Oracle Manipulation 3

Intro

Following a significant hack in the past, the Lendly team made a pivotal decision to rebrand themselves as "LendLand". They took proactive steps to address the vulnerability that led to the breach. Additionally, they engaged with a reputable Web3 security firm for a comprehensive smart contract audit, which didn't uncover any further issues.

Now, the question remains: Is it still possible to breach their protocol?

You start only with 1 ETH in balance 😢

Note: This exercise is executed on an Ethereum mainnet Fork block number `15969633`. Everything is already configured in the `hardhat.config.js` file

Ethereum MAINNET Addresses

```
WETH Token: 0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2
DAI Token: 0x6B175474E89094C44Da98b954EedeAC495271d0F
Uniswap V2 DAI-WETH Pair: 0xA478c2975Ab1Ea89e8196811F51A7B7Ade33eB11

Impersonated Account (Whale / Binance Hot Wallet):
0xf977814e90da44bfa03b6295a0616a897441acec
```

Accounts

- 0 - Deployer & Owner
- 1 - Attacker (You)

Tasks

Task 1

Drain at least 92% of the protocol funds (again 😉).