[hw0x05] writeup

莊翔旭, woolninesun, b04902083

echo

1. 發現輸出是用 dprintf, 有 fmt 的漏洞，且發現 dprintf 的 fd 是 2(stderr)，要先改成 1(stdout) 才能開始 leak 資訊，發現 fd 存在 0x601010 上，且可寫沒開 PIE 可以想辦法改成 1。透過觀察發現可以用 RBP Chain 改掉它，第一個將第二個位置改成 0x601010，下個迴圈後用改過的第二個 address，蓋掉 2 變成 1，就能開始 leak infomation
2. 之後 leak 在 stack 上的 __libc_start_main 的位置算出 libc_base，加上用 `one_gadget libc-2.27.so` 找到限制是 rcx == NULL 的 gadget，串一串控 rip 就能拿到 shell 了。