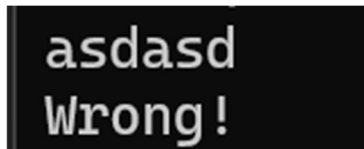


Запускаем программу, вводим строку, получаем «Wrong»



Идем в гидру, ищем вхождения строки

```
140007368 57 72 6f ds s_Wrong!_140007368 "Wrong!\n" XREF[1]: FUN_140003200:140004847(*)
6e 67 21
0a 00
```

Идем в XREF-функцию, смотрим там

```
if (uVar2 == 0) {
    pvStack_1138 = local_e10;
    free(local_e10);
    if (pvStack_1138 == (void *)0x0) {
        local_e08 = 0;
    }
    else {
        local_1288 = (void *)0x8123;
        local_e08 = 0x8123;
    }
    FUN_1400030b0("Correct!\n", uVar5, uVar8, in_R9);
}
else {
    pvStack_1130 = local_e10;
    free(local_e10);
    if (pvStack_1130 == (void *)0x0) {
        local_e00 = 0;
    }
    else {
        local_1288 = (void *)0x8123;
        local_e00 = 0x8123;
    }
    FUN_1400030b0("Wrong!\n", uVar5, uVar8, in_R9);
}
```

Видим функцию, которая проверяет соответствие, смотрим её виртуальный адрес

47b5

Запускаем x634dbg, переходим в модуль программы, переходим к адресу инструкции, ставим точку останова

00007FF6C77F47B5	75 4F	jne stringprotector.7FF6C77F4806
00007FF6C77F47B7	48:8B45 18	mov rax,qword ptr ss:[rbp+18]
00007FF6C77F47B8	48:8985 68010000	mov qword ptr ss:[rbp+168],rax
00007FF6C77F47C2	48:8B8D 68010000	mov rcx,qword ptr ss:[rbp+168]
00007FF6C77F47C9	E8 E20A0000	call stringprotector.7FF6C77F52B0
00007FF6C77F47CE	48:83BD 68010000	cmp qword ptr ss:[rbp+168],0
00007FF6C77F47D6	75 0D	jne stringprotector.7FF6C77F47E5
00007FF6C77F47D8	48:C785 98040000	mov qword ptr ss:[rbp+498],0
00007FF6C77F47E3	EB 13	jmp stringprotector.7FF6C77F47F8
00007FF6C77F47E5	48:C745 18 23810000	mov qword ptr ss:[rbp+18],8123

Запускаем отладку, пока не остановимся в месте проверки

Видим следующее

```
rax=1
qword ptr ss:[rbp+18]=[00000579E2FE58 4"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMN0PQRSTUVWXYZ0123456789!@#$%^&*(){}"]
.text:0007FF6C77F4806 stringprotector.exe:4806 #3C06
```

Кроме того, в стеке также записано

```
000000579E2FE5A8 0000000000000000
000000579E2FE5B0 0000000000000000
000000579E2FE5B8 000001A28F0938F0 "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMN0PQRSTUVWXYZ0123456789!@#$%^&*(){}"
000000579E2FE5C0 0000000000000064
```

Пробуем ввести эту строку

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMN0PQRSTUVWXYZ0123456789!@#$%^&*(){}`
Correct!
```

Или, например, смотрим куда переходит ветвление проверки

```
00007FF6C77F47B5 75 4F jne stringprotector.7FF6C77F4806
00007FF6C77F47B7 48:8B45 18 mov rax,qword ptr ss:[rbp+18]
00007FF6C77F47B8 48:8985 68010000 mov qword ptr ss:[rbp+168],rax
00007FF6C77F47C2 48:888D 68010000 mov rcx,qword ptr ss:[rbp+168]
00007FF6C77F47C9 E8 E20A0000 call stringprotector.7FF6C77F52B0
00007FF6C77F47CE 48:83BD 68010000 0 cmp qword ptr ss:[rbp+168],0
00007FF6C77F47D6 75 0D jne stringprotector.7FF6C77F47E5
00007FF6C77F47D8 48:C785 98040000 0 mov qword ptr ss:[rbp+498],0
00007FF6C77F47E3 EB 13 jmp stringprotector.7FF6C77F47F8
00007FF6C77F47E5 48:C745 18 23810000 mov qword ptr ss:[rbp+18],8123
00007FF6C77F47ED 48:8B45 18 mov rax,qword ptr ss:[rbp+18]
00007FF6C77F47F1 48:8985 98040000 mov qword ptr ss:[rbp+498],rax
00007FF6C77F47F8 48:8D00 592B0000 lea rcx,qword ptr ds:[7FF6C77F7358]
00007FF6C77F47FF E8 ACE8FFFF call stringprotector.7FF6C77F30B0
00007FF6C77F4804 EB 4D jmp stringprotector.7FF6C77F4853
00007FF6C77F4806 48:8B45 18 mov rax,qword ptr ss:[rbp+18]
```

Переходим к дампу по значению

```
00007FF6C77F4806 48:8B45 18 mov rax,qword ptr ss:[rbp+18]
00007FF6C77F480A 48:8985 70010000 mov qword ptr ss:[rbp+168],rax
00007FF6C77F4811 48:888D 70010000 mov rcx,qword ptr ss:[rbp+168]
00007FF6C77F4818 E8 930A0000 call stringprotector.7FF6C77F52B0
00007FF6C77F481D 48:83BD 70010000 0 cmp qword ptr ss:[rbp+168],0
00007FF6C77F4825 75 0D jne stringprotector.7FF6C77F47E5
00007FF6C77F4827 48:C785 A0040000 0 mov qword ptr ss:[rbp+498],0
00007FF6C77F4832 EB 13 jmp stringprotector.7FF6C77F47F8
00007FF6C77F4834 48:C745 18 23810000 mov qword ptr ss:[rbp+18],8123
00007FF6C77F483C 48:8B45 18 mov rax,qword ptr ss:[rbp+18]
00007FF6C77F4840 48:8985 A0040000 mov qword ptr ss:[rbp+498],rax
00007FF6C77F4847 48:8D00 1A2B0000 lea rcx,qword ptr ds:[7FF6C77F7358]
00007FF6C77F484E E8 5DE8FFFF call stringprotector.7FF6C77F30B0
00007FF6C77F4853 48:8B45 28 mov rax,qword ptr ss:[rbp+18]
00007FF6C77F4857 48:8985 60010000 mov qword ptr ss:[rbp+168],rax
00007FF6C77F485E 48:888D 60010000 mov rcx,qword ptr ss:[rbp+168]
00007FF6C77F4865 E8 460A0000 call stringprotector.7FF6C77F52B0
00007FF6C77F486A 48:83BD 60010000 0 cmp qword ptr ss:[rbp+168],0
00007FF6C77F4872 75 0D jne stringprotector.7FF6C77F47E5
00007FF6C77F4874 48:C785 A8040000 0 mov qword ptr ss:[rbp+498],0
00007FF6C77F487F EB 13 jmp stringprotector.7FF6C77F47F8
00007FF6C77F4881 48:C745 28 23810000 mov qword ptr ss:[rbp+18],8123
00007FF6C77F4888 48:8B45 28 mov rax,qword ptr ss:[rbp+18]
```

Видим необходимую строку

```
0000017A9C425A40 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
0000017A9C425A50 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F 80 qrstuvwxyzABCDEF
0000017A9C425A60 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 GHIJKLMNOPQRSTU
0000017A9C425A70 57 58 59 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 WXYZ0123456789!@
0000017A9C425A80 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 #%^&*(){}.`<<<<
```