Arithmetic Over/Underflow Exercise 1

Intro

In this exercise, you will have to hack a time vault! When users deposit ETH into the contract it will be locked there for at least 30 days.

The user may extend the wait time if they choose, but once deposited, the user can be sure its ETH is locked in safely for at least 30 days.

Yesterday, you were able to compromise a private key of a user that has ETH locked in the time vault. The problem is that you can't withdraw the ETH because there is a time lock! Can you bypass the timelock restriction and withdraw the ETH from the vault?

Accounts

- 0 - Deployer & Owner
- 1 - Victim (Stolen Keys)
- 2 - Attacker (You)

Tasks

Task 1

Assuming you got the Victim's (account[1]) private key, try to withdraw all his ETH from the timelock contract NOW, WITHOUT waiting 30 days. Then, send it to your Attacker account.

Task 2

Fix the vulnerability in the `Timelock.sol` smart contract, so this attack won't be possible to execute.