Alpha Finance的闪电贷漏洞

SPELL是Abracadabra的项目治理代币，可用于项目治理和抵押生息

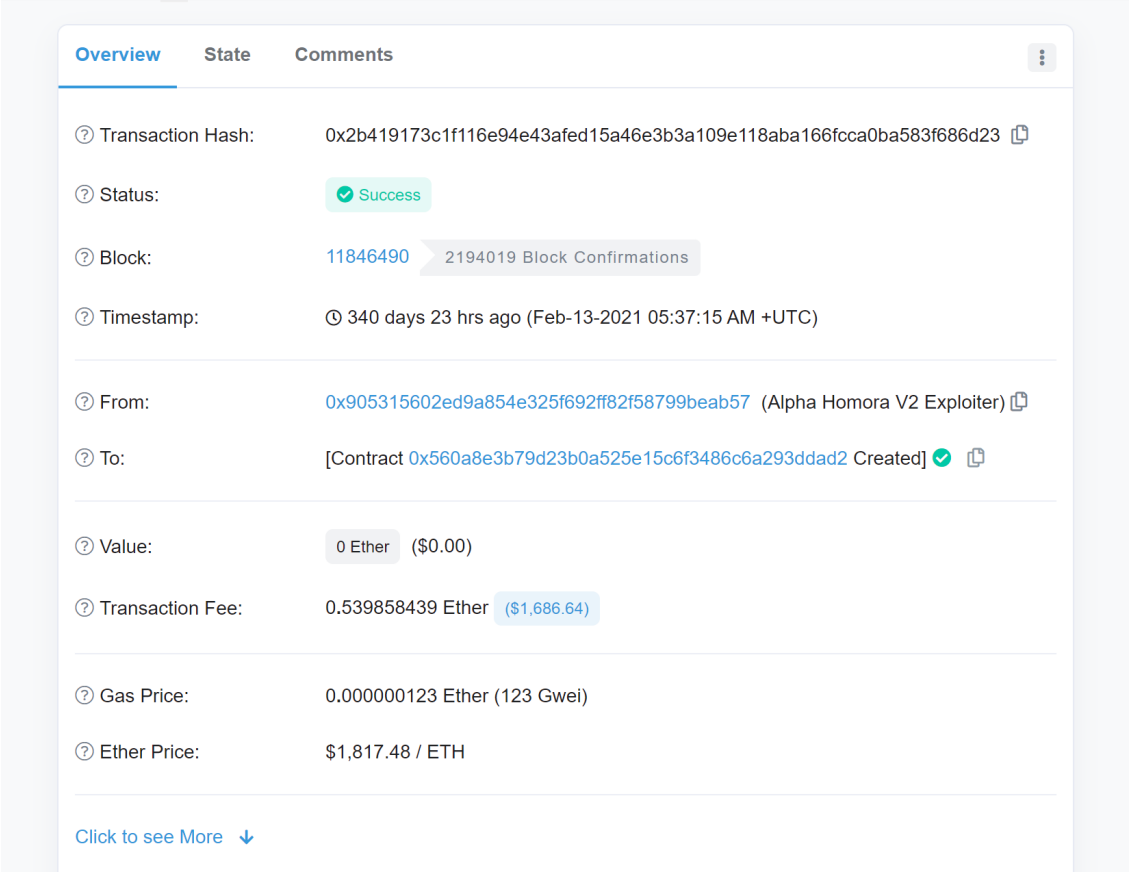
攻击方法

HomoraBankv2允许使用任何自定的spell，这类似Yearn策略，唯一的检查是贷款中使用的抵押品大于借入的金额，在这种情况下，攻击者使用自定义的恶意spell来执行攻击。

过程

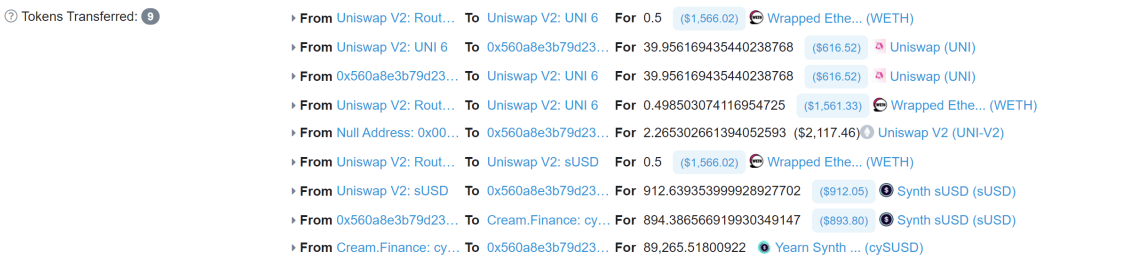
第一阶段 舍入误差利用

1. 攻击者制造了一个恶意的spell，https://etherscan.io/tx/0x2b419173c1f116e94e43afed15a46e3b3a109e118aba166fcca0ba583f686d23



2. 攻击者将ETH交换成UNI，并将ETH+UNI提供给Uniswap池子（获得ETH/UNI LP代币）。同一笔交易中，在Uniswap上交换ETH->sUSD，并将sUSD存入Cream的Iron Bank（获得cySUSD）

   https://etherscan.io/tx/0x4441eefe434fbef9d9b3acb169e35eb7b3958763b74c5617b39034decd4dd3ad



3. 使用恶意的spell调用execute到HomoraBankV2，执行：借用1000^{18} sUSD，将UNI-WETH LP存到WERC20，并在此过程中用作抵押品（绕过collateral > borrow检查），攻击者拥有1000e18 sUSD债务份额（因为攻击者是第一个借款人）https://etherscan.io/tx/0xcc57ac77dc3953de7832162ea4cd925970e064ead3f6861ee40076aca8e7e571

Input Data:

```
Function: execute(uint256 _value, address _to, bytes _data) ***

MethodID: 0x710a9f68
[0]:
0000000000000000000000000000000000000000000000000000000000000000
0
[1]:
000000000000000000000000560a8e3b79d23b0a525e15c6f3486c6a293ddad
2
[2]:
```

Overview | Internal Txns | Logs (12) | State | Comments

Transaction Action:
- Mint of () To 0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2
  - 2,265,302,661,394,050,000 of Token ID [12092999322909806657...]
- Transfer of () From 0x560a8e3b79d23b0a52... To 0x5f5cd91070960d13ee...
  - 2,265,302,661,394,050,000 of Token ID [12092999322909806657...]

From: 0x905315602ed9a854e325f692ff82f58799beab57 (Alpha Homora V2 Exploiter)

Interacted With (To): Contract 0x5f5cd91070960d13ee549c9cc47e7a4cd00457bb

Tokens Transferred: 3
- From Cream.Finance: cy... To 0x5f5cd91070960... For 1,000 ($994.38) Synth sUSD (sUSD)
- From 0x5f5cd91070960... To 0x560a8e3b79d23... For 1,000 ($994.38) Synth sUSD (sUSD)
- From 0x560a8e3b79d23... To 0xe28d9df7718b0... For 2.265302661394052593 ($2,109.65) Uniswap V2 (UNI-V2)

Tokens Transferred: (2 ERC-1155 Transfers found)
- From Null Address: 0x00... To 0x560a8e3b79d23... ERC-1155 For 2265302661394052593 of TokenID [12092999322909806657...] ERC1155
- From 0x560a8e3b79d23... To 0x5f5cd91070960... ERC-1155 For 2265302661394052593 of TokenID [12092999322909806657...] ERC1155

4. 再次使用恶意spell调用execute到HomoraBankV2，利用了协议中的舍入错误，偿还了1000000098548938710983 sUSD（加上利息，实际债务为1000000098548938710984 sUSD），导致偿还份额比总份额少1。结果，攻击者现在有1 minisUSD债务和1份债务份额。https://etherscan.io/tx/0xf31ee9d9e83db3592601b854fe4f8b872cecd0ea2a3247c475eea8062a20dd41

Input Data:

```
Function: execute(uint256 _value, address _to, bytes _data) ***

MethodID: 0x710a9f68
[0]:
0000000000000000000000000000000000000000000000000000000000000037
3
[1]:
000000000000000000000000560a8e3b79d23b0a525e15c6f3486c6a293ddad
2
```

View Input As | Decode Input Data

Status:	Success
Block:	11846608 2194468 Block Confirmations
Timestamp:	341 days 1 hr ago (Feb-13-2021 06:05:57 AM +UTC)
From:	0x905315602ed9a854e325f692ff82f58799beab57 (Alpha Homora V2 Exploiter)
Interacted With (To):	Contract 0x5f5cd91070960d13ee549c9cc47e7a4cd00457bb
Tokens Transferred: 2	From 0x560a8e3b79d23… To 0x5f5cd91070960… For 1,000.000098548938710983 ($998.29) Synth sUSD (sUSD) From 0x5f5cd91070960… To Cream.Finance: cy… For 1,000.000098548938710983 ($998.29) Synth sUSD (sUSD)
Value:	0 Ether ($0.00)
Transaction Fee:	0.1070384 Ether ($335.99)
Gas Price:	0.0000002 Ether (200 Gwei)
Ether Price:	$1,817.48 / ETH

5. 调用sUSD银行的resolveReserve，创建19709787742196债务，总借入份额设为1。当前状态：totalDebt = 19709787742197，而totalShare = 1 https://etherscan.io/tx/0x98f623af655f1e27e1c04ffe0bc8c9bbdb35d39999913bedfe712d4058c67c0e

Input Data:

```
Function: resolveReserve(address token) ***

MethodID: 0xcd607941
[0]:
000000000000000000000000 57ab1ec28d129707052df4df418d58a2d46d5f5
```

View Input As | Decode Input Data

Click to see Less

From:	0x905315602ed9a854e325f692ff82f58799beab57 (Alpha Homora V2 Exploiter)
Interacted With (To):	Contract 0x5f5cd91070960d13ee549c9cc47e7a4cd00457bb
Tokens Transferred:	From Cream.Finance: cy… To 0x5f5cd91070960… For 0.000019709787742196 ($0.00) Synth sUSD (sUSD)
Value:	0 Ether ($0.00)
Transaction Fee:	0.1041422 Ether ($326.73)
Gas Price:	0.0000002 Ether (200 Gwei)
Ether Price:	$1,817.48 / ETH
Gas Limit & Usage by Txn:	802,835 | 520,711 (64.86%)

6. 再次使用恶意spell调用execute到HomoraBankV2，执行（重复16次，每次翻倍借入金额）：借入19709787742196美元并转移给攻击者（每次翻倍，因为每次借入成功totalDebt都翻倍）。在每个阶段，攻击者借入的 minisUSD 比当前的总债务少一个（每次借款翻倍）。由于攻击者只有一个借入份额，这相当于零借入份额，因此协议将其视为无债务借贷。在交易结束时，攻击者将他们设法积累的 19.54 sUSD 存入 Cream 的 Iron Bank。然后，攻击者在另一个事务中重复该过程。这笔存入的 sUSD 最终被用作 USDC 贷款的抵押品，供攻击后期使用。 https://etherscan.io/tx/0x2e387620bb31c067efc878346742637d650843210596e770d4e2d601de5409e3

Input Data:

```
Function: execute(uint256 _value, address _to, bytes _data) ***

MethodID: 0x710a9f68
[0]:
0000000000000000000000000000000000000000000000000000000000000000
0
[1]:
000000000000000000000000560a8e3b79d23b0a525e15c6f3486c6a293ddad
2
[2]:
```

View Input As | Decode Input Data

Tokens Transferred: 34

- From Cream.Finance: cy… To 0x5f5cd91070960… For 0.000019709787742196 ($0.00) Synth sUSD (sUSD)
- From 0x5f5cd91070960… To 0x560a8e3b79d23… For 0.000019709787742196 ($0.00) Synth sUSD (sUSD)
- From Cream.Finance: cy… To 0x5f5cd91070960… For 0.000039419575484392 ($0.00) Synth sUSD (sUSD)
- From 0x5f5cd91070960… To 0x560a8e3b79d23… For 0.000039419575484392 ($0.00) Synth sUSD (sUSD)
- From Cream.Finance: cy… To 0x5f5cd91070960… For 0.000078839150968784 ($0.00) Synth sUSD (sUSD)
- From 0x5f5cd91070960… To 0x560a8e3b79d23… For 0.000078839150968784 ($0.00) Synth sUSD (sUSD)

Scroll for more

Tokens Transferred: 34

($0.32) Synth sUSD (sUSD)

From 0x5f5cd91070960… To 0x560a8e3b79d23… For 0.322925162368139264 ($0.32) Synth sUSD (sUSD)

From Cream.Finance: cy… To 0x5f5cd91070960… For 0.645850324736278528 ($0.65) Synth sUSD (sUSD)

From 0x5f5cd91070960… To 0x560a8e3b79d23… For 0.645850324736278528 ($0.65) Synth sUSD (sUSD)

From 0x560a8e3b79d23… To Cream.Finance: cy… For 19.544369470744682432 ($19.54) Synth sUSD (sUSD)

From Cream.Finance: cy… To 0x560a8e3b79d23… For 1,950.65232027 Yearn Synth ... (cySUSD)

Scroll for more

第二阶段 cySUSD囤积

7. 继续这个过程：再次使用恶意的spell调用execute到HomoraBankV2，执行（重复10次，每次翻倍借来的金额）。在交易结束时，攻击者将1321 sUSD存入Cream的Iron Bank，https://etherscan.io/tx/0x64de824a7aa339ff41b1487194ca634a9ce35a32c65f4e78eb3893cc183532a4

Input Data:

```
Function: execute(uint256 _value, address _to, bytes _data) ***

MethodID: 0x710a9f68
[0]:
0000000000000000000000000000000000000000000000000000000000000000
0
[1]:
000000000000000000000000560a8e3b79d23b0a525e15c6f3486c6a293ddad
2
[2]:
```

Tokens Transferred: 22

From Cream.Finance: cy… To 0x5f5cd91070960… For 330.675366265545444864 ($330.68) Synth sUSD (sUSD)

From 0x5f5cd91070960… To 0x560a8e3b79d23… For 330.675366265545444864 ($330.68) Synth sUSD (sUSD)

From Cream.Finance: cy… To 0x5f5cd91070960… For 661.350732531090889728 ($661.35) Synth sUSD (sUSD)

From 0x5f5cd91070960… To 0x560a8e3b79d23… For 661.350732531090889728 ($661.35) Synth sUSD (sUSD)

From 0x560a8e3b79d23… To Cream.Finance: cy… For 1,321.409764412706992562 ($1,321.41) Synth sUSD (sUSD)

From Cream.Finance: cy… To 0x560a8e3b79d23… For 131,885.08558758

Scroll for more

8. 通过Aave取出1000万美元的USDC贷款，并立即使用Curve发送给Alpha Homora，允许他们提取sUSD。这个sUSD被发送到Cream的Iron Bank，使攻击者可以提取cySUSD。通过反复从 Alpha Homora 借 sUSD 并将其借给 Iron Bank，攻击者能够建立起大量 cySUSD。最后，借给 Alpha Homora 的 USDC 被归还，然后 Aave 的初始闪电贷被偿还。

Tokens Transferred: 29

1 From Aave: aUSDC Tok… To 0x560a8e3b79d23… For 10,000,000 ($10,000,000.00) USD Coin (USDC) 2

From 0x560a8e3b79d23… To Curve.fi: sUSD v2 … For 10,000,000 ($10,000,000.00) USD Coin (USDC) 3

From Curve.fi: sUSD v2 … To 0x560a8e3b79d23… For 4 9,668,335.323847933878106727 ($9,668,335.32) 5 Synth sUSD (sUSD)

From 0x560a8e3b79d23… To Cream.Finance: cy… For 9,668,335.323847933878106727 ($9,668,335.32) Synth sUSD (sUSD)

From Cream.Finance: cy… To 0x560a8e3b79d23… For 964,961,152.19998179 Yearn Synth ... (cySUSD)

From Cream.Finance: cy… To 0x5f5cd91070960… For 1,354,446.300450081800581945 ($1,354,446.30) Synth sUSD (sUSD)

Scroll for more

Tokens Transferred: 29

10,088,930.38819954832496857 ($10,088,930.39) Synth sUSD (sUSD)

From 0x5f5cd91070960… To 0x560a8e3b79d23… For 10,088,930.38819954832496857 ($10,088,930.39) Synth sUSD (sUSD)

From 0x560a8e3b79d23… To Curve.fi: sUSD v2 … For 10,088,930.38819954832496857 ($10,088,930.39) Synth sUSD (sUSD)

From Curve.fi: sUSD v2 … To 0x560a8e3b79d23… For 10,418,583.378592 ($10,418,583.38) USD Coin (USDC)

From Null Address: 0x00… To Aave: Aave Collect… For 8.086381 ($8.09) Aave interes... (aUSDC)

From 0x560a8e3b79d23… To Aave: aUSDC Tok… For 10,009,000 ($10,009,000.00) USD Coin (USDC)

Scroll for more

9. 重复步骤8，这次金额大约是1000万USDC，https://etherscan.io/tx/0xd7a91172c3fd09acb75a9447189e1178ae70517698f249b84062681f43f0e26e
10. 重复1000万USDC，https://etherscan.io/tx/0xacec6ddb7db4baa66c0fb6289c25a833d93d2d9eb4fbe9a8d8495e5bfa24ba57

9,689,298.724170490767391241 ($9,670,288.32) Synth sUSD (sUSD)

From Cream.Finance: cy… To 0x560a8e3b79d23… For 967,051,935.79274729 Yearn Synth ... (cySUSD)

From Cream.Finance: cy… To 0x5f5cd91070960… For 9,689,298.724170490767391241 ($9,670,288.32) Synth sUSD (sUSD)

From 0x5f5cd91070960… To 0x560a8e3b79d23… For 9,689,298.724170490767391241 ($9,670,288.32) Synth sUSD (sUSD)

From 0x560a8e3b79d23… To Curve.fi: sUSD v2 … For 9,689,298.724170490767391241 ($9,670,288.32) Synth sUSD (sUSD)

From Curve.fi: sUSD v2 … To 0x560a8e3b79d23… For 9,991,982.748053 ($9,991,982.75) USD Coin (USDC)

From Null Address: 0x00… To Aave: Aave Collect… For 0.567359 ($0.57) Aave interes... (aUSDC)

From 0x560a8e3b79d23… To Aave: aUSDC Tok… For 10,009,000 ($10,009,000.00) USD Coin (USDC)

第三阶段 恶意提款

11. 在完成上述多次交易后，攻击者积累了大量的 cySUSD。借款13.2k WETH+360万USDC+560万USDT+426万DAI，向Aave供应稳定币（以获得aToken，因此USDC和USDT不能冻结），向Curve a3Crv池子供应aDAI、 aUSDT以及aUSDC，https://etherscan.io/tx/0x745ddedf268f60ea4a038991d46b33b7a1d4e5a9ff2767cdba2d3af69f43eb1b

Tokens Transferred: 20

From Cream.Finance: cy... To 0x560a8e3b79d23... For 13,244.630331762545750401 ($41,525,492.14) Wrapped Ethe... (WETH)

From Cream.Finance: cy... To 0x560a8e3b79d23... For 3,605,354.889525 ($3,605,354.89) USD Coin (USDC)

From Cream.Finance: cy... To 0x560a8e3b79d23... For 5,647,242.107646 ($5,647,242.11) Tether USD (USDT)

From Cream.Finance: cy... To 0x560a8e3b79d23... For 4,263,138.929122643119834654 ($4,263,138.93) Dai Stableco... (DAI)

From Cream.Finance: cy... To 0x560a8e3b79d23... For 0 ($0.00) Synth sUSD (sUSD)

From 0x560a8e3b79d23... To Alpha Homora V2 ... For 0 ($0.00) Synth sUSD (sUSD)

Scroll for more

Tokens Transferred: 20

From 0xdebf206177088... To Aave: aDAI Token ... For 4,263,138.929122643119834654 ($4,263,138.93) Dai Stableco... (DAI)

From Null Address: 0x00... To 0xdebf206177088... For 4,263,138.929122643119834654 ($4,263,138.93) Aave interes... (aDAI)

From 0x560a8e3b79d23... To 0xdebf206177088... For 3,997,921.01617 ($3,997,921.02) USD Coin (USDC)

From Null Address: 0x00... To Aave: Aave Collect... For 5.171324 ($5.17) Aave interes... (aUSDC)

From 0xdebf206177088... To Aave: aUSDC Tok... For 3,997,921.01617 ($3,997,921.02) USD Coin (USDC)

From Null Address: 0x00... To 0xdebf206177088... For 3,997,921.01617 ($3,997,921.02) Aave interes... (aUSDC)

Scroll for more

12. 将a3Crv LP代币添加到Curve的流动性计量器中 https://etherscan.io/tx/0xc60bc6ab561af2a19ebc9e57b44b21774e489bb07f75cb367d69841b372fe896

Tokens Transferred: 2

From Alpha Homora V2 ... To 0xd662908ada2ea... For 13,532,845.885656673015123177 Curve.fi aDA... (a3CRV)

From Null Address: 0x00... To Alpha Homora V2 ... For 13,532,845.885656673015123177 Curve.fi a3C... (a3CRV-...)

13. 攻击者提取的 13.2k 以太币分布在多个不同的地方: 1000ETH发送给IronBank合约部署者，1000ETH发送到Homora合约部署者，220 ETH发送到Tornado Cash，100 ETH发送给gitcoin并资助给Tornado，还剩10925 ETH仍处于攻击者地址余额。

最终，Alpha Homora 攻击者通过利用易受攻击的合约赚取了大约 3750 万美元。

攻击后

针对Alpha Homora的攻击利用了几个主要的安全问题：

- 借用代码中的舍入错误
- 允许使用自定义的spell
- 对resolveReserve函数的公开访问

攻击发生后，Alpha Finance 团队解决了这些问题，并将购买和还款限制为四种代币（ETH、DAI、USDC 和 USDT）。这些更正旨在防止将来发生类似的攻击。

参考链接

https://halborn.com/explained-the-alpha-homora-defi-hack-feb-2021/

https://coingape.com/cream-finance-gets-exploited-for-37-5-million/