SharkTeam

Flash Loan & Reentrancy Attack: Analysis of Hundred and Agave Hack

Mar 17, 2022

SharkTeam, a leading blockchain security service team, offers smart contract audit services for developers. To satisfy the demands of different clients, thesmart contract audit services provide both manual auditing and automated auditing.

We implement almost 200 auditing contents that cover four aspects: high-level language layer, virtual machine layer, blockchain layer, and business logiclayer, ensuring that smart contracts are completely guaranteed and Safe.

Flash Loan & Reentrancy Attack: Analysis of Hundred and Agave Hack

Flash loans attacked both Hundred Finance and Agave, the Gnosis chain's lending protocols, on March 16, 2022. This includes Agave from AAVE, and Hundred Finance from Compound. Losses in excess of $11 million.

SharkTeam analyzed the attack technology for the first time, And summarized the security precautions. He hoped that the following blockchain projects would learn from this and build a security defense line for the blockchain industry.

1. Incident Analysis

Hundred Finance was attacked tx:

0x534b84f657883ddc1b66a314e8b392feb35024afdec61dfe8e7c510cfac1a098

Attack contract: 0xdbf225e3d626ec31f502d435b0f72d82b08e1bdd

Attack address: 0xd041ad9aae5cf96b21c3ffcb303a0cb80779e358

Cross-chain after attack :

https://etherscan.io/txs?a=0xd041ad9aae5cf96b21c3ffcb303a0cb80779e358

Agave was attacked tx:

0xa262141abcf7c127b88b4042aee8bf601f4f3372c9471dbd75cb54e76524f18e

Attack contract 0xF98169301B06e906AF7f9b719204AA10D1F160d6

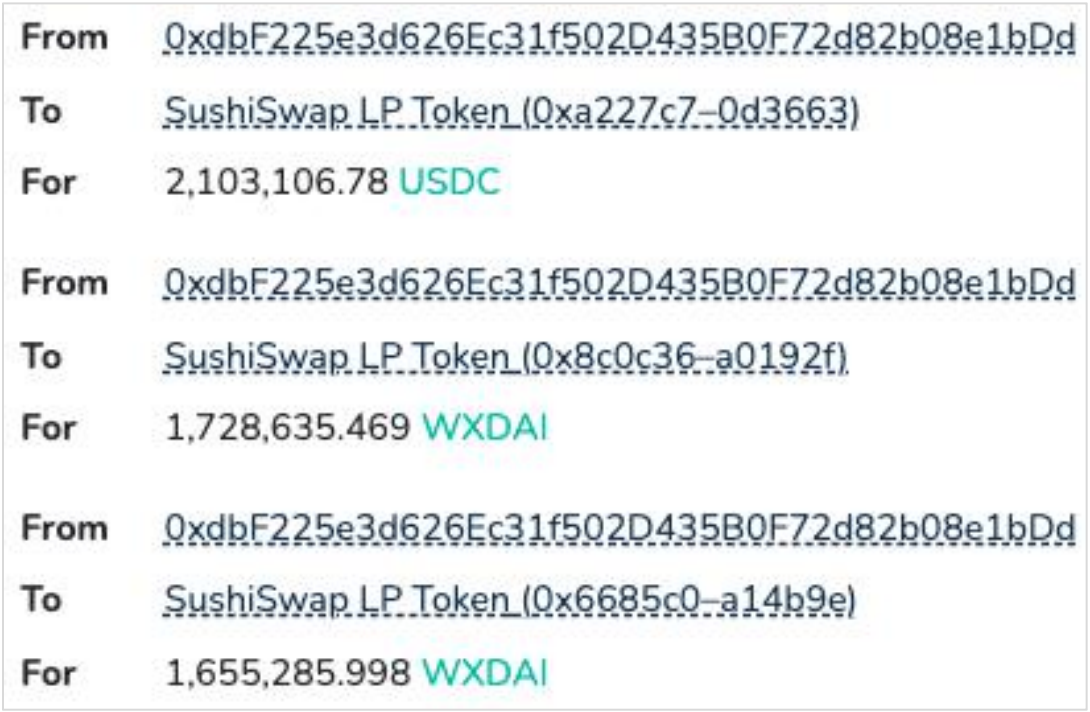
Attack address: 0x0a16a85be44627c10cee75db06b169c7bc76de2c

Cross-chain after the attack:

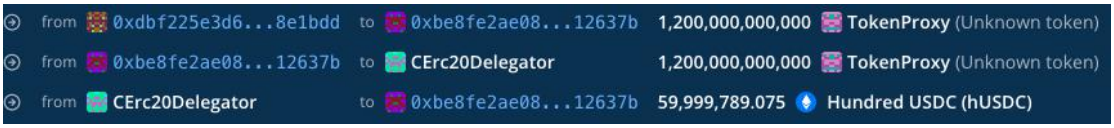
https://etherscan.io/txs?a=0x0a16a85be44627c10cee75db06b169c7bc76de2c

Taking the attack transaction of Hundred Finance Agave as an example, the analysis is as follows:

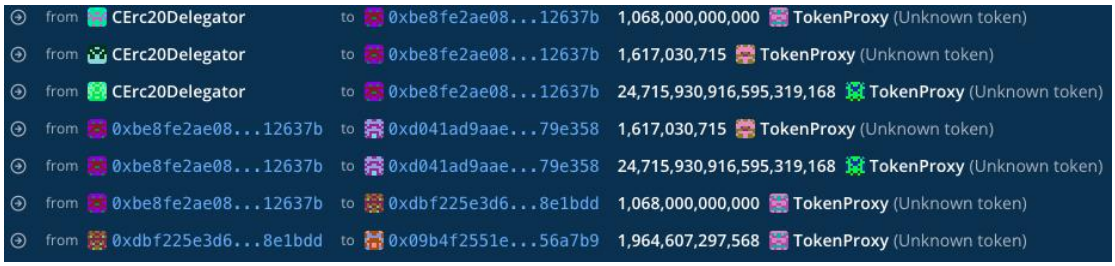
(1) Lend USDC and wXDAI from SushiSwap via Lightning Exchange



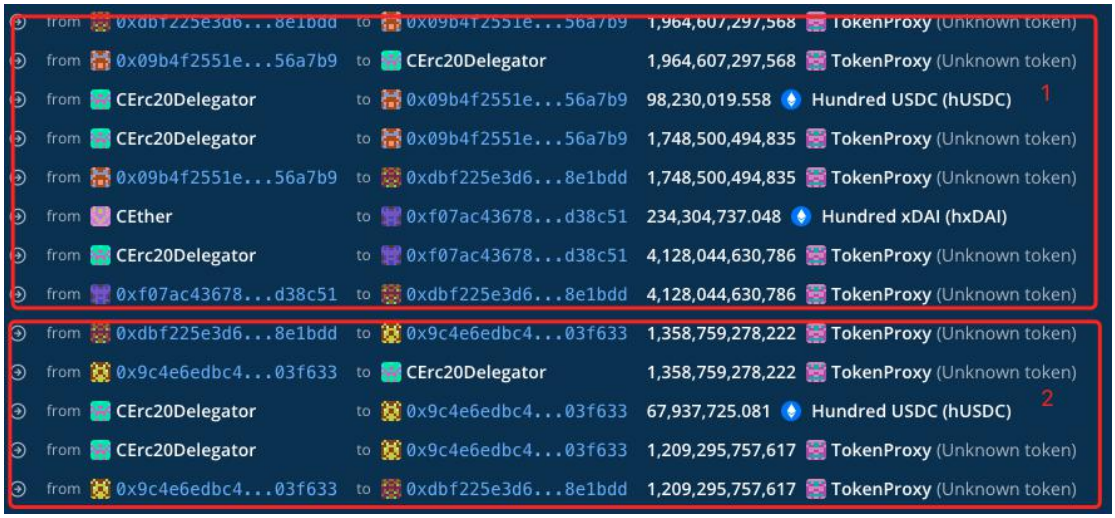
(2) Mortgage 1,200,000 USDC and borrow 59,999,789.075 hUSDC.



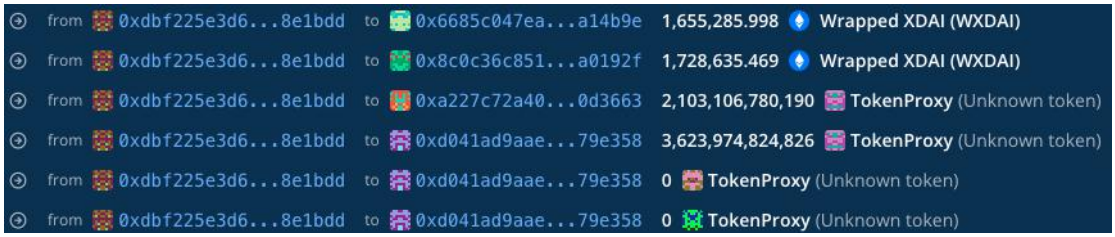
(3) Continue to lend out other tokens, there is obviously an issue with overborrowing.



(4) Continue to overborrow by repeating the same attack.



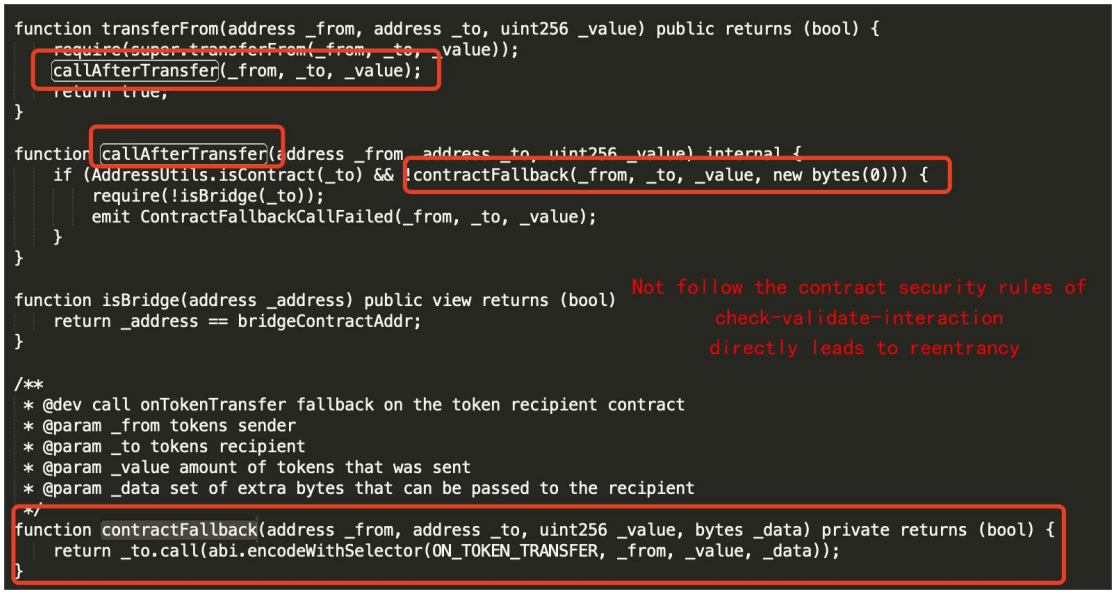
(5) Repay the flash loan and complete the attack.



The main reason of this attack is that there is an over-lending vulnerability in the contract. By analyzing the specific contract, we find that there is a reentrancy problem in the contract, which allows the attacker to complete the attack and perform over-lending.

Problem contract address:

https://blockscout.com/xdai/mainnet/address/0xf8D1677c8a0c961938bf2f9aDc3F3CFDA759A9d9/contracts



2. Security suggestion

SharkTeam reminds you that please be vigilant when setting foot in blockchain projects. Try to choose more stable, More secure, public chains, and projects that have been audited for several rounds, In initiating a transaction. Never put your assets at risk and become a hacker's ATM.

SharkTeam

In Math, We Trust !

https://sharkteam.org

https://t.me/sharkteamorg

https://twitter.com/sharkteamorg