Unchecked Returns Exercise 2

Intro

NFT Escrow is a decentralized application that enables users to securely make escrow agreements by depositing ETH to the contract, specifying the receiver, and locking it for a fixed period.

Upon depositing the receiver receives an NFT, which can be redeemed at the end of the period.

The NFT serves as proof of ownership of the escrowed ETH, and can be redeemed for the ETH.

Upon redeeming, the NFT is burned, and the ETH is sent to the receiver.

Recently, EscrowNFT became popular, and there are already some users that are using it.

Can you find an exploit and steal all the ETH that is stored in the escrow smart contract?

Accounts

- 0 - Deployer & Owner
- 1 - User1
- 2 - User2
- 3 - User3
- 4 - Attacker

Tasks

Task 1

Find a way to drain all the user's ETH from the `Escrow.sol` smart contract!

Task 2

Fix `Escrow.sol` and create a secured version without the bug under the `/contracts/unchecked-returns-2/solution` folder, name your contract `EscrowSecured.sol`.

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