Kuma Wallet Audit Report

The following document is an audit report covering Kuma Wallet App (https://github.com/blockcoders/kuma-wallet), a cross-chain wallet that offers management and transfer of assets between EVM and WASM chains, which will make it the first of its kind. It's currently under development and a release is expected in Q3. It currently works as an extension in Mozilla Firefox and Google Chrome.

Independent contractor and software security expert, Piotr Romashov (https://piotromashov.github.io/), has been hired to perform an unbiased and isolated audit of the code at commit hash fd51deaa81b61058927f80e467bb57cee0b3321e.
Debrief was performed on April 20th 2023.

Report is to be used combined with the debrief and code review submitted to the repository.

Introduction

The scope of the audit is to check general code security and quality, specially focused on potential vulnerabilities regarding password/seed phrase encryption, salt generation, and storage, for current implementation. Research and comparisons has been performed on standards from similar products such Metamask and Polkadot.

Audited Files

The source code to audit has been supplied in the form of a GitHub repository:
https://github.com/blockcoders/kuma-wallet
Commit hash: fd51deaa81b61058927f80e467bb57cee0b3321e

The scope of the audit was limited to the following files:

```
kuma/src/
├── Extension.ts
├── accounts
│   ├── AccountManager.ts
└── storage
    ├── Auth.ts
    ├── Storage.ts
    └── entities
        ├── Account.ts
        ├── Accounts.ts
        ├── BackUp.ts
        ├── BaseEntity.ts
        ├── CacheAuth.ts
        ├── Keyring.ts
        ├── SelectedAccount.ts
        └── Vault.ts
```

Audit Findings

This section presents the detailed findings from the audit, including both security and quality issues identified during the assessment.

Security Findings

This subsection focuses on security-related issues identified in kuma wallet app, including vulnerabilities, misconfigurations, and weaknesses in the security controls implemented.

Each finding is categorized by severity level (i.e., critical, high, medium, low) and include a description of the issue, its potential impact, and the recommended actions for remediation.

High Severity

1. **Password hash: *Cryptographic failure vulnerability.***
   Password is stored hashed in browser storage (referenced as caché in kuma wallet). It's being used to caché credentials and bypass password prompts for 24h.
   The hashing is performed with passworder from metamask, which has been widely tested and is an industry standard, but it's using a custom made salt with browser environment variables. This salt is not random enough and could be guessed by an attacker, and with access to storage, could unhash the password and with that the ability to decrypt all the vault contents: seed phrases and privateKeys, which gives access to all the funds from all accounts.
   Recommendation: Use a safer salt generation, such as passworder.generateSalt()

Medium Severity

1. **Insecure default configuration**
   Password keeping for the "stay logged in" feature is turned on by default and lasts 24h. This could give the chance to a possible attacker to get access to the funds whilst the computer is unattended. Configurations should be always secure by default. Apps that give access to finances should have stricter default measures.
   Recommendation: Disable password caching by default. When enabled it should be around 15m. This could be an advanced security configuration as well.

Low Severity

1. **Seed phrase/Private Key/Mnemonic**
   Seed phrase is stored with each account added with the Keyring. Storing sensitive data such as seed phrases should be done carefully, and preferably in one place, this reduces the vector of a possible attack.
   Recommendation: Refactor Keyring object to store only once the seed/private key.

2. **Password Storage (twice):**
   Password is saved twice in storage, one to be used as caché and "stay logged in" feature, and the other one to restore password feature, both times using metamask passworder, the first using a custom made salt, and the latter with the seed phrase. It should be stored only once, having it duplicated amplifies the vector of potential attacks.
   Recommendation: Restore password feature can be achieved without storing it. Delete all accounts and use seed phrase to regenerate them, the same process is used by metamask and polkadot, see appendix for more information.

Quality and Test Coverage

This subsection focuses on quality-related issues identified in kuma wallet app, including issues related to code quality, architecture, design patterns, error handling, logging, and *other quality-related aspects that may impact the reliability, maintainability, and performance of the application. In order to help with the evaluation of the remaining risk, we provide a measure of the following key indicators: Design complexity, code readability, level of documentation, and test coverage.*

***Note**: Design complexity or lower test coverage does equate to a higher risk. Certain bugs are more easily detected in unit testing than a security audit and vice versa. It is, therefore, more likely that undetected issues remain if the test coverage is low or non-existent.*

Criteria	**Status**	**Comment**
Design complexity	**Medium**	Improvements regarding object oriented programming good practices.
Code readability and clarity	**High**	Besides specific cases regarding caché naming for storage and Keyring behavior, most code is easy to read.
Level of Documentation	**Medium**	Github Readme is clear to start. Points to https://docs.kumawallet.io/ but it's empty.
Test Coverage	**High**	See annex on test coverage

Code Review

The following is a summary of manual code analysis. Full comments have been shared in the repository.

Restore password screen

1. Text says "Password" and "Confirm Password",
   *Recommendation: use "**New** Password" and "Confirm **new** password"*

Extension.ts

1. Keep consistency on where the password is being stored, currently is stored in cache and in storage. Should only be stored in one place.
2. Usage of cachePassword is breaking encapsulation. Should be executed inside signIn and signUp.
3. createAccount has an untested **isSignUp** parameter, and it's not clear when it's used.

Auth.ts

1. Order of internal execution when signing in and signing out with Cache set and expiration.

2. Check for passworder.decrypt validity instead of empty.
3. Throwing misleading errors.

Keyring.ts

1. Object naming and responsibility is confusing.
2. Review implementation between Keyring and AccountManager.
3. Should be in charge of generating paths and deriving new keys.
4. Don't save seed phrase each time for EVM Keyring accounts, do save it in WASM.

AccountManager.ts

1. Improve checking for validity instead of empty, improve file readability.
   Recommendation: Replace mnemonic validation with bip39.validateMnemonic().

CacheAuth.ts

1. Timeout is currently set up at **24h**, advised to use much less (<15m). Banks don't allow for this, you could walk away from the computer and get your funds stolen.
2. Password caching should be disabled by default. This feature compromises security.
3. Improvements on responsibilities and collaboration between Auth and CacheAuth.
4. Creating a new CacheAuth should create an object with a valid timestamp, not 0.

CacheAuthTest.ts

1. CacheAuth expired should be **true** when the timestamp is set to 0. Currently is false.

SelectedAccounts.ts

1. Creating default invalid objects is a bad practice.
   Recommendation: pass the parameters and create a valid object.

Vault.ts

1. There is a problem in the delegation of responsibilities with Auth. Vault shouldn't be loading Auth from cache, or checking for its contents.
   Recommendation: *Auth can unencrypt directly; Internally Auth will load from caché and perform all the operations. Vault will be agnostic.*
2. Auth class should be responsible for checking if the user is logged in, not the vault.
3. Methods not being used: getKeyring and setKeyring.

Disclaimer

This security audit is not a security warranty, investment advice, or an endorsement of Kuma Wallet or its authors. This audit does not provide a security or correctness guarantee of the audited app. Securing crypto wallets is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

Appendix

This section includes any additional information, such as technical details, supporting evidence, and references used during the audit process.

Metamask Research

https://support.metamask.io/hc/en-us/articles/4404722782107
Mnemonic phrase: Stored in app, to unlock it you need app password.
Password: Not stored. Secures the app itself. To reset it you need the mnemonic. Removes accounts from wallet when forgot password feature is used.

"...This action will delete your current wallet and Secret Recovery Phrase from this device, along with the list of accounts you've curated. After resetting with a Secret Recovery Phrase, you'll see a list of accounts based on the Secret Recovery Phrase you use to reset. **This new list will automatically include accounts that have a balance.** …"

Polkadot research

https://wiki.polkadot.network/docs/learn-account-generation, https://polkadot.js.org
Password: Not stored. Secures the app itself. To reset it you need the mnemonic. Removes accounts from wallet when forgot password feature is used.

Test coverage report

```
-------------------------------|---------|----------|---------|---------|----------
------------------------------------------------------------------------------------
-----------
File                           | % Stmts | % Branch | % Funcs | % Lines |
Uncovered Line #s
-------------------------------|---------|----------|---------|---------|----------
------------------------------------------------------------------------------------
-----------
All files                      |   92.57 |   79.34 |   86.03 |   92.57 |
 src                           |     100 |  95.69 |      100 |  100 |
  Extension.ts                 |     100 |  95.69 |      100 |  100 |
72,94,256,300
 src/accounts                  |   98.26 |   66.66 |   93.75 |   98.26 |
  AccountManager.ts            |   98.17 |   65.3 |   93.33 |   98.17 |
113,140,157-158
  types.ts                     |     100 |        100 |  100 |  100 |
 src/hooks                     |     100 |        100 |  100 |  100 |
  index.ts                     |     100 |        100 |  100 |  100 |
 src/hooks/common              |   98.91 |   92.85 |      100 |    98.91 |
  useCopyToClipboard.tsx       |   98.03 |   83.33 |      100 |    98.03 | 20
  useLoading.tsx               |     100 |        100 |  100 |  100 |
  useToast.tsx                 |     100 |        100 |  100 |  100 |
 src/i18n                      |     100 |        100 |  100 |  100 |
  index.ts                     |     100 |        100 |  100 |  100 |
 src/pages/accountForm         |   81.38 |   52.27 |   21.42 |   81.38 |
  AccountForm.tsx              |   81.38 |   52.27 |   21.42 |   81.38 |
87-88,92-95,99,114-120,126-127,141,149,182,213-250,281-282,309,340-341,347,376-377,
390-402
 src/pages/addAccount          |     100 |        100 |  100 |  100 |
  AddAccount.tsx               |     100 |        100 |  100 |  100 |
  OptionButton.tsx             |     100 |        100 |  100 |  100 |
 src/pages/balance/components  |   93.13 |     56.98 |   71.79 |   93.13 |
  AccountList.tsx              |   91.05 |   66.66 |   42.85 |   91.05 |
27-28,47,93,96-98,101-104
  AccountSelected.tsx          |     100 |  66.66 |      100 |  100 | 13
  Activity.tsx                  |   94.03 |  58.06 |      100 |   94.03 |
62-63,76-77,88,91,101,115,117,119,157-159
  Assets.tsx                    |   96.15 |  46.66 |       40 |   96.15 |
43-45,52-53
  ChainSelector.tsx             |   94.76 |       75 |   88.88 |   94.76 |
68-70,73,93-94,164-166,185
  ConfirmChainChangeModal.tsx  |   84.05 |     20 |   66.66 |   84.05 |
72,80,89-91,112-128
  TotalBalance.tsx              |     100 |       60 |   50 |   100 | 28-35
 src/pages/manageAssets         |   96.75 |       50 |   66.66 |   96.75 |
  ManageAssets.tsx              |   96.75 |       50 |   66.66 |   96.75 |
52,54-55,87-88
 src/pages/receive              |     100 |       50 |   66.66 |      100 |
  Receive.tsx                   |     100 |       50 |   66.66 |      100 |
20-41
 src/pages/send/components      |     91.2 | 74.56 |   79.16 |   91.2 |
  ConfirmTx.tsx                 |     100 |       50 |   66.66 |      100 |
36-82
  Destination.tsx               |     83.9 | 78.12 |      62.5 | 83.9 |
33-39,46-52,58-63,138-146,160-163
  EvmForm.tsx                   |   81.73 |  60.86 |      100 |   81.73 |
81,125-155,157,181,193-200
  Fees.tsx                      |     100 |      100 |  100 |  100 |
  SelectableAsset.tsx           |     100 |  88.88 |      100 |  100 | 27
  SelectableChain.tsx           |     100 |      100 |  100 |  100 |
  WasmForm.tsx                  |   93.18 |  70.58 |       75 |   93.18 |
97-99,160-165,170-171,217-218,234-238
 src/pages/settings             |   90.96 |  73.41 |   46.34 |   90.96 |
  Contacts.tsx                  |   92.36 |  71.42 |   54.54 |   92.36 |
42-48,83-84,98,106-112,123,220-221
  General.tsx                   |   93.04 |  84.61 |       70 |   93.04 |
48-49,68-76,93-94
  Security.tsx                  |   88.91 |       64 |   30 |   88.91 |
46-48,51-53,56-57,60-61,64-72,83-84,95-96,99-102,110-111,118-124,166-167,190-192
 src/pages/signIn               |   90.21 |       70 |   62.5 |   90.21 |
  SignIn.tsx                    |   90.21 |       70 |   62.5 |   90.21 |
26-27,37-39,42-43,70-71
 src/pages/signMessage          |   98.31 |  62.5 |      100 |   98.31 |
  SignMessage.tsx               |   98.31 |  62.5 |      100 |   98.31 | 76-77
 src/pages/welcome              |     100 |      100 |  100 |  100 |
  Welcome.tsx                   |     100 |      100 |  100 |  100 |
 src/providers                  |     100 |      100 |  100 |  100 |
  index.ts                      |     100 |      100 |  100 |  100 |
 src/providers/accountProvider |   76.69 |     75 |  87.5 |   76.69 |
  AccountProvider.tsx           |   76.58 |       75 |  87.5 |   76.58 |
50-62,64,97-99,112-116,136-137,141-162,184-185
  index.ts                      |     100 |      100 |  100 |  100 |
 src/providers/assetProvider   |   87.97 |  68.65 |      100 |   87.97 |
  AssetProvider.tsx             |   87.95 |  68.65 |      100 |   87.95 |
89,136-138,173-188,206-208,251-252,256,258-259,278-279,283,285-286,309-310,334-356,
380-381,434-435,504
  index.ts                      |     100 |      100 |  100 |  100 |
 src/providers/authProvider     |     100 |  95.83 |      90.9 |      100 |
  AuthProvider.tsx              |     100 |  95.83 |      90.9 |      100 | 79
  index.ts                      |     100 |      100 |  100 |  100 |
 src/providers/networkProvider |   90.21 |  80.43 |   83.33 |   90.21 |
  NetworkProvider.tsx           |   90.17 |  80.43 |   83.33 |   90.17 |
35,73-78,132-133,177-178,188-189,193-202
  index.ts                      |     100 |      100 |  100 |  100 |
 src/providers/txProvider        |   92.41 |   76.92 |   81.81 |   92.41 |
  TxProvider.tsx                 |   92.34 |   76.92 |   81.81 |   92.34 |
52,54,102,113-114,138-139,177-186
  index.ts                       |     100 |         100 |  100 |  100 |
 src/storage                     |     100 |  97.5 |       100 |  100 |
  Auth.ts                        |     100 |         100 |  100 |  100 |
  Storage.ts                     |     100 |  92.3 |       100 |  100 | 22
 src/storage/entities            |   96.22 |   92.85 |   96.39 |   96.22 |
  Account.ts                     |     100 |         100 |  100 |  100 |
  Accounts.ts                    |     90.9 | 95.65 |      87.5 | 90.9 |
43-46,49-52
  Assets.ts                      |   90.74 |   91.66 |   85.71 |   90.74 | 28-32
  BackUp.ts                      |     100 |         100 |  100 |  100 |
  BaseEntity.ts                  |     100 |         100 |  100 |  100 |
  CacheAuth.ts                   |   88.29 |   84.21 |      90.9 |   88.29 |
27-28,45-46,60-63,74-76
  Chains.ts                      |   98.26 |   93.54 |       100 |   98.26 | 111-112
  Keyring.ts                     |     100 |   88.88 |       100 |  100 | 24-25
  Network.ts                     |     100 |   90.9 |       100 |  100 | 33
  SelectedAccount.ts             |     100 |   66.66 |       100 |  100 | 27-29
  TrustedSites.ts                |     100 |         100 |  100 |  100 |
  Vault.ts                       |   98.19 |   96.77 |       100 |   98.19 | 37-38
 src/storage/entities/activity |  97.5 | 80.64 |       90 |   97.5 |
  Activity.ts                    |   95.71 |   77.77 |      87.5 |   95.71 |
17-18,36
  types.ts                       |     100 |         100 |  100 |  100 |
 src/storage/entities/registry |   96.15 |    77.14 |       100 |   96.15 |
  Contact.ts                     |     100 |         100 |  100 |  100 |
  Register.ts                    |     100 |         100 |  100 |  100 |
  Registry.ts                    |   95.57 |   74.19 |       100 |   95.57 |
91-93,96-97
 src/storage/entities/settings | 100 |  96.66 |       100 |  100 |
  LanguageSetting.ts             |     100 |         100 |  100 |  100 |
  Setting.ts                     |     100 |         100 |  100 |  100 |
  Settings.ts                    |     100 |   93.75 |       100 |  100 | 66
  types.ts                       |     100 |         100 |  100 |  100 |
 src/utils                       |   89.35 |   87.27 |       90 |   89.35 |
  account-utils.ts               |     100 |         100 |  100 |  100 |
  assets.ts                      |   75.29 |          75 |   90 |   75.29 |
25-30,34-46,73-74
  constants.ts                   |     100 |         100 |  100 |  100 |
  env.ts                         |     100 |   66.66 |       50 |   100 | 5
  i18n.ts                        |     100 |         100 |  100 |  100 |
  utils.ts                       |   95.55 |   91.66 |       100 |   95.55 | 39-40
-------------------------------|---------|----------|---------|---------|----------
-----------------------------------------------------------------------------------
-----------
=============================== Coverage summary ===============================
Statements   : 92.57% ( 6691/7228 )
Branches     : 79.34% ( 872/1099 )
Functions    : 86.03% ( 425/494 )
Lines        : 92.57% ( 6691/7228 )
================================================================================
```