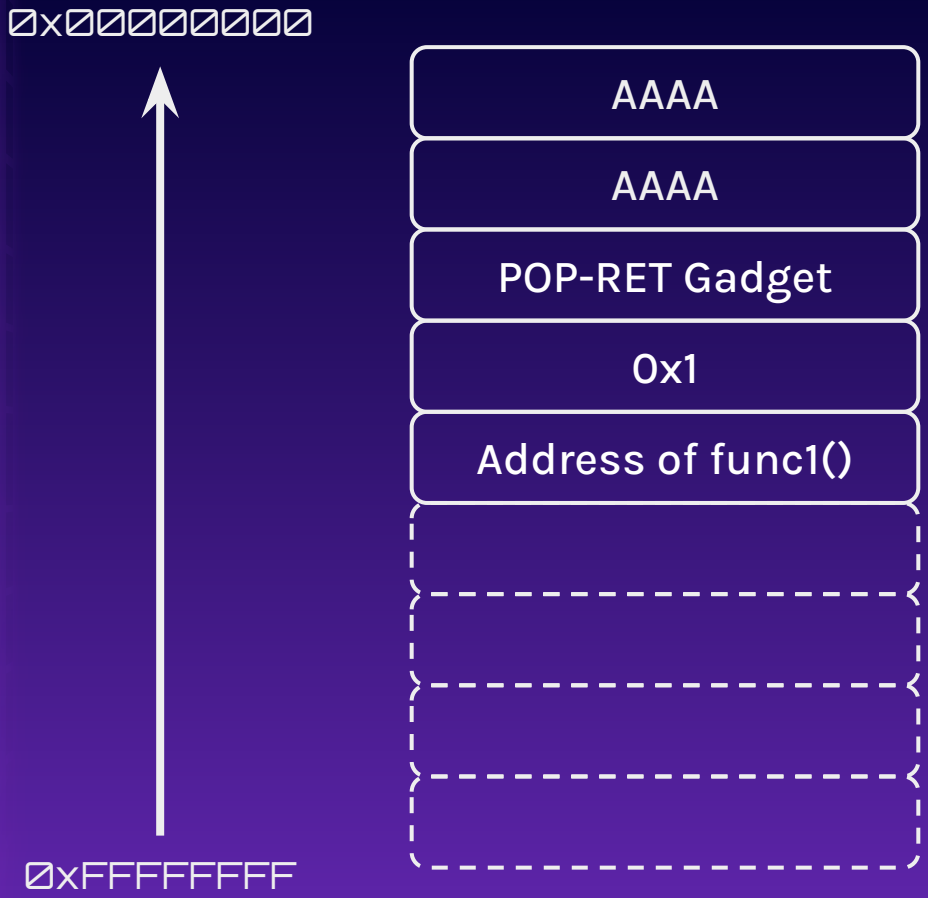
HOW?

64-bit stores parameters
in registers

Find the specific gadget
POP RDI; RET;


0x00000000
0xFFFFFFFF
AAAA
AAAA
POP-RET Gadget
0x1
Address of func1()

ret2func.c

25 mins to pwn ret2func64

Download files at:
http://ctfd.platypew.social

`nc pwn.platypew.social 30005`

```
bool win1 = false;
bool win2 = false;

void func1(int arg1) {
    if (arg1 == 0xdeadbeef)
        win1 = true;
}

void func2(int arg2) {
    if (arg2 == 0xcafebabe)
        win2 = true;
}

void win(char* secret) {
    if (!(win1 && win2)) {
        return;
    }

    if (!strncmp(secret, "magicman", 8))
        system("/bin/sh");
}

void vuln() {
    char buffer[64];
    gets(buffer);
}
```