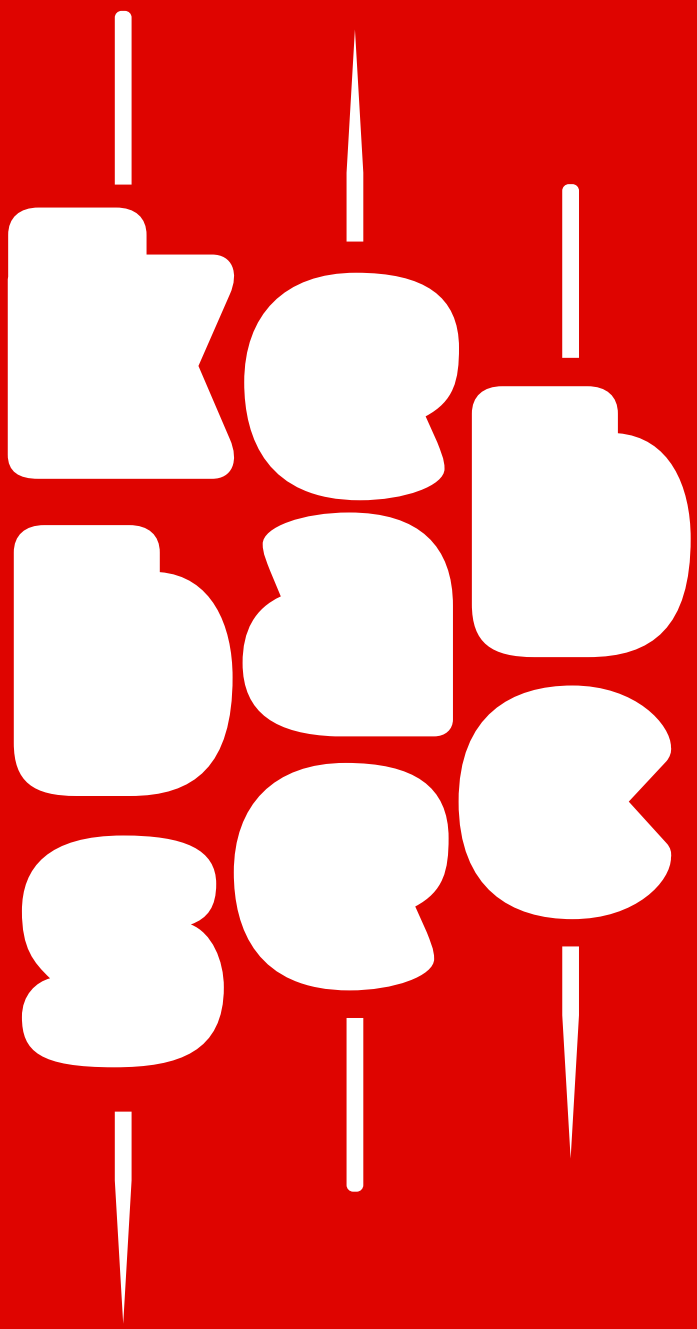

Introduction & Scope

This audit looks into the `Bread.sol` contract and it was conducted by kebabsec members, Flame-Horizon, okkothejawa.

Note: This report does not provide any guarantee or warranty of security for the project.

This is a pro bono security review, as Breadchain is a project created with the purpose of funding public goods.

Executive Summary

Table of Contents

Findings:

1. [INFORMATIONAL] Unnecessary storage read in function

Review Comment

Context: Bread.sol#L118-L120

Description: Since function `rescueToken` has a `onlyOwner` modifier, it is unnecessary to do a storage read with `owner()`, as only the owner can interact with the function in the first place.

Recommendation: Use `msg.sender` instead.

2. [INFORMATIONAL] Initializers could be disabled during contract creation

Review Comment

Context: Bread.sol#L49-L51

Description: It is best practice to call `_disableInitializers` during contact creation

Recommendation: Call `_disableInitializers` in the constructor.

3. [LOW] `claimYield` clears out delegation for `recipient`

Context: Bread.sol#L113

Description: `claimYield` function, unlike the other functions which transfer tokens to a recipient, do not check if the `recipient` has an existing delegation and proceeds to self-delegate. This can be used by the privileged roles, the admin and the yield claimer, to remove the delegation of any user by specifying them as the yield recipient.

Recommendation: Check if the `recipient` has an existing delegation.