

# **PasswordStore Initial Audit Report**

Version 0.1

# PasswordStore Audit Report

#### Felix Moser

September 1, 2023

# **PasswordStore Audit Report**

Prepared by: Felix Moser Lead Auditors: Felix Moser

• [FelixMoser]

**Assisting Auditors:** 

None

# **Table of contents**

#### See table

- PasswordStore Audit Report
- Table of contents
- About YOUR\_NAME\_HERE
- Disclaimer
- Risk Classification
- Audit Details
  - Scope
- Protocol Summary
  - Roles
- Executive Summary

- Issues found
- Findings
  - High
    - \* [H-1] Passwords stored on-chain are visable to anyone, not matter solidity variable visibility
    - \* [H-2] PasswordStore::setPassword is callable by anyone

## **About YOUR\_NAME\_HERE**

### **Disclaimer**

The YOUR\_NAME\_HERE team makes all effort to find as many vulnerabilities in the code in the given time period, but holds no responsibilities for the 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	Н	H/M	М
	Medium	H/M	М	M/L
	Low	М	M/L	L

#### **Audit Details**

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

1 **2**e8f81e263b3a9d18fab4fb5c46805ffc10a9990

#### Scope

```
1 src/
2 --- 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	0		
Gas Optimizations	0		
Total	0		

## **Findings**

#### High

#### [H-1] Passwords stored on-chain are visable to anyone, not matter solidity variable visibility

**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.

However, anyone can directty read this using any number of

**Impact:** The password is not private.

**Proof of Concept:** The below test case shows how anyone could read the password directly from the blockchain. We use foundry's cast tool to read directly from the storage of the contract, without being the owner.

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:

You can then parse that hex to a string with:

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 on-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 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.

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

**Impact:** Anyone can set/change the password of the contract.

#### **Proof of Concept:**

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

```
function test_anyone_can_set_password(address randomAddress) public {
    vm.prank(randomAddress);
    string memory expectedPassword = "myNewPassword";
    passwordStore.setPassword(expectedPassword);
    vm.prank(owner);
    string memory actualPassword = passwordStore.getPassword();
    assertEq(actualPassword, expectedPassword);
}
```

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

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