




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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

```
IDA VIEW A 4E1350000000 A STACK OF main HEX VIEW 1
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   char s[240]; // [rsp+0h] [rbp-1E0h] BYREF
4   char v5[240]; // [rsp+F0h] [rbp-F0h] BYREF
5
6   memset(s, 0, 0x1EuLL);
7   printf("Please Input Key: ");
8   __isoc99_scanf("%s", v5);
9   encode(v5, (__int64)s);
10  if ( strlen(v5) == key )
11  {
12    if ( !strcmp(s, enflag) )
13      puts("You are Right");
14    else
15      puts("flag{This_1s_f4cker_flag}");
16  }
17  return 0;
18 }
```

https://blog.csdn.net/qq_48274326

打开encode函数

```
IDA VIEW A 4E1350000000 A STACK OF main HEX VIEW 1
1 int __fastcall encode(const char *a1, __int64 a2)
2 {
3   char v3[104]; // [rsp+10h] [rbp-70h]
4   int v4; // [rsp+78h] [rbp-8h]
5   int i; // [rsp+7Ch] [rbp-4h]
6
7   i = 0;
8   v4 = 0;
9   if ( strlen(a1) != key )
10    return puts("Your Length is Wrong");
11   for ( i = 0; i < key; i += 3 )
12   {
13     v3[i + 64] = key ^ (a1[i] + 6);
14     v3[i + 33] = (a1[i + 1] - 6) ^ key;
15     v3[i + 2] = a1[i + 2] ^ 6 ^ key;
16     *(_BYTE *) (a2 + i) = v3[i + 64];
17     *(_BYTE *) (a2 + i + 1LL) = v3[i + 33];
18     *(_BYTE *) (a2 + i + 2LL) = v3[i + 2];
19   }
20   return a2;
21 }
```

https://blog.csdn.net/qq_48274326

寻找key的16进制

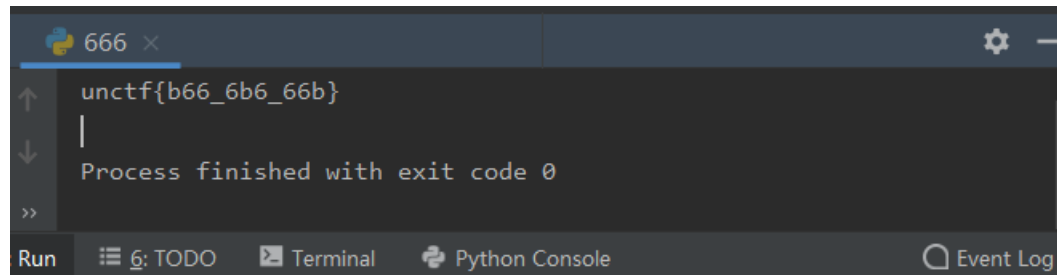
```
0000000000004040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....X@.....
0000000000004050  00 00 00 00 00 00 00 00 58 40 00 00 00 00 00 00  .....X@.....
0000000000004060  69 7A 77 68 72 6F 7A 22 22 77 22 76 2E 4B 22 2E  izwhroz""wv.K".
0000000000004070  4E 69 00 00 00 00 00 00 00 00 00 00 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

```
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)
```



The screenshot shows a Python IDE window titled '666'. The code from the previous block is pasted into the editor. The output console shows the result of the program's execution: 'unctf{b66_6b6_66b}'. Below the output, it states 'Process finished with exit code 0'. The IDE interface includes a 'Run' button, a '6: TODO' list, and tabs for 'Terminal', 'Python Console', and 'Event Log'.

```
666 x
↑ unctf{b66_6b6_66b}
|
↓ Process finished with exit code 0
>>
Run 6: TODO Terminal Python Console Event Log
```