PasswordStore Audit Report

Version 1.0

0xmaurice

December 2, 2023

PasswordStore Audit Report

0xmaurice

December 2, 2023

Prepared by: 0xmaurice Lead Auditor: - 0xmaurice

Table of Contents

Protocol Summary

PasswordStore is a protocol dedicated to store and retrieve password's. The protocol is designed to be used be a single user. Only the owner should be able to set and access this password.

Disclaimer

0xmaurice 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  2e8f81e263b3a9d18fab4fb5c46805ffc10a9990
```

Scope

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

Roles

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

Executive Summary

This audit was part of the Cyfrin Updraft tutorials. By following the course instructions, I acquired the skills necessery to setup my first audit report and document the vulnerabilities along with their respective severities. The tutorial took me a total of 6 hours to complete. For the proof of concepts, we used Foundry, while for the final report we used Pandoc and LaTeX to convert it into a PDF.

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 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.

Impact: Anyone can read the private password, severly braking 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

```
1  anvil
```

2. Deploy the contract to the chain

```
1  forge script script/DeployPasswordStore.s.sol:DeployPasswordStore --rpc
     -url http://127.0.0.1:8545 --private-key {$PRIVATE_KEY} --broadcast
```

3. Run the storage tool

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

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

You will 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: `myPassword`

Recommended Mitigation:

Due to this, the overall architecture of the contract should be rethought.

[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
3          s_password = newPassword;
4          emit SetNetPassword();
5      }
```

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

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 `PasswordStore.sol::setPassword` function.

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

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) {
```

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

Impact: The natspec is incorrect.

Recommended Mitigation: Remove the incorrect natspec line.

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