Unchecked Returns Exercise 3

Intro

StableSwap is a decentralized exchange that allows users to swap stable coins with 0 fees.

Currently it supports 3 tokens: DAI, USDC, and UST.

The exchange already has $3M of TVL in liquidty.

What could go wrong?

Accounts

- 0 - Deployer
- 1 - User1
- 2 - User2
- 3 - User3
- 4 - Attacker (You)

Tasks

Task 1

Find a vulnerability in `StableSwap.sol` and use it to drain ALL the stablecoins from the contract (All the USDC, DAI, and UST). Your attacker EOA account should own all the funds.

Task 2

Fix `StableSwap.sol` and create a secured version without the bug under the `/contracts/unchecked-returns-2/solution/StableSwapSecured.sol`.

Modify the test file so the secured contract will be used, and make sure that your attack fails.