Reverse - Reverse doesn't like licencer

Le programme nous demande une licence pour se connecter...

Après une analyse du code en statique la licence ne semble pas brute forçable, essayons de patcher le binaire qui réalise une simple comparaison :

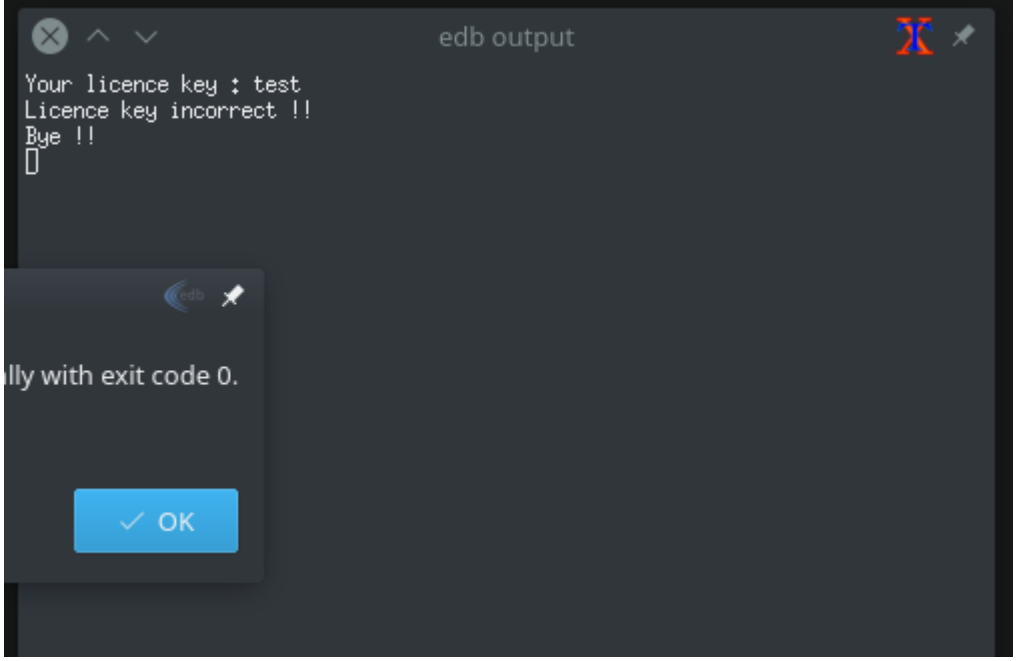
```
int __cdecl main(int argc, const char **argv, const char **er
{
  char v4[48]; // [rsp+0h] [rbp-B0h] BYREF
  char v5[48]; // [rsp+30h] [rbp-80h] BYREF
  char v6[32]; // [rsp+60h] [rbp-50h] BYREF
  char v7[48]; // [rsp+80h] [rbp-30h] BYREF

  strcpy(v7, "521e5bd28cbb28fb5333120540dfaff6");
  printf("Your licence key : ");
  __isoc99_scanf("%s", v6);
  hash_password(v6, v5);
  create_digest(v5, v4);
  if ( (unsigned int)v7 )
    puts("Licence key incorrect !! \nBye !!");
  else
    print_flag(v7, v4);
  return 0;
}
```

Ouvrons edb et essayons de trouver cette comparaison :

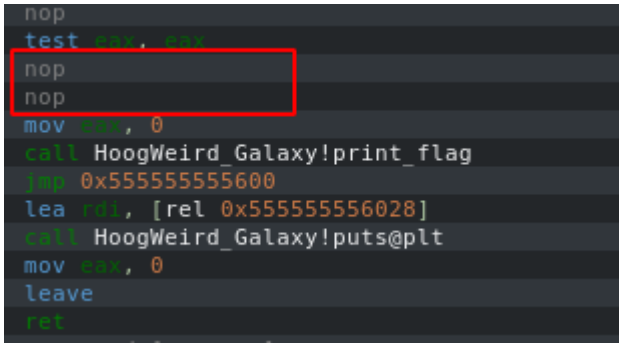
```
lea rax, [rbp-0x80]
mov rsi, rdx
mov rdi, rax
call HoogWeird_Galaxy!create_digest
lea rdx, [rbp-0xb0]
lea rax, [rbp-0x30]
mov rsi, rdx
mov rdi, rax
nop
nop
nop
nop
nop
test eax, eax
jne 0x5555555555f4
mov eax, 0
call HoogWeird_Galaxy!print_flag
jmp 0x555555555600
lea rdi, [rel 0x555555556028]
call HoogWeird_Galaxy!puts@plt
mov eax, 0
leave
ret
nop word [rax+rax]
push r15
lea r15, [rel 0x555555557000]
push r14
mov r14, rdx
push r13
mov r13, rsi
push r12
```

Trouvé !

Essayons sans patch :



maintenant avec le patch :



Et Voila, vous avez patch un binaire :)