XCTF嘉年华 re1 Writeup

原创

ChengKaoAO 于 2017-10-17 16:00:59 发布

分类专栏： CTF CTF 文章标签： XCTF Reverse

摘要

CTF解题 > XCTF嘉年华体验赛

>> re1

Reverse 题目描述

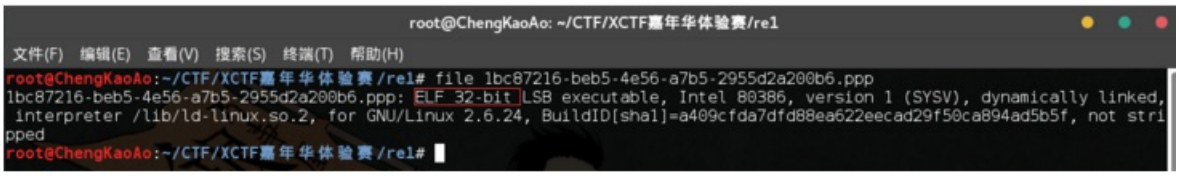
Github https://github.com/Cherishao

it's easy

文件后缀是个.ppp，感觉是个二进制文件，放到kali下查看一下（用file命令查看）。

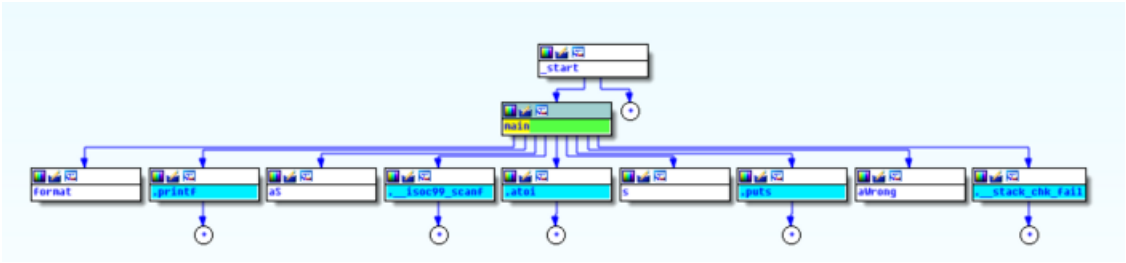
```
root@kali:file 1bc87216-beb5-4e56-a7b5-2955d2a200b6.ppp
```

由结果知，是一个32位的二进制文件。

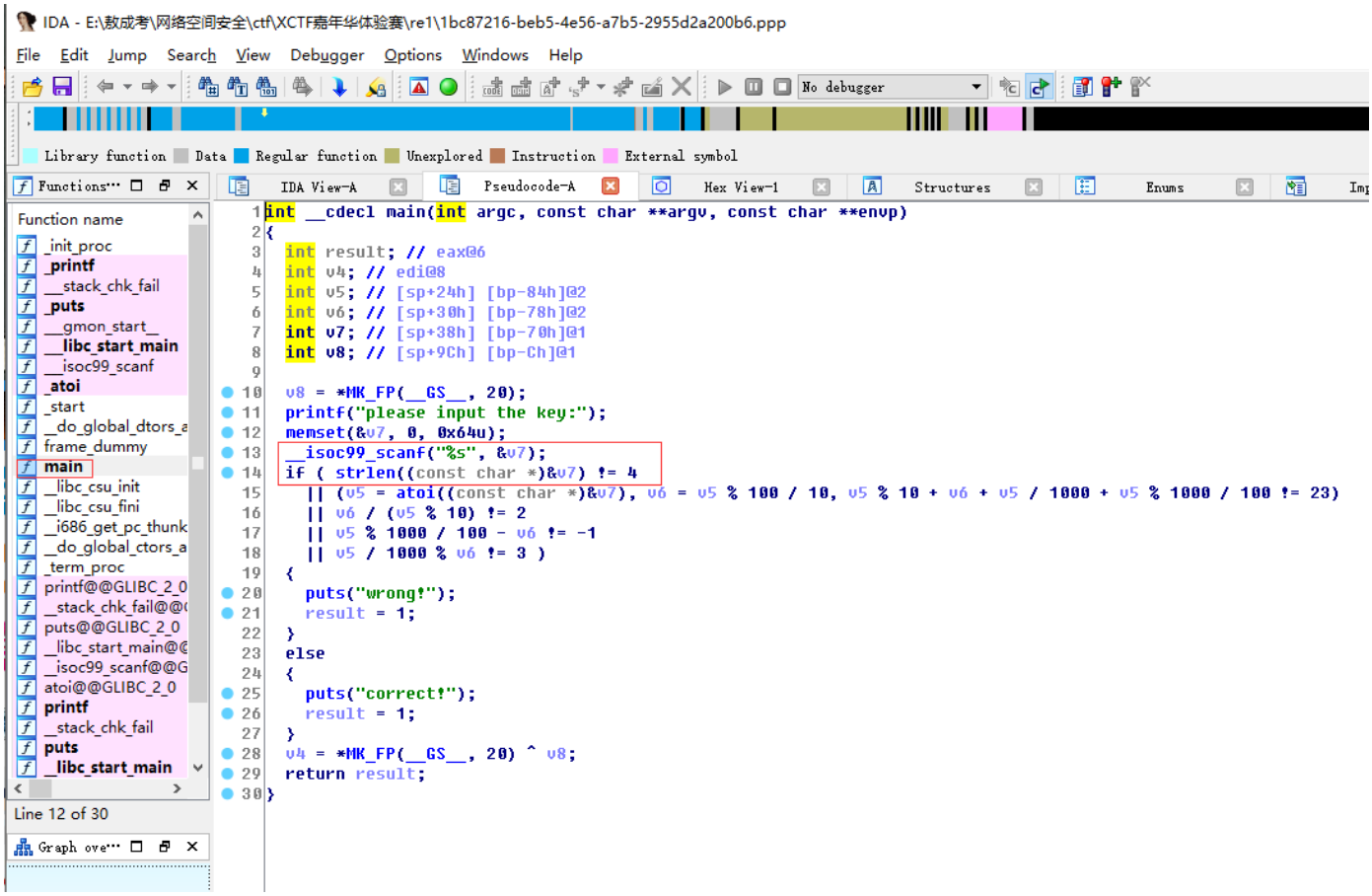


测试运行情况，报错，知需要输入一个正确的值。

64位IDA pro打开，查看到文件的整体结构，找到main函数，双击函数地址，按F5，把汇编变成C语言。



找到main函数，双击函数地址，按F5，把汇编变成C语言，这个函数可以看出，软件的运行流程大致是，先输入一个字符串，然后看这个字符串是否符合一定运算规则，符合运算规则正确，不符合的错误。



在运算规则中，可以看书第一条是检测输入的字符串长度是否为四位数。

- 因此我们就可以写个程序，从1000开始计算，一直循环到9999。

```c
#include <stdio.h>

int main(void)
{
    int count = 0;
    int i = 0, j = 0;
    for (count = 1000; count <= 9999; count++)
    {
        if ((i = count, j = i % 100 / 10, i % 10 + j + i / 1000 + i % 1000 / 100 != 23)
            || (j / (i % 10) != 2)
            || (i % 1000 / 100 - j != -1)
            || (i / 1000 % j != 3))
        {
            continue;
        }
        else
        {
            printf("%d\n", i);
        }
    }

    printf("Hello World!\n");
    return 0;
}
```

直接运行会终端因为有的数字不符合规则，调试碰到错误，跳过这个数字继续。最终我们得到的答案是：