Guild Audits

# AN OVERVIEW AND ANALYSIS OF THE MIM-SPELL HACK

Reviewing how it went down , visualizing and getting into the mind of the hacker

**Presented By** @jaydhales @dev_pelz @otaikisadiq @0xkenzman

MARCH 27TH 2024

# AGENDA

Get Ready to get down

| | |
|---|---|
| What is MIM-SPELL ? | 3 |
| Explaining Key-Words | 5 |
| The Attack | 6 |
| How it went Down ? | 7 |
| Code-time ! | 8 |
| Analysis and Mitigation | 9 |
| Conclusion | 10 |

Guild Audits

# What is MIM_SPELL ?

Abracadabra utilizes interest-bearing crypto assets as collateral to borrow its stablecoin, Magic Internet Money (MIM). It aims to provide users with a platform to leverage their assets into a stablecoin. With significant growth, $267.63 million total value locked, and an average APY of 15.58%, it's governed by its token SPELL and powered by Sushi's Kashi Lending technology.

MIM is created with yield-bearing assets, offering users a capital-efficient option to borrow stablecoins through whitelisted assets. It's a unique take on decentralized stablecoin design, providing users with a way to leverage their assets in a capital-efficient manner

Back to Agenda

Guild Audits

# What is MIM_SPELL ?

MIM_SPELL is linked to the Abracadabra Money protocol, comprising Magic Internet Money (MIM) and SPELL tokens. MIM, pegged to the US Dollar, utilizes yield-bearing assets for collateral, offering capital efficiency. SPELL tokens act as the platform's governance token, granting holders governance rights and passive income through staking

Holding SPELL tokens also yields sSPELL tokens, which provide utility and earnings from the protocol. MIM_SPELL is commonly referenced in decentralized exchange trading pairs, where MIM and SPELL are exchanged against each other.

Back to Agenda

# Explaining Key-Words

KeyWords you should take note of

**ELASTIC / BASE VARIABLE**

In the codebase, borrow shares are referred to as base/part and borrow assets amounts are referred to as elastic/amount

**DEGENBOX**

DegenBox is a strategic program created by Abracadabra Money. It's used to solve the issue of accepting non-interest-bearing tokens

**ASSETS/ COLLATERAL**

Assets in web3 refer to tokens , cryptocurrencies like ETH or BTC. Collateral on the other hand refers to digital assets users deposit to secure a loan (also tokens).

**FLASHLOANS**

Type of loan in the DeFi space where a user borrows assets with no upfront collateral and returns the borrowed assets within the same blockchain transaction

**INFLATION ATTACK**

Artificial increase in total supply of tokens , often by exploiting a flaw in the  smart contract code, leading to devaluation of the system's native token.

**PROTOCOL MECHANISM**

The protocol uses shares mechanism to calculate a user's current debt. When a user borrows certain funds, they get minted borrow shares based on current totalBorrowAssets and totalBorrowShares Ratio.

As interest is owed from the user, totalBorrowAssets increases without totalBorrowShares increasing and in turn it increases the proportional amount that the user has to repay as well

Back to Agenda

Back to Agenda

# THE ATTACK

## OVERVIEW

In January 2024, MIM_SPELL suffered an inflation attack ny utilizing flashloans, resulting in a loss of **$6.4 million**

## PROPONENTS

The essence of the attack was an accuracy problem when calculating loan variables, which caused key variables to be manipulated and proportions to be out of balance, resulting in excessive lending of MIM tokens.

1. Alice wants to borrow funds.

2. The protocol calculates the exchange rate by dividing total borrowed assets by total borrow shares.

3. Alice receives borrow shares when she borrows, based on the current exchange rate.

4.If the exchange rate is 10, and Alice borrows 100 units, she gets 10 borrow shares.

5. Over time, interest accrues on Alice's loan, increasing the total borrowed assets.

6. Bob, another borrower, has borrow shares that remain the same even as total borrowed assets increase.

7. The exchange rate goes up if total borrowed assets increase but number of shares stays the same.

8. A higher exchange rate means each of Alice's borrow shares represents a larger portion of the borrowed assets.

9. This effectively increases Alice's total debt because each share she holds represents more to repay.

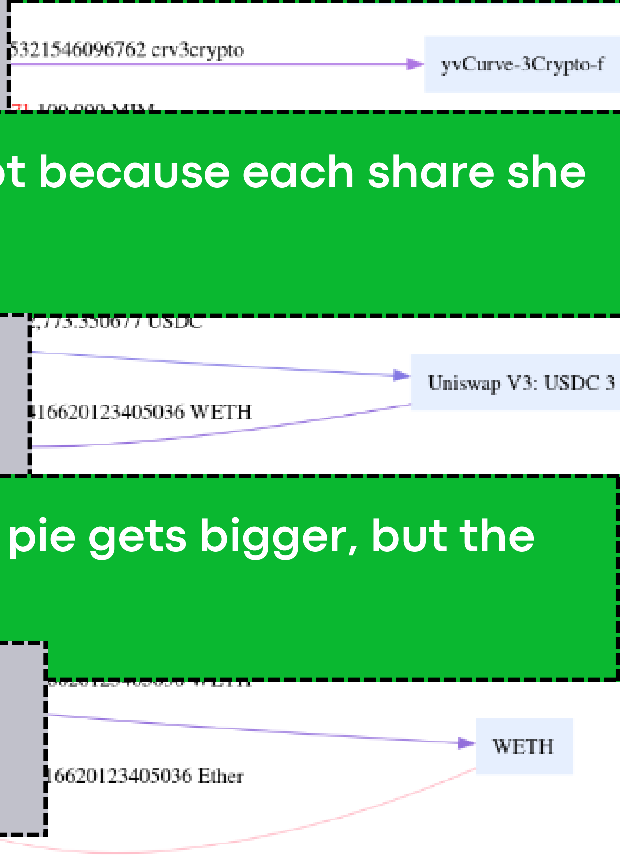
10. Imagine a pie representing the total borrowed assets, and each borrow share is a slice of that pie.

11. When Alice borrows and interest accrues, the pie gets bigger, but the number of slices stays the same.

12. As a result, each slice becomes a bigger portion of the pie, representing a larger debt for Alice.

13. This system helps track debt efficiently, even with interest.

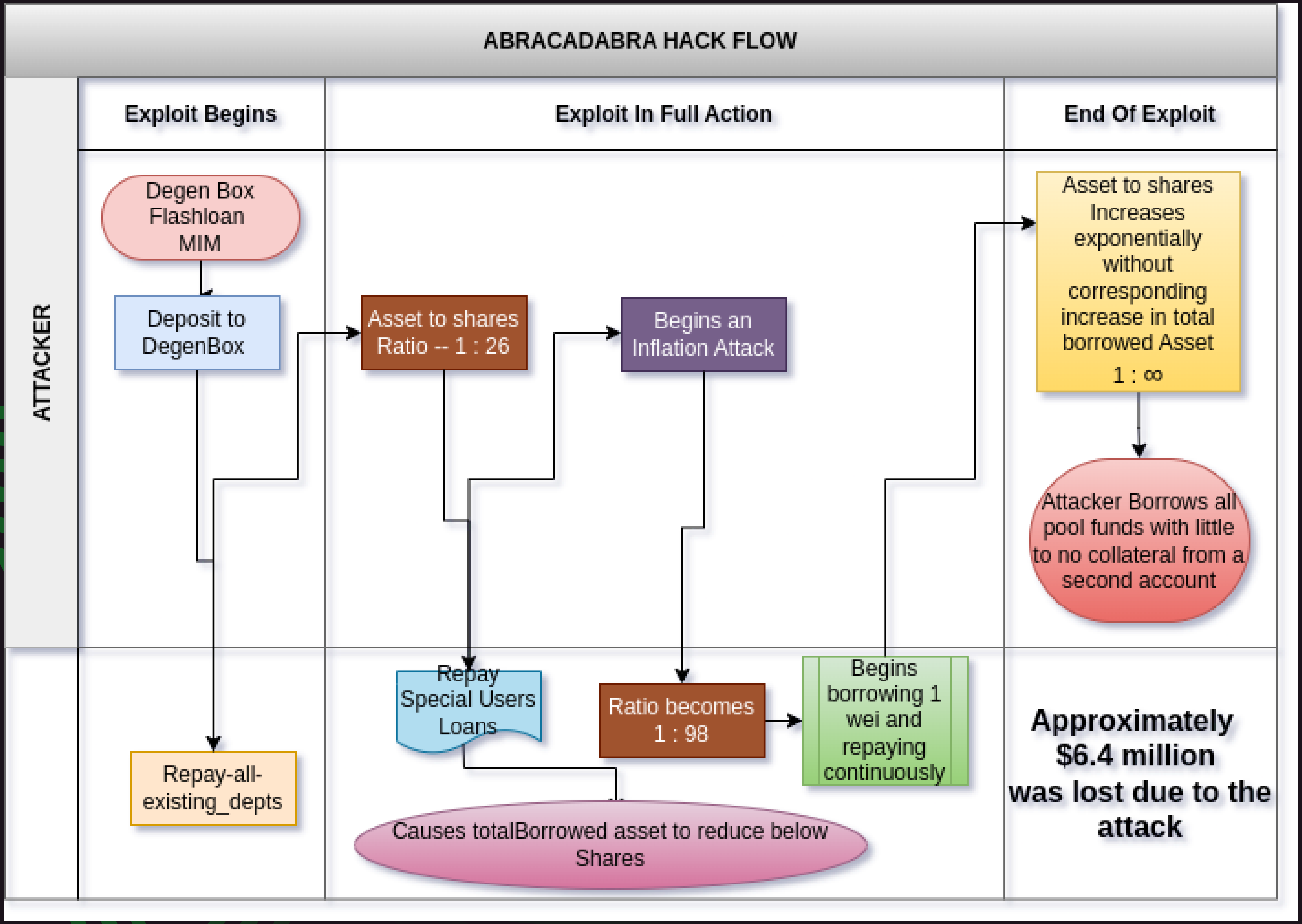
14. Borrow shares represent ownership in the total borrowed assets, and their value adjusts based on the overall debt.



Guild Audits

# HOW IT WENT DOWN

Back to Agenda



ABRACADABRA HACK FLOW

ATTACKER

Exploit Begins

Exploit In Full Action

End Of Exploit

Degen Box Flashloan MIM

Deposit to DegenBox

Repay-all-existing_depts

Asset to shares Ratio -- 1 : 26

Repay Special Users Loans

Begins an Inflation Attack

Ratio becomes 1 : 98

Begins borrowing 1 wei and repaying continuously

Causes totalBorrowed asset to reduce below Shares

Asset to shares Increases exponentially without corresponding increase in total borrowed Asset 1 : ∞

Attacker Borrows all pool funds with little to no collateral from a second account

Approximately $6.4 million was lost due to the attack

# C0D3 T1M3 !!!

Lets get into the cod3 and try to r3play the 4tt4ck that happen3d

Head over to https://github.com/jaydhales/MIM-Spell-Hack-Review

Back to Agenda

# ANALYSIS AND MITIGATION

For lending protocols that use shares calculation to calculate owed interest, make sure there is no way to reduce totalBorrowAssets less than totalBorrowShares

And remember, there is no such thing as an over-audited code.

Back to Agenda

# Thanks!. Arigato!. Connect with us

| | |
|---|---|
| JAYDHALES | https://twitter.com/jaydhales1 |
| OT | https://twitter.com/otaikisadiq |
| PELZ | https://twitter.com/Pelz_Dev |
| KENZMAN | https://twitter.com/kenzman18 |

Guild Audits