

Открываем в Ghidra. Ищем, какие строки определены в бинарнике

| | | | |
|-----------|------------------------------|-----------------------------------|----|
| 140003418 | Enter username: | "Enter username: " | ds |
| 140003430 | Enter password: | "Enter password: " | ds |
| 140003444 | admin | "admin" | ds |
| 14000344c | C0pl3x | "C0pl3x" | ds |
| 140003458 | You Win ! | "You Win !\n" | ds |
| 140003468 | You entered a wrong password | "You entered a wrong password..." | ds |

В целом данные для входа можно заметить уже здесь, но проверим дополнительно – перейдем в функцию, где они используются

```
FUN_1400015d0((basic_ostream<> *)cout_exref, "Enter username: ");
FUN_1400017a0((basic_istream<> *)cin_exref, (longlong *)&usr_input);
FUN_1400015d0((basic_ostream<> *)cout_exref, "Enter password: ");
FUN_1400017a0((basic_istream<> *)cin_exref, (longlong *)&pwd_input);
uVar4 = local_20;
pppuVar3 = pwd_input;
uVar2 = local_40;
pppuVar1 = usr_input;
ppppuVar6 = &usr_input;
if (0xf < local_40) {
    ppppuVar6 = (undefined8 ****)usr_input;
}
if (local_48 == 5) {
    iVar5 = memcmp(ppppuVar6, "admin", 5);
    if (iVar5 == 0) {
        ppppuVar6 = &pwd_input;
        if (0xf < uVar4) {
            ppppuVar6 = (undefined8 ****)pppuVar3;
        }
        if (local_28 == 6) {
            iVar5 = memcmp(ppppuVar6, "C0pl3x", 6);
            if (iVar5 == 0) {
                pcVar8 = "You Win !\n";
                pbVar7 = (basic_ostream<> *)cout_exref;
                goto LAB_1400013ac;
            }
        }
    }
}
```

Да, предположение оказалось верным – это данные для входа

```
Enter username: admin
Enter password: C0pl3x
You Win !
```