攻防世界666

原创

Outsider 于 2020-12-24 18:42:04 发布 71 收藏

分类专栏： 攻防世界逆向

本文链接：https://blog.csdn.net/qq_48274326/article/details/111646567

版权

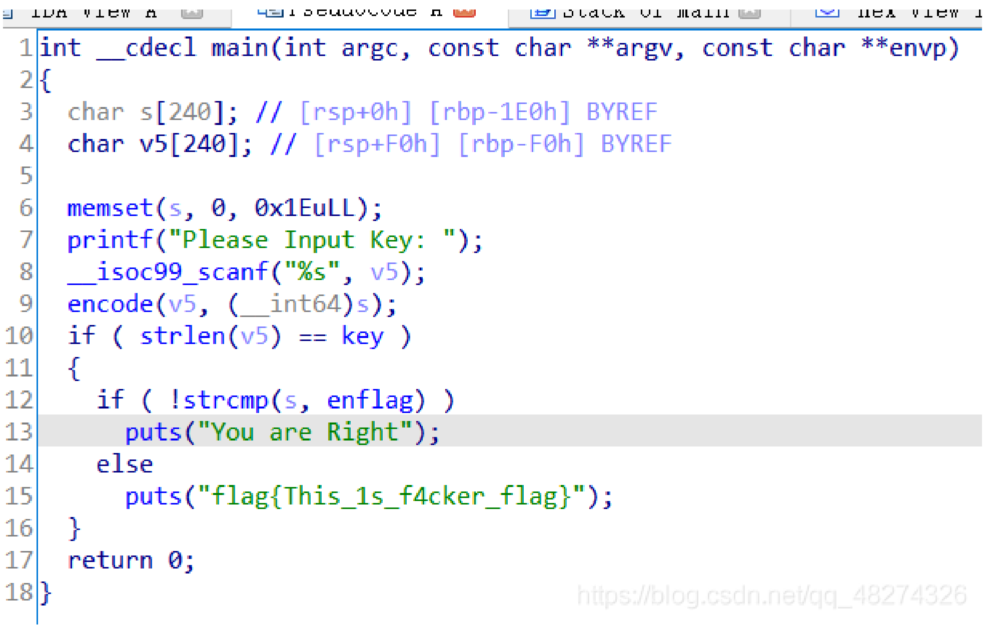
攻防世界逆向 专栏收录该内容

18 篇文章 0 订阅

订阅专栏

攻防世界666

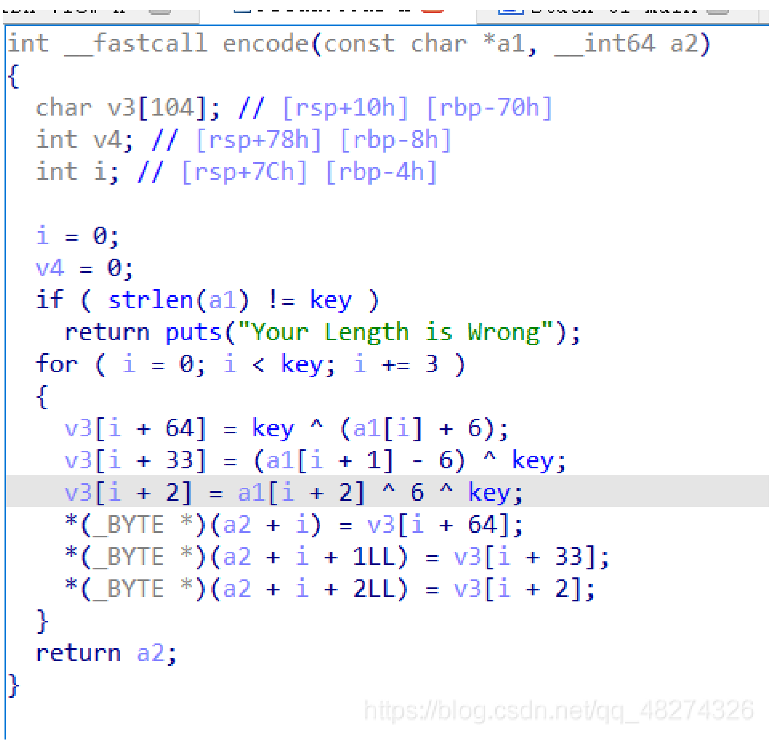
ida打开



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s[240]; // [rsp+0h] [rbp-1E0h] BYREF
  char v5[240]; // [rsp+F0h] [rbp-F0h] BYREF

  memset(s, 0, 0x1EuLL);
  printf("Please Input Key: ");
  __isoc99_scanf("%s", v5);
  encode(v5, (__int64)s);
  if ( strlen(v5) == key )
  {
    if ( !strcmp(s, enflag) )
      puts("You are Right");
    else
      puts("flag{This_1s_f4cker_flag}");
  }
  return 0;
}
```

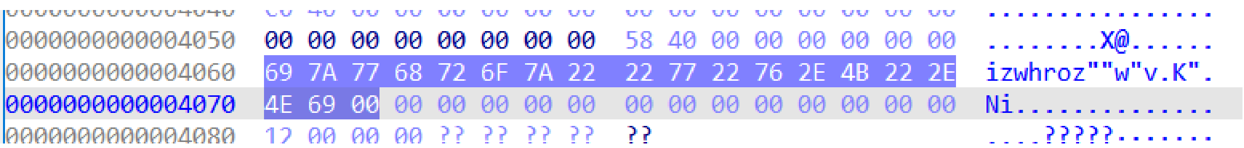
打开encode函数



```
int __fastcall encode(const char *a1, __int64 a2)
{
  char v3[104]; // [rsp+10h] [rbp-70h]
  int v4; // [rsp+78h] [rbp-8h]
  int i; // [rsp+7Ch] [rbp-4h]

  i = 0;
  v4 = 0;
  if ( strlen(a1) != key )
    return puts("Your Length is Wrong");
  for ( i = 0; i < key; i += 3 )
  {
    v3[i + 64] = key ^ (a1[i] + 6);
    v3[i + 33] = (a1[i + 1] - 6) ^ key;
    v3[i + 2] = a1[i + 2] ^ 6 ^ key;
    *(_BYTE *)(a2 + i) = v3[i + 64];
    *(_BYTE *)(a2 + i + 1LL) = v3[i + 33];
    *(_BYTE *)(a2 + i + 2LL) = v3[i + 2];
  }
  return a2;
}
```

寻找key的16进制

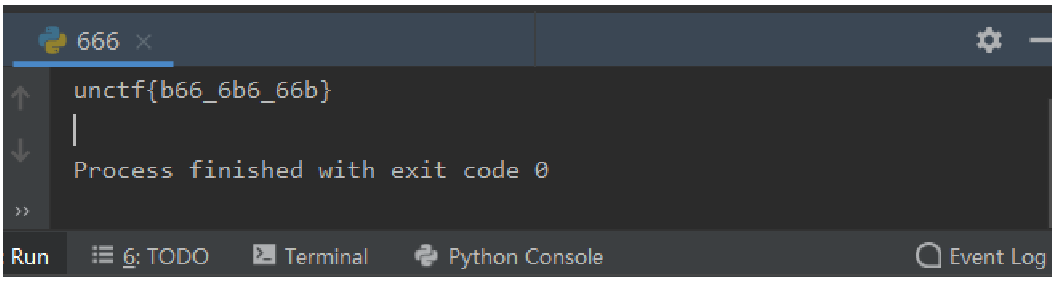


```
0000000000004040  C0 40 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0000000000004050  00 00 00 00 00 00 00 00  58 40 00 00 00 00 00 00  ........X@......
0000000000004060  69 7A 77 68 72 6F 7A 22  22 77 22 76 2E 4B 22 2E  izwhroz""w"v.K".
0000000000004070  4E 69 00 00 00 00 00 00  00 00 00 00 00 00 00 00  Ni..............
0000000000004080  12 00 00 00 ?? ?? ?? ??  ??                       ....?????.......
```

进制转换不错的网站：http://www.ab126.com/goju/1711.html

写个Python脚本

```python
key=[105, 122 ,119, 104, 114,111 ,122 ,34 , 34 ,119, 34, 118, 46 ,75 ,34 ,46 ,78 ,105,0]
flag=''
for i in range(0,18,3):
    flag+=chr((18^key[i])-6)
    flag+=chr((18^key[i+1])+6)
    flag+=chr(18^key[i+2]^6)
print(flag)
```



```
unctf{b66_6b6_66b}

Process finished with exit code 0
```