

Protocol Audit Report

Version 1.0

Smartinex.ir

January 13, 2024

Protocol Audit Report

HosseinMirzapur

January 13th, 2024

Prepared by: Hossein Mirzapur Lead Auditors: - Hossein Mirzapur

Table of Contents

- Table of Contents
- Protocol Summary
- Disclaimer
- Risk Classification
- Audit Details
 - Scope
 - Roles
- Executive Summary
 - Issues found
- Findings
 - High
 - * [H-1] Storing the password on-chain makes it visible to anyone, and no longer private
 - Likelihood & Impact:
 - * [H-2] `PasswordStore::setPassword` is callable by anyone
 - * Likelihood & Impact:
 - Informational
 - * [I-1] The `PasswordStore::getPassword` natspec indicates a parameter that doesn't exist, causing the natspec to be incorrect
 - * Likelihood & Impact:

Protocol Summary

Protocol does X, Y, Z

Disclaimer

The Smartinex 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

Commit Hash: 2e8f81e263b3a9d18fab4fb5c46805ffc10a9990

Scope

```
1 ./src/  
2 # => PasswordStore.sol
```

Roles

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. `PasswordStore::s_password` variable is intended to be a private variable, 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 method of reading any data off chain below. (check proof of concept)

Impact: Anyone can read the private password, severely breaking the functionality 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
```

1. Deploy the contract to the chain

```
1 make deploy
```

1. 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 which looks like this:

[illegible]

You can the parse that hex to a string with:

```
1 cast parse-bytes32-string 0  
   x6d7950617373776f726440000000000000000000000000000000000000000014
```

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 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.

Likelihood & Impact:

- Impact: HIGH
- Likelihood: HIGH
- Severity: HIGH (CRIT)

[H-2] PasswordStore::setPassword is callable by anyone

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.

Proof of Concept:

Add the following to the `PasswordStore.t.sol` test suite.

Code

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

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

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

Likelihood & Impact:

- Impact: HIGH
- Likelihood: HIGH
- Severity: HIGH (CRIT)

Informational

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

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) {
6     if (msg.sender != s_owner) {
7         revert PasswordStore__NotOwner();
8     }
9     return s_password;
10 }
```

The `PasswordStore::getPassword` function signature is `getPassword()` while the natspec says it should be `getPassword(string)`

Impact: The natspec is incorrect.

Recommended Mitigation: Remove the incorrect Natspec line.

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

Likelihood & Impact:

- Impact: NONE
- Likelihood: HIGH