Protocol Audit Report

Version 1.0

Victor.zsh

January 13, 2025

Protocol Audit Report

Victor.zsh

Jan 13, 2025

Prepared by: Victor.zsh Lead Auditors:

- Victor.zsh

Table of Contents

Protocol Summary

Protocol allows the owner store a password and retrieve it. Only the owner can set the password and only the owner can retrieve the password.

Disclaimer

The Victor.zsh 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
	High	H	H/M	M
Likelihood	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:

```
1  226e6a4a53fc5021695b67c16de5501eccc94436
```

Scope

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

Roles

- Owner: The user who can set the password and read the password.
- Outsides: No one else should be able to set or read the password.

Executive Summary

Issues found

Severity	Number of issues found
High	2
Medium	0
Low	0
Info	1
Total	3

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 a private valuable and only accessed through the `PasswordStore::getPassword` function, which is intended to be called by the owner of the contract.

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

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

Proof of Concept: (Proof of code)

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

1. Create a locally running chain

```
1    make anvil
```

2. Deploy the contract to the chain

```
1    make deploy
```

3. Run the storage tool

We use 1 because that's the storage slot of `s_password` in the contract.

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

You'll get an output that looks like this:

0x6d7950617373776f726400000000000000000000000000000000000000000014

You can then parse that hex to a string with:

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

And get an output of:

```
1    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 stored password. However, you're also likely want to remove the view function as you wouldn't want the user to accidentally send a transaction with this decryption key.

[H-2] `PasswordStore::setPassword` has no access control, meaning anyone can set/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
3           s_password = newPassword;
4           emit SetNewPassword();
5       }
```

Impact: Anyone can set/change the password, serverly breaking the functionality of the protocol.

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

Code

```
1      function test_anyone_can_set_password(address randomAddress) public
         {
2        vm.assume(randomAddress != owner);
3        vm.prank(randomAddress);
4        string memory expectedPassword = "myNewPassword";
5        passwordStore.setPassword(expectedPassword);
6
7        vm.prank(owner);
8        string memory actualPassword = passwordStore.getPassword();
9        assertEq(actualPassword, expectedPassword);
10   }
```

Recommended Mitigation: Add an access control conditional to the `setPassword` function.

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

Informational

[I-1] The `PasswordStore::getPassword` NatSpec Indicates a Non-Existent Parameter, Causing an Incorrect NatSpec

Description:

```
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) {
```

The NatSpec for the `PasswordStore::getPassword` function signature is `getPassword()`, yet the NatSpec suggests it should be getPassword(string).

Impact: The NatSpec documentation is incorrect.

Recommended Mitigation: Remove the incorrect NatSpec line.

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