# GDB Test Drive

Medium | Reverse Engineering | picoCTF 2022 | binary | gdb

AUTHOR: LT 'SYREAL' JONES

## Description

Can you get the flag?

Download this binary.

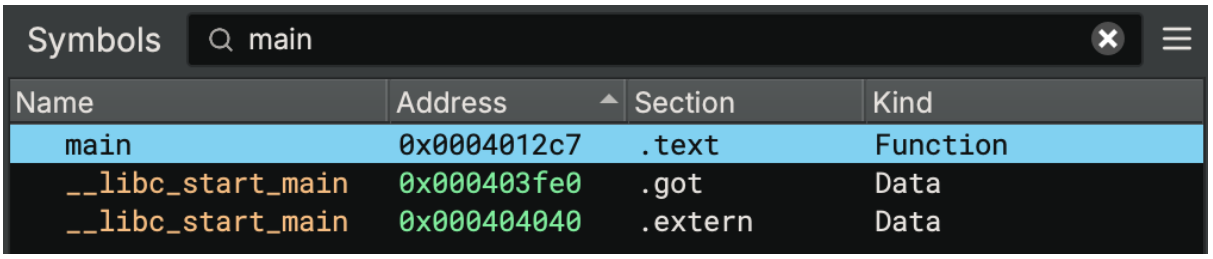
Here's the test drive instructions:

- `$ chmod +x gdbme`
- `$ gdb gdbme`
- `(gdb) layout asm`
- `(gdb) break *(main+99)`
- `(gdb) run`
- `(gdb) jump *(main+104)`

## Hints

(None)

Langsung saja kita mencari fungsi main dari program.




| Name | Address | Section | Kind |
|---|---|---|---|
| main | 0x0004012c7 | .text | Function |
| __libc_start_main | 0x000403fe0 | .got | Data |
| __libc_start_main | 0x000404040 | .extern | Data |

Hasil dari fungsi main adalah berikut.

```
004012c7    int32_t main(int32_t argc, char** argv, char** envp)

004012d3        int32_t argc_1 = argc
004012d6        char** argv_1 = argv
004012da        void* fsbase
004012da        int64_t rax = *(fsbase + 0x28)
004012fd        int64_t var_38
004012fd        __builtin_strncpy(dest: &var_38, src: "A:4@r%uL5b3F88bC05C`Gb0`hf4bfg2N",
004012fd            count: 0x21)
0040132a        sleep(seconds: 0x186a0)
0040133b        char* str = rotate_encrypt(0, &var_38)
00401355        fputs(str, fp: __TMC_END__)
0040135f        putchar(c: 0xa)
0040136b        free(mem: str)
0040136b
00401382        if (rax == *(fsbase + 0x28))
0040138a            return 0
0040138a
00401384        __stack_chk_fail()
00401384        noreturn
```

Jika kita perhatikan, program tersebut menyimpan string tidak jelas pada variabel var_38, lalu jika kita lihat kebawah, string yang disimpan tersebut di enkripsi dengan metode rotate.

Bisa kita asumsikan metode enkripsi tersebut adalah ROT. Lalu kita coba untuk masuk ke dalam fungsi rotate_encrypt() tersebut dan berikut isinya.

```
char* rotate_encrypt(int64_t arg1, char* arg2)

    int64_t var_30 = arg1
    char* result = strdup(s: arg2)
    uint64_t rax_2 = strlen(result)

    for (void* i = nullptr; i u< rax_2; i += 1)
        if (*(i + result) s> 0x20 && *(i + result) != 0x7f)
            int32_t rax_13 = sx.d(*(i + result)) + 0x2f

            if (rax_13 s<= 0x7e)
                *(i + result) = rax_13.b
            else
                *(i + result) = rax_13.b - 0x5e

    return result
```

program tersebut mungkin saja merupakan metode untuk mendecrypt, jadi langsung saja kita konversi ke bahasa c++ saja seperti berikut :

```
#include <cstring>
#include <cstdint>
#include <iostream>

using namespace std;

char* func(int64_t arg1, const char* arg2) {
   (void)arg1;

   char* result = strdup(arg2);
   size_t len = strlen(result);

   for (size_t i = 0; i < len; i++) {
       uint8_t ch = (uint8_t)result[i];

       if (ch > 0x20 && ch != 0x7F) {
           uint8_t shifted = ch + 0x2F;
```

```
            if (shifted <= 0x7E)
                result[i] = shifted;
            else
                result[i] = shifted - 0x5E;
        }
    }

    return result;
}

int main() {
    string p = "A:4@r%uL5b3F88bC05C`Gb0`hf4bfg2N";

    char* output = func(0, p.c_str());
    cout << output << endl;

    free(output);
    return 0;
}
```

```
                                                |___/
GDB-Test-Drive % cd "/Users/user/Docum
atihan/PicoCTF/GDB-Test-Drive/"gdbme
picoCTF{d3bugg3r_dr1v3_197c378a}
GDB-Test-Drive %
```

Hasil run adalah flagnya.