PasswordStore Audit Report

Version 1.0

EzSwim

January 17, 2024

PasswordStore Audit Report

EzSwim

January 17, 2024

PasswordStore Audit Report

Prepared by: EzSwim

Lead Auditors:
- EzSwim

Table of Contents

See table

- PasswordStore Audit Report
- Table of Contents
- Disclaimer
- Risk Classification
- Audit Details
  - Scope
- Protocol Summary
  - Roles
- Executive Summary
  - Issues found
- Findings

- High
  - [H-1] Storing the password on-chain makes it visible to anyone, and no longer private
  - [H-2] `PasswordStore::setPassword()` has no access controls, meaning a non-owner could change the password
- Medium
- Low
- Informational
  - [I-1] The `PasswordStore::getPassword()` natspec indicates a parameter that doesn't exist, causing the natspec to be incorrect
- Gas
  - [G-1] The `PasswordStore::s_owner` is store in storage

Disclaimer

The Ez Flow team makes all effort to find as many vulnerabilities in the code in the given time period, but holds no responsibilities for the findings provided in this document. A security audit by the team is not an endorsement of the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the Solidity implementation of the contracts.

Risk Classification

		Impact		
		High	Medium	Low
Likelihood	High	H	H/M	M
	Medium	H/M	M	M/L
	Low	M	M/L	L

We use the CodeHawks severity matrix to determine severity. See the documentation for more details.

Audit Details

The findings described in this document correspond the following commit hash:

```
2e8f81e263b3a9d18fab4fb5c46805ffc10a9990
```

Scope

```
./src/
#-- PasswordStore.sol
```

Protocol Summary

PasswordStore is a protocol dedicated to storage and retrieval of a user's passwords. The protocol is designed to be used by a single user, and is not designed to be used by multiple users. Only the owner should be able to set and access this password.

Roles

- Owner: Is the only one who should be able to set and access the password.

For this contract, only the owner should be able to interact with the contract.

Executive Summary

Issues found

Severity	Number of issues found
High	2
Medium	0
Low	0
Info	1
Gas Optimizations	1
TOTAL	4

Findings

High

[H-1] Storing the password on-chain makes it visible to anyone, and no longer private

Description: All data stored on-chain is visible to anyone, and can be read directly from the blockchain. The `PasswordStore::s_password` variable is intended to be private and only accessed through the `PasswordStore::getPassword()` function, which is intended to be only called by the owner of the contract.

We show one such methode of reading any data off-chain below.

Impact: Anyone can read the private password, severly breaking the functionality of the protocol.

Proof of Concept:

The below test case shows how anyone can read the password directly from the blockchain.

1. Create a locally running chain

```
make anvil
```

2. Deploy the contract to the chain

```
make deploy
```

3. Run the storage tool We use `1` because that is the storage slot of `PasswordStore::s_password` in the contract.

```
cast storage <CONTRACT_ADDRESS_HERE> 1 --rpc-url http://127.0.0.1:8545
```

You will get an output that looks like this: `0x6d7950617373776f726400000000000000000000000000000000`

You can than parse that hex to a string with:

```
cast parse-bytes32-string 0
    x6d7950617373776f726400000000000000000000000000000000000000000014
```

and get the output of: `myPassword`

Recommended Mitigation: Due to this, the overall architecture of the contract should be rethought. One could encrypt the password off-chain, and then store the encrypted password on-chain. This would require the user to remember another password off-chain to decrypt the password. However,

you'd also likely want to remove the view function as you wouldn't want the user to accidentally send a transaction with the password that decrypts your password.

[H-2] `PasswordStore::setPassword()` has no access controls, meaning a non-owner could change the password

Description: The `PasswordStore::setPassword()` function is set to be an external function, however the natspec of the function and overall purpose of the smart contract is that `This function allows only the owner to set a new password`.

```
1 function setPassword(string memory newPassword) external {
2 @>  // @audit - There are no access controls here
3     s_password = newPassword;
4     emit SetNetPassword();
5 }
```

Impact: Anyone can set/change the password of the contract, severly breaking the contract intended functionality.

Proof of Concept: Add the following to the `PasswordStore.t.sol` test suite.

Code

```
1 function test_anyone_can_set_password(address randomAddr) public {
2     vm.prank(randomAddr);
3     string memory expectedPassword = "newPassword";
4     passwordStore.setPassword(expectedPassword);
5     vm.prank(owner);
6     string memory currentPassword = passwordStore.getPassword();
7
8     assert(keccak256(abi.encodePacked(currentPassword)) == keccak256(
          abi.encodePacked(expectedPassword)));
9 }
```

Recommended Mitigation: Add an access control modifier to the `PasswordStore::setPassword()` function.

```
1 if (msg.sender != s_owner) {
2     revert PasswordStore__NotOwner();
3 }
```

Medium

N/A

Low

N/A

Informational

[I-1] The `PasswordStore::getPassword()` natspec indicates a parameter that doesn't exist, causing the natspec to be incorrect

Description: The natspec for the function `PasswordStore::getPassword()` indicates it should have a parameter with the signature `getPassword(string)`. However, the actual function signature is getPassword().

```
1       /*
2        * @notice This allows only the owner to retrieve the password.
3    @>  * @param newPassword The new password to set.
4        */
5       function getPassword() external view returns (string memory) {
```

Impact: The natspec is incorrect.

Recommended Mitigation: Remove the incorrect natspec line.

```
1   -     * @param newPassword The new password to set.
```

Gas

[G-1] The `PasswordStore::s_owner` is store in storage

Description: The `PasswordStore::s_owner` is set in the constructor and never changed after that. Varibales that are only set once should eithr be constant or immutable.

```
1       constructor() {
2    @>     s_owner = msg.sender;
3       }
```

Impact: `PasswordStore::s_owner` is stored in the contract storage and therefore costs more gas.

Recommended Mitigation: Add `immutable` keyword to `PasswordStore::s_owner`. Furthermore to indicate that the owner is an immutable variable you could right it like so:

```
1   +   address private immutable i_owner;
```

Refactoring needed: `PasswordStore::s_owner` => `PasswordStore::i_owner`