Call Attacks 3

CryptoKeeper is a smart contract project designed to provide users with a secure and reliable personal wallet for managing their cryptocurrency assets.

When a user creates a CryptoKeeper wallet, a new instance of the smart contract is deployed through a factory. This method minimizes gas fees by deploying proxy clones for each new wallet instance, which is a clone of a pre-existing wallet instance that acts as a template.

Once a user has created a CryptoKeeper wallet, they can perform various operations, such as sending and receiving cryptocurrencies, interacting with DeFi protocols, checking their account balance, and managing their transaction history.

There are already some users that are using CryptoKeeper wallets. Can you hack them all?

Accounts

- 0 - Deployer
- 1 - User 1
- 2 - User 2
- 3 - User 3
- 4 - Attacker (You)

Tasks

Task 1

Find a vulnerability that will allow you to steal ALL the money from ALL deployed CryptoKeeper wallets.

Task 2

Suggest a way to fix the vulnerability, and make sure that your attack isn't working anymore.