

  v9 = __readfsqword(0x28u);
  for ( i = 0; i < strlen(s); ++i )
  {
    if ( (i & 1) != 0 )
      v3 = 1;
    else
      v3 = -1;
    *(&t + i + 10) = s[i] + v3;
  }
  strcpy(filename, "/tmp/flag.txt");
  stream = fopen(filename, "w");
  fprintf(stream, "%s\n", u);
  for ( j = 0; j < strlen(&t); ++j )
  {
```

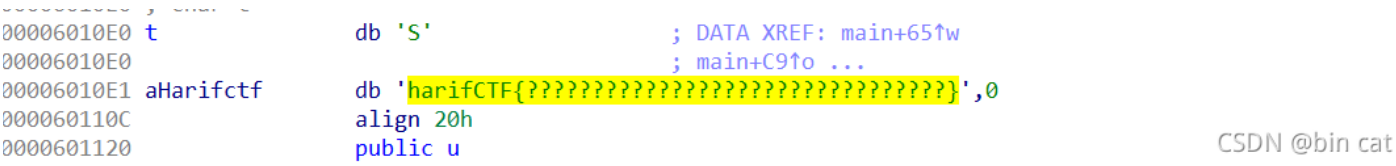
跟下几个重点

s



```
0A0 ; char s[]
0A0 s              db 'c61b68366edeb7bdce3c6820314b7498',0
0A0                                          ; DATA XREF: main+25↑o
0A0                                          ; main+3F↑r
0C1                align 20h
0E0                public t
0E0 ; char t
```

t



```
00006010E0 ; char t
00006010E0 t              db 'S'                  ; DATA XREF: main+65↑w
00006010E0                                        ; main+C9↑o ...
00006010E1 aHarifctf      db 'harifCTF{????????????????????????????????}',0
000060110C                align 20h
0000601120                public u
```

可以发现这里先输入了S

后面还有一串总的来说就是

```
SharifCTF{????????????????????????????????}
```

按照红色圈的逻辑上代码

```
t="SharifCTF{????????????????????????????????}"
s="c61b68366edeb7bdce3c6820314b7498"
i=0
t=list(t)
while(i<len(s)):
    if(i & 1):  #and

        v3=1
    else:
        v3=-1
    t[i+10]=chr(ord(s[i])+v3)
    i+=1
print(t)
flag=''
for xx in t:
    flag+=xx
print(flag)
```

出flag

SharifCTF{b70c59275fcfa8aebf2d5911223c6589}

这里附上一个我看来的C代码

```c
#include <stdio.h>
#include <stdlib.h>
#include <Windows.h>

#pragma warning(disable:4996)

int main(void)
{
    char v3;
    __int64 v5;
    char s[] = "c61b68366edeb7bdce3c6820314b7498";
    char t[] = "SharifCTF{????????????????????????????????}";

    v5 = 0;
    while (v5 < strlen(s)) {
        if (v5 & 1)
            v3 = 1;
        else
            v3 = -1;
        *(t + v5 + 10) = s[v5] + v3;
        v5++;
    }
    printf("%s", t);

    system("PAUSE");
    return 0;
}
```