



Star Key

Web Wallet Audit

April 26, 2024

Iwaki Hiroto

Table of Contents

Table of Contents	1
Overview	3
Project Details	3
Audit Checklist.....	4
Risk Classification	5
Finding Classification	5
Finding Details.....	6
Medium	6
In recovery-phrase screen, choice words should be selected randomly, not shuffling.....	6
Low	8
Cannot go to next step when creating new account in the case that you backed from selecting security type to password setting.	8
In the window of “Import Account”, the input of private should be typed as hidden character so that others cannot read it.....	11
Info	13
In Settings page, links of Feedback and Help don't work.	13
In the page of Edit Account, if you reopen edit window and click close after changing avatar, the avatar will be reset as default.....	14
In Address page, if you input address and then select network, already input address is removed.....	15
When delete registered address, it would be better to ask confirm.	16

After adding new token, it would be better to using loading state when loading the price of added token..... 17

Overview

This document describes the result of auditing the Star Key Web Wallet project. This project is a web extension that provides the functionalities of managing assets and transactions for several chains.

This project is developed using react library and can be built using webpack as web browser extension.

This auditing is performed against the entire project and built extension's workflow in web browsers including its transactions and interacting with chain.

Project Details

Project Name	Star Key
Project Type	Web Wallet Extension
Audit Period	April 12 ~ April 19

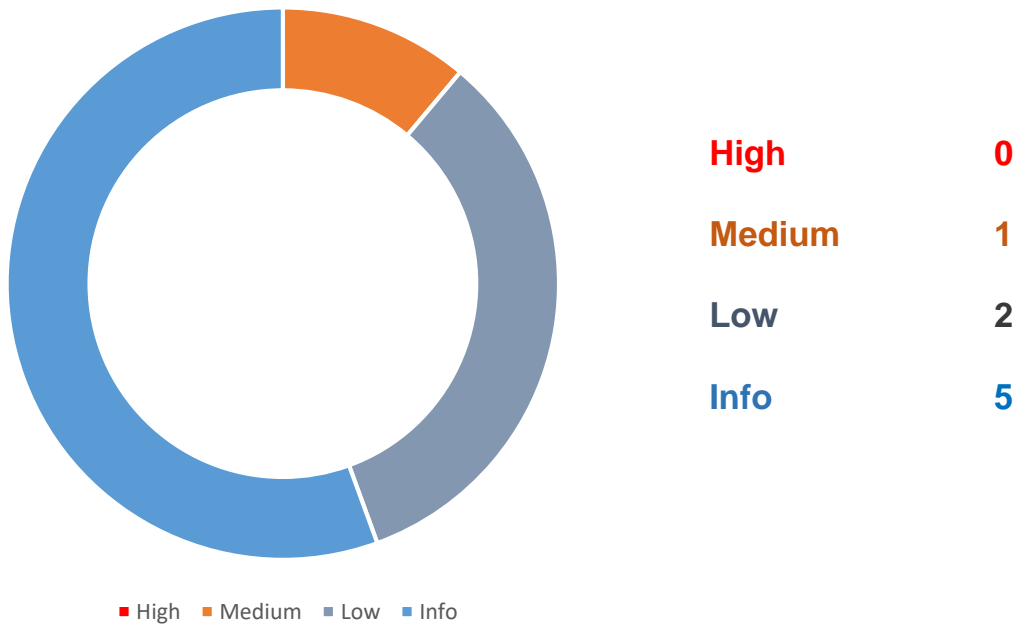
Audit Checklist

Audit Class	Audit Subclass	Review Status
Transfer Security	Signature	✓
	Deposit / Transfer	✓
	Transaction Broadcast	✓
Secret Key Security	Secret Key Generation	✓
	Secret Key Storage	✓
	Secret Key Usage	✓
	Secret Key Backup	✓
	Secret Key Destruction	✓
	Cryptography Security	✓
Architecture and Business Security	Wallet Lock	✓
	Business Logic	✓
	Architecture Design	✓
	DoS (Denial of Service)	✓
Frontend Security	Cross-Site Scripting	✓
	HTTP Response Header	✓
Components Security	Third-Party Components Security	✓
Communication Security	Communication Encryption	✓
User Interaction Security	Password Complexity Requirements	✓
	Contact Whitelisting	✓
	WYSIWYS	✓

Risk Classification

		Difficulty		
		High	Medium	Low
Severity	High	High	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

Finding Classification



Finding Details

Medium

In recovery-phrase screen, choice words should be selected randomly, not shuffling.

Severity

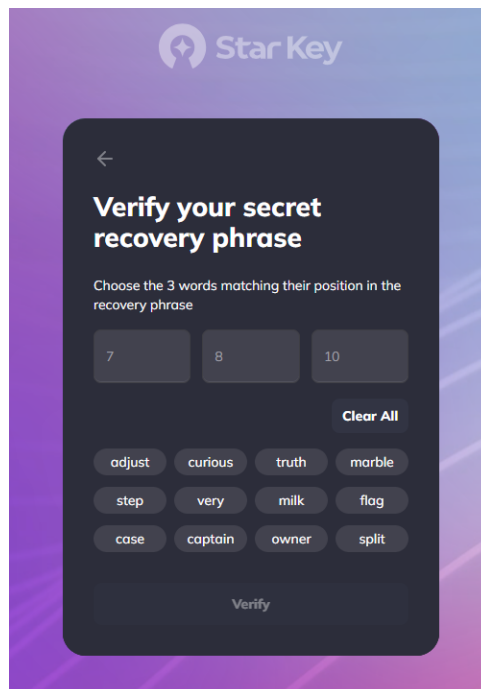
High

Difficulty

Low

Impact

In recovery-phrase screen, choice words should be selected randomly, not just shuffling. And whenever clear all, should change order. If you possible, make user should type the words directly in the input.



Vulnerability Details

When verifying the recovery phrase, they are using all mnemonic as the candidate words just with changing order.

RecoveryPhrase.tsx

```
useEffect(() => {
  if (wallet) {
    // eslint-disable-next-line @typescript-eslint/restrict-plus-operands
    const words = wallet.mnemonic.phrase.split(' ').map((name: any, id: number)
=> ({ id: id + 1, name })))
    // eslint-disable-next-line @typescript-eslint/no-unsafe-argument
    setPhrase(words) // set phrase to get name as per words indexes
    @> setChips(shuffle(words))
  }
}, [wallet])
```

This may harm safety to prevent private information of wallet from being public to the malicious crackers.

They should use randomly selected words as candidate words by adding real some phrases into them.

In addition, it would be better to select candidates words again whenever click “Clear All” to prevent using several types of automatic bot.

Low

Cannot go to next step when creating new account in the case that you backed from selecting security type to password setting.

Severity

Low

Difficulty

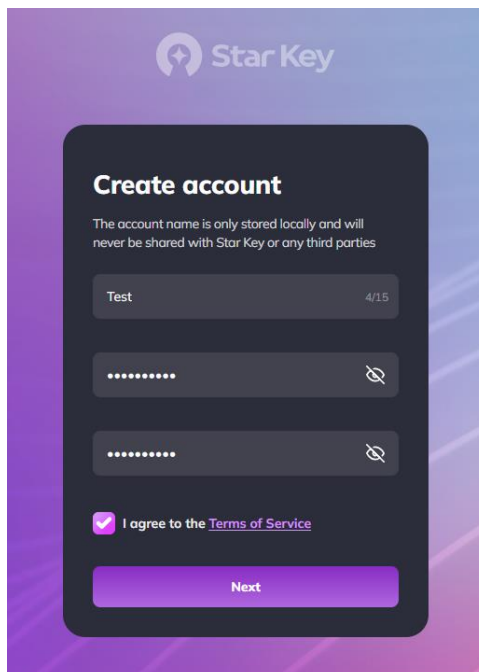
Medium

Impact

Users cannot go to next step when creating new account in the case that he backed from selecting security.

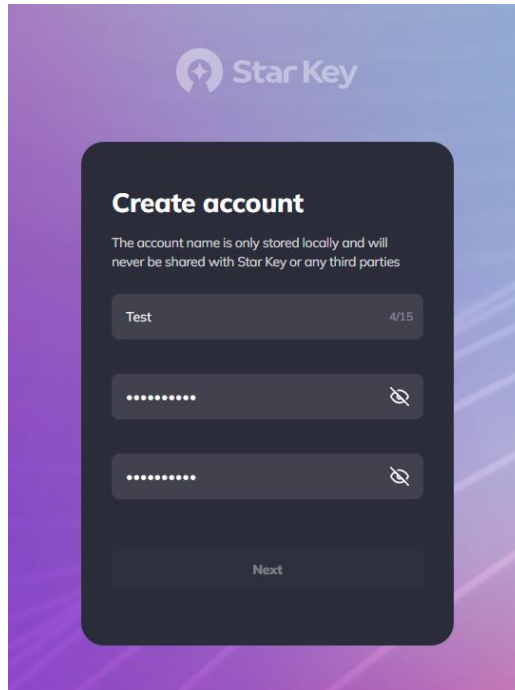
Vulnerability Details

To create account, users will input their account name, password and confirm password, then check the “Terms of Service” and click the “Next” button.



The screenshot shows a mobile application interface for creating a new account. At the top, the 'Star Key' logo is visible. The main heading is 'Create account', followed by a note: 'The account name is only stored locally and will never be shared with Star Key or any third parties'. The form contains three input fields: the first is for the account name (containing 'Test' and a character count '4/15'), the second is for the password (masked with dots and a toggle icon), and the third is for the confirm password (also masked with dots and a toggle icon). Below these fields is a checkbox labeled 'I agree to the Terms of Service'. At the bottom of the form is a prominent 'Next' button.

After that, when the user click the back button (e.g. to change the account name), then the user cannot click “Next” button again even he input all requirements correctly.



That's because the component of checkbox for “Terms of Service” is hidden in this case.

Therefore, the user should reinstall the wallet again to overcome this problem.

It needs to modify the filtering checkbox component by `onboardingBy` state.

CreateAccount.tsx

```
@> {onboardingBy === '' && (  
  <div className="mt-4 space-y-4">  
    <div className="flex items-center">  
      <Checkbox  
        size="lg"  
        radius="sm"  
        icon={<CheckboxIcon />}  
        onChange={(e) => acceptTermsConditions(e)}  
        isSelected={isTermsConditionsChecked}  
      />  
    </div>  
  </div>  
)}
```

```
        <span className="text-sm font-  
bold">{t('Onboarding.agreefortermsAndConditions')}</span>  
        </Checkbox>  
        &nbsp;{termsAndServicesLink}  
    </div>  
</div>  
    )}
```

In the window of “Import Account”, the input of private should be typed as hidden character so that others cannot read it.

Severity

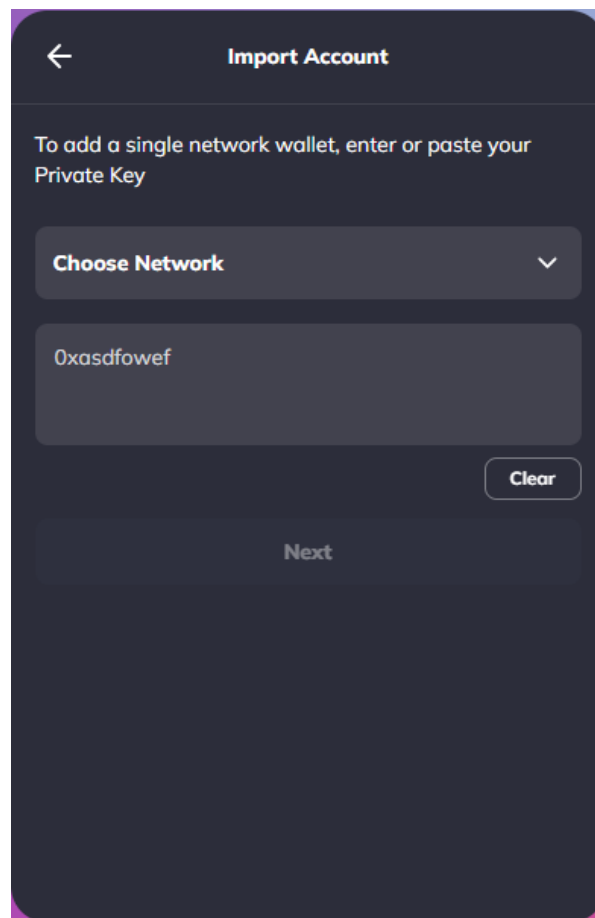
Medium

Difficulty

Low

Vulnerability Details

To prevent critical information such as private key to be public, you should hidden its strings so that others cannot read it.



However, in the window of “Import Account”, the typed or copied private key is shown as real strings itself.

It may harm the security of user private information.

Info

In Settings page, links of Feedback and Help don't work.

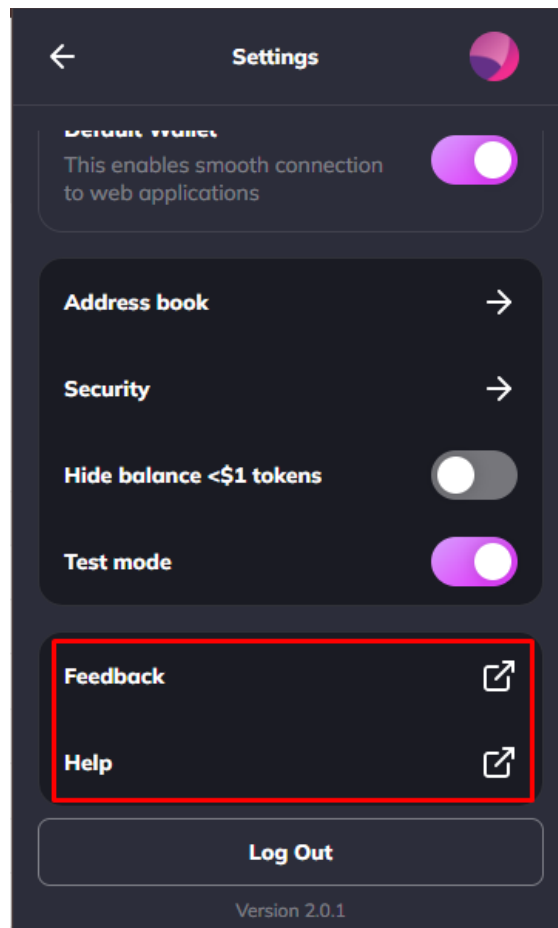
Severity

Info

Impact

Users cannot browser contents of feedback and help of this wallet.

Vulnerability Details



In Settings of the wallet, there are 2 links of “Feedback” and “Help”, but their links don’t work now.

In the page of Edit Account, if you reopen edit window and click close after changing avatar, the avatar will be reset as default.

Severity

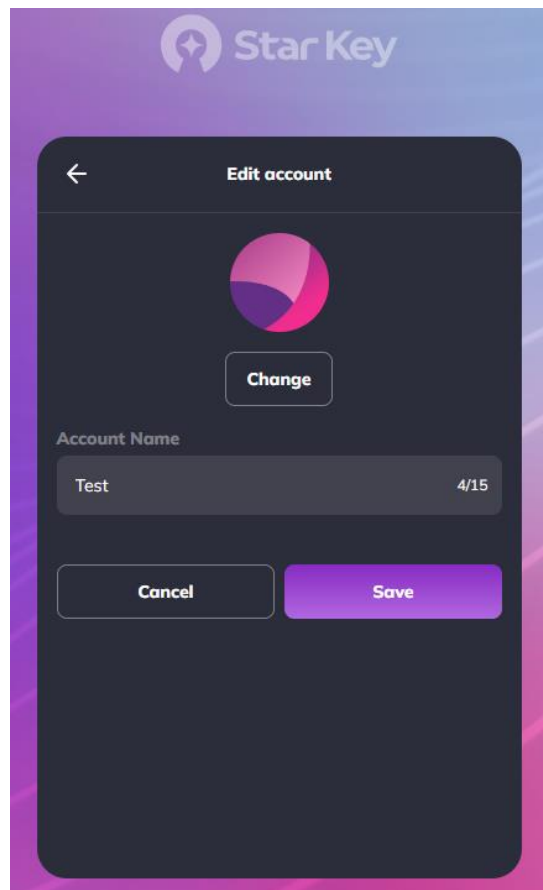
Info

Impact

Users will have issue to change their avatar images of star key wallet.

Vulnerability Details

In the page of “Edit Account”, if you reopen edit window and click close after changing avatar, the avatar will be reset as default.



In Address page, if you input address and then select network, already input address is removed.

Severity

Info

Impact

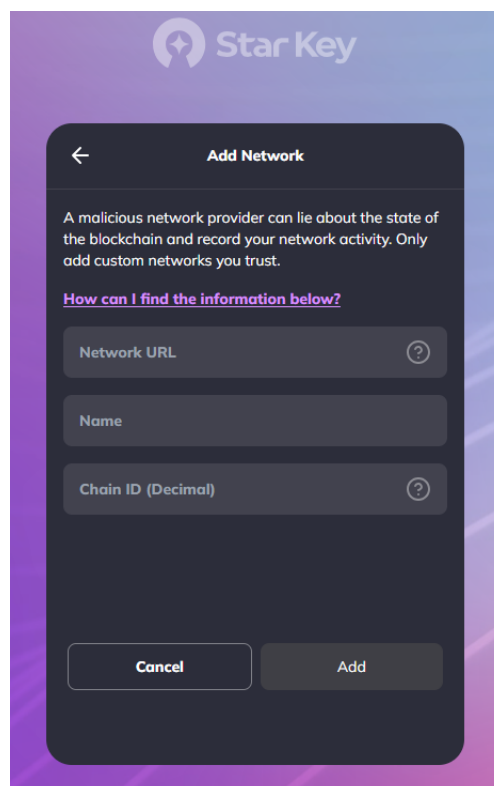
Users will have issue to input and save their contract information.

Vulnerability Details

When type address before changing chain, the content of typed address will be removed and user should type it again.

It will be uncomfortable for the case that type same address between EVM chains.

To keep user experience, it would be better to check address validation for selected network, then decide whether remove it or not.



When delete registered address, it would be better to ask confirm.

Severity

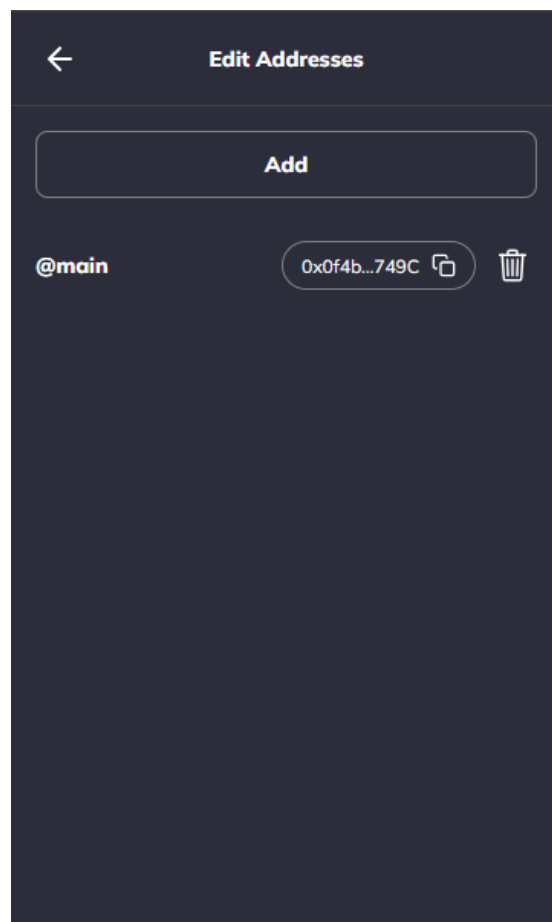
Info

Impact

It needs to show confirm message when a user delete his address.

Vulnerability detail

When, a user try to delete the address in his book, it is deleted instantly. To keep user experience, it would be better to ask confirm message that check if user really wants to delete it.



After adding new token, it would be better to using loading state when loading the price of added token

Severity

Info

Impact

While loading latest price of the token after it is added, the price is shown as 0. This may harm user experience in wallet usage.

Vulnerability Detail

To keep user experience and quality, it would be better to change the price component as loading component while loading latest price of newly added token.

