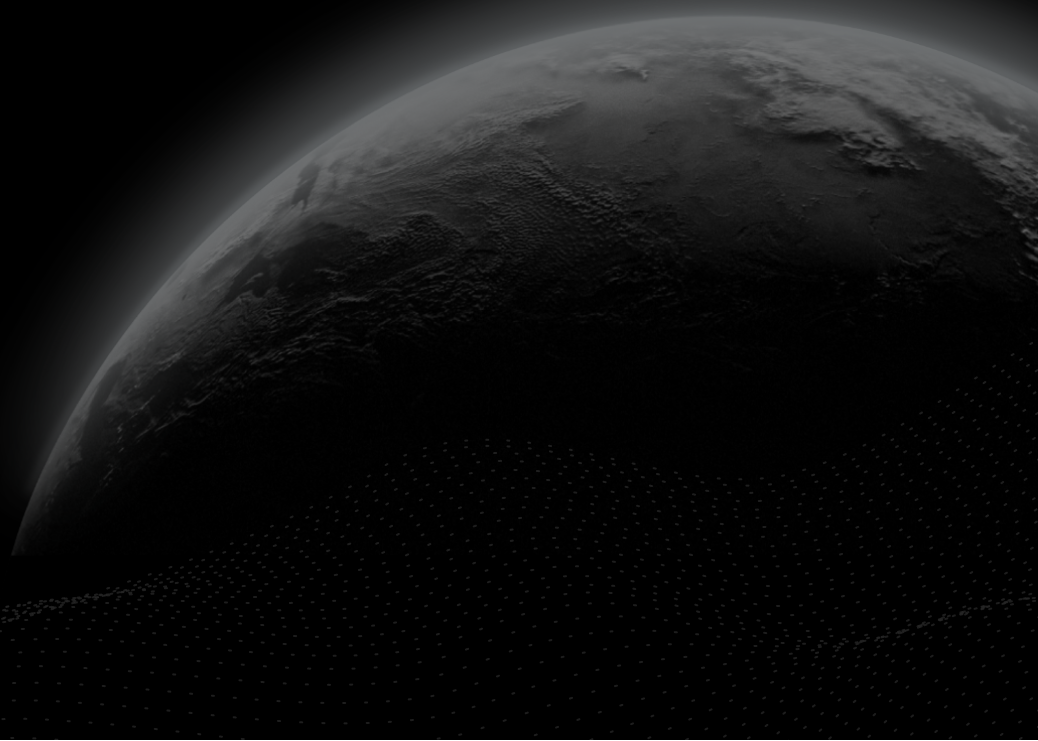
CERTIK

Security Assessment

Internet Money Wallet

CertiK Assessed on Jan 9th, 2023



CertiK Assessed on Jan 9th, 2023

Internet Money Wallet

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Other	Dynamic Testing, Manual Review

LANGUAGE	TIMELINE	KEY COMPONENTS
TypeScript	Delivered on 01/09/2023	N/A

Vulnerability Summary

12	11	0	0	1	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined

0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed immediately. Users should be cautious when interacting with any application with outstanding critical risks.
0	High		High risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds, thief of user data, and/or loss control of the application.
8	Medium	7 Resolved, 1 Acknowledged	Medium risks may not pose a security risk at a large scale, but they can affect the overall functioning of a platform or be used to target a certain group of users.
3	Low	3 Resolved	Low risks can be any of the above, but on a smaller impact. They generally do not compromise the overall integrity of the project.
1	Informational	1 Resolved	Informational errors are often recommendations to improve the configuration or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the application.

TABLE OF CONTENTS | INTERNET MONEY WALLET

SCOPE | INTERNET MONEY WALLET

Chrome Extension	Version Beta 1.0.36
Android Application	Version Beta 1.0.36
iOS Application	Version Beta 1.0.35

APPROACH & METHODS | INTERNET MONEY WALLET

This report has been prepared for Internetmoney to discover issues and vulnerabilities in the application of the Internet Money Wallet project. The Internet Money Wallet is a non-custodial crypto wallet that supports multiple ecosystems.

The pentest was a manual assessment of the security of the application's functionality, business logic, and vulnerabilities, such as those cataloged in the OWASP Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters leveraged tools to facilitate their work. However, the majority of the assessment involved manual analysis.

The main objective of the engagement is to test the overall resiliency of the application to various real-world attacks against the application's controls and functions and thereby be able to identify its weaknesses and provide recommendations to fix and improve its overall security posture.

Two members of the CertiK team were involved in completing the engagement, which took place over the course of 7 days in December 2022 and yielded 12 security-relevant findings. The most significant vulnerabilities are related to the insecure cryptography algorithms used against the password and encryption keys, credential reuse between different environments, and lack of sensitive information protection on the mobile application.

Other weaknesses were also found and are detailed in the Findings section of the report. We recommend addressing these findings to ensure a high level of security standards and industry practices and to raise the security posture of the application.

REVIEW NOTES | INTERNET MONEY WALLET

limitation

The "Wallet Dividend" feature in the application is not available for testing. The application display the message "Internet Money Wallet Dividend (WD) Coming Soon"

Source code for the initial review:

- imaginovation-imcrypto-chrome-extension-react-7b5e7f380a51
- imaginovation-imcrypto-mobile_app-react_native-2625263395e8
- imaginovation-imcrypto-web3-javascript-d84bd867dd33
- imaginovation-imcrypto-backend-nodejs-0003bb856803

Source code for the remediation:

- imaginovation-imcrypto-chrome-extension-react-7dbb7c248bbf
- imaginovation-imcrypto-mobile_app-react_native-fa4a9ca53c1b
- imaginovation-imcrypto-web3-javascript-a3bdde6bec05

FINDINGS | INTERNET MONEY WALLET

12	0	0	8	3	1
Total Findings	Critical	High	Medium	Low	Informational

This report has been prepared to discover issues and vulnerabilities for Internet Money Wallet. Through this security assessment, we have uncovered 12 issues ranging from different severity levels. Utilizing the techniques of Dynamic Testing & Manual Review to complement rigorous testing process, we discovered the following findings:

ID	Title	Category	Severity	Status
GLOBAL-01	Insecure Key Derivation Function	Insufficient Cryptography	Medium	Resolved
GLOBAL-02	Insecure Password Hashing Algorithm	Insufficient Cryptography	Medium	Resolved
GLOBAL-03	Mnemonic Display Allow Screenshot	Information Disclosure	Medium	Resolved
GLOBAL-04	Screenshot Backgrounding	Information Disclosure	Medium	Resolved
GLOBAL-05	Accounts, Secrets, And API Keys Reuse In Different Environments	Application Resource Handling	Medium	Resolved
GLOBAL-06	Unlimited Token Approval To A Unverified Contract	Centralization Risks	Medium	Resolved
GLOBAL-07	Problematic Behaviors When Swapping BNB To WBNB	Logic Flaws	Medium	Resolved
GLOBAL-08	Abusable "Claim Airdrop" Feature	Application Resource Handling	Medium	Acknowledged
GLOBAL-09	Verbose Error Message	Information Disclosure	Low	Resolved
GLOBAL-10	No Root Or Jailbreak Detection On Android/IOS Application	Reverse Engineering and Code Tampering	Low	Resolved

ID	Title	Category	Severity	Status
GLOBAL-11	Lack Of Token Name, Symbol And Decimal Validation	Application Resource Handling	Low	Resolved
GLOBAL-12	ATS Misconfiguration	Security Misconfiguration	Informational	Resolved

GLOBAL-01 | INSECURE KEY DERIVATION FUNCTION

Category	Severity	Location	Status
Insufficient Cryptography	Medium	https://github.com/brix/crypto-js/blob/971c31f0c931f913d22a76ed488d9216ac04e306/src/evpkdf.js#L22 imaginovation-imcrypto-web3-javascript-d84bd867dd33/web3-layer/web3Layer.js	Resolved

Description

The application uses the crypto-js's EVPKDF derivation function, which does a single iteration of the MD5 hash function to generate the encryption key. MD5 hash algorithm is not a key derivation function.

The code below from crypto-js library, shows the configuration used in the derivation function:

```
22  cfg: Base.extend({
23      keySize: 128/32,
24      hasher: MD5,
25      iterations: 1
26  }),
```

Impact

Using a fast hash function like MD5 can help an attacker accelerate a brute force attack.

Recommendation

Use a password-based key derivation function such as Argon2d, Scrypt, Bcrypt with sufficient iteration and salt to generate an encryption key with the user password.

Alleviation

Fixed in the version:"imaginovation-imcrypto-web3-javascript-a3bdde6bec05/web3-layer/web3Layer.js"

GLOBAL-02 | INSECURE PASSWORD HASHING ALGORITHM

Category	Severity	Location	Status
Insufficient Cryptography	Medium	imaginovation-imcrypto-web3-javascript-d84bd867dd33/web3-layer/web3Layer.js	Resolved

Description

The application generates the password hash by doing a double "keccak256", which is considered an insecure way to perform the password hashing.

```
export const getPasswordHash = (password) => {
  const web3 = new Web3();
  try {
    return web3.utils.keccak256(web3.utils.keccak256(password.toString()));
  } catch (error) {
    return null;
  }
};
```

Impact

Using a fast hash function like keccak256 can help an attacker accelerate a brute force attack. It's also possible vulnerable to the "rainbow table attack". https://en.wikipedia.org/wiki/Rainbow_table

Recommendation

It's recommended to use a strong and slow hashing algorithm like Argon2 or Bcrypt, combined with salt for password hashing.

Alleviation

Fixed in the version:"imaginovation-imcrypto-web3-javascript-a3bdde6bec05/web3-layer/web3Layer.js"

GLOBAL-03 | MNEMONIC DISPLAY ALLOW SCREENSHOT

Category	Severity	Location	Status
Information Disclosure	Medium		Resolved

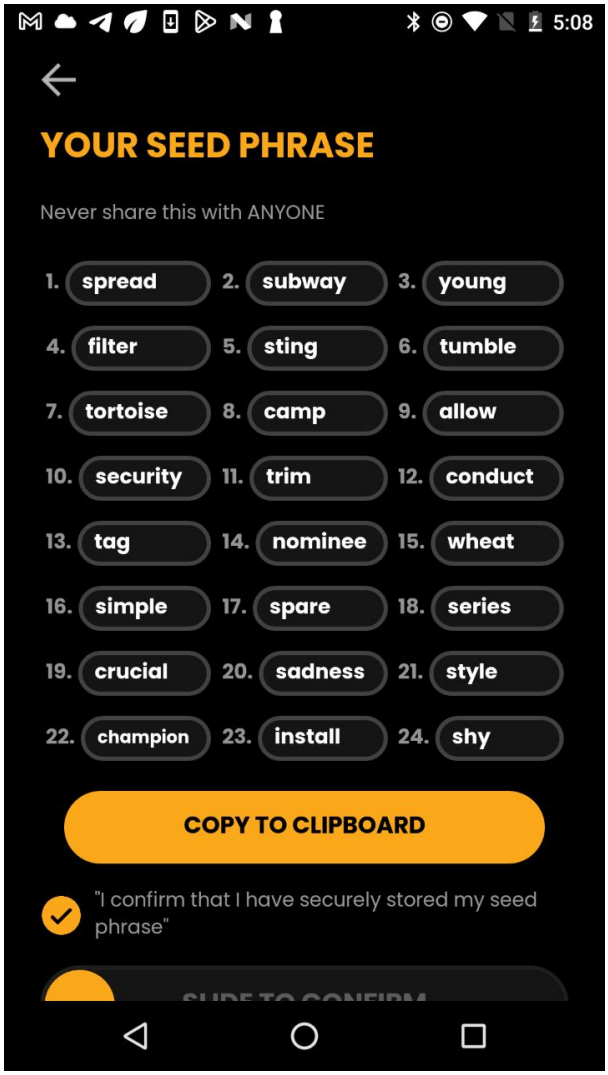
Description

The mnemonic phrase is a list of words that can be used to recover a wallet account. Obtaining the mnemonic can potentially allow the attacker to gain full control of the wallet. The application neither has a mechanism in place to stop a user from taking the screenshot of the displayed wallet secrets nor display a warning to remind the user of the risk of taking a screenshot.

Impact

Third party apps with "READ_EXTERNAL_STORAGE" permission on an Android device or apps with all photo access on an iPhone can read screenshots on the device. Third party apps can retrieve the mnemonic if the mnemonic is included in a screenshot taken by the user.

Proof of Concept



Recommendation

Screen capture can be prevented by setting the FLAG_SECURE option. The FLAG_SECURE flag can prevent user and malicious third-party apps from recording the mnemonic screens and taking screenshots of sensitive information. For more information about the FLAG_SECURE flag, please see “https://developer.android.com/reference/android/view/Display#FLAG_SECURE”

iOS

There isn't a built-in solution on iOS to prevent the user from taking the screenshot. It's recommended adding a warning to remind a user not to take screenshots when viewing their wallet secrets.

Alleviation

Fixed in version 1.0.44

GLOBAL-04 | SCREENSHOT BACKGROUNDING

Category	Severity	Location	Status
Information Disclosure	Medium		Resolved

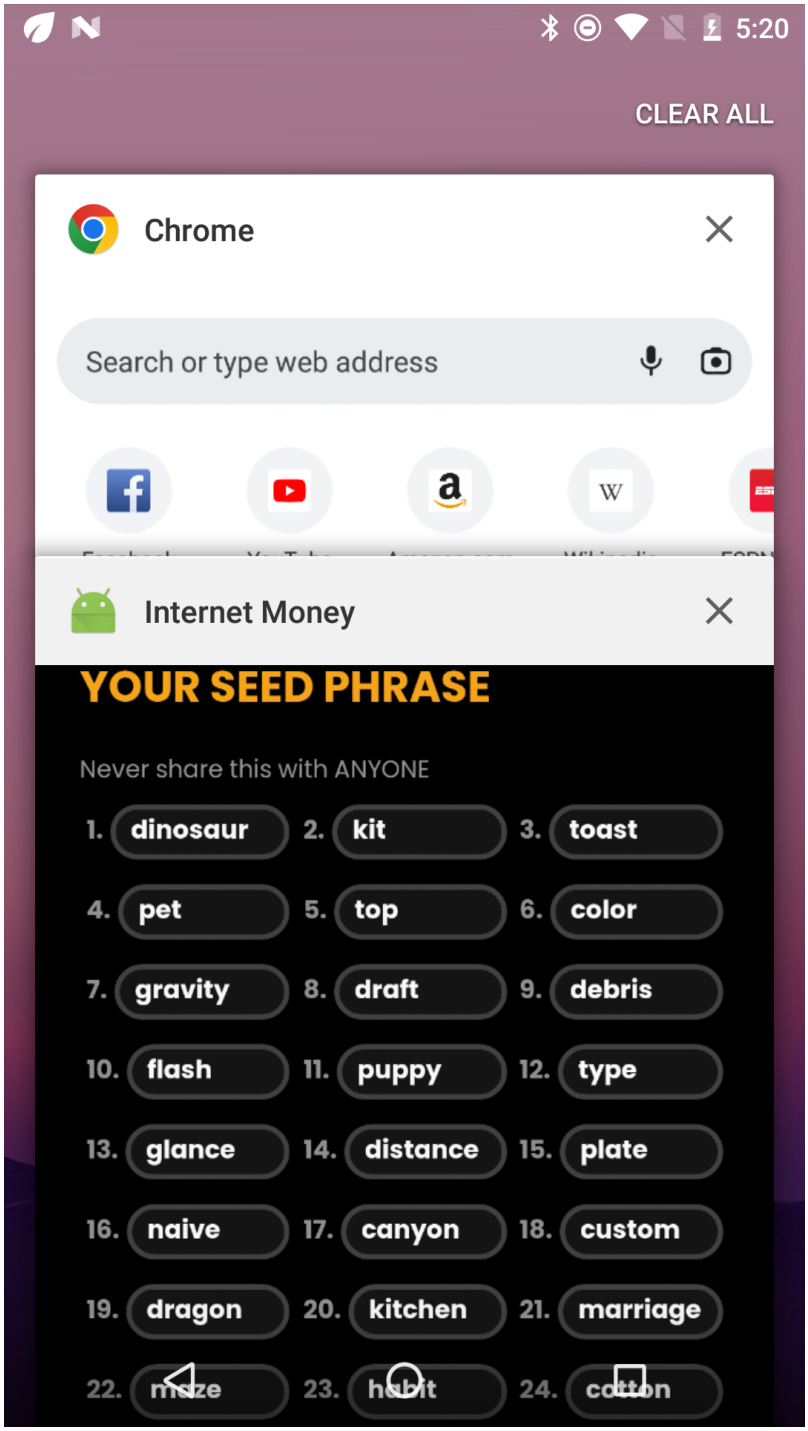
Description

On mobile devices, a screenshot of the current activity is taken when an application goes into the background and displayed for aesthetic purposes when the app returns to the foreground. This feature may pose a security risk. Sensitive data may be exposed if the user background the application while sensitive data is displayed. A malicious application that is running on the device and able to continuously capture the screen may also expose data.

Impact

An attacker with physical access to the unlocked device or a malicious third party app with access to the auto-generated screenshot of the application can retrieve sensitive information included in the screenshot.

Proof of Concept



Recommendation

It's recommended for the application to add an overlay to hide or obscure the application screen before moving to the background.

For iOS, add an overlay screen before the application goes into the background, and remove the screen when the application goes into the foreground.

For Android, in addition to adding an overlay, this can be done by setting the FLAG_SECURE option. The FLAG_SECURE flag can prevent sensitive information included in the auto-generated screenshot. For more information about the FLAG_SECURE flag, please see https://developer.android.com/reference/android/view/Display#FLAG_SECURE and

https://stackoverflow.com/questions/9822076/how-do-i-prevent-android-taking-a-screenshot-when-my-app-goes-to-the-background

GLOBAL-05 ACCOUNTS, SECRETS, AND API KEYS REUSE IN DIFFERENT ENVIRONMENTS

Category	Severity	Location	Status
Application Resource Handling	Medium	backend-nodejs/.env.development backend-nodejs/.env.production	Resolved

Description

Two environment variable files `.env.development` and `.env.production`, are found in the `backend-nodejs` folder. Many important accounts, secrets, and API keys are re-used between the development and the production environment.

Impact

It demonstrates a poor and insecure operation practice. The development environment should be intended for development and testing, and it's common for things to go wrong in this environment. If the development and the production environment share the account and APIs, any software error and security vulnerability will affect applications not only in the dev but also in production.

Recommendation

It's recommended the team use a completely different set of accounts, secrets, and API keys for two different environments.

Alleviation

The team updated the variables and provided proof that two environments use different environment variables

GLOBAL-06 UNLIMITED TOKEN APPROVAL TO A UNVERIFIED CONTRACT

Category	Severity	Location	Status
Centralization Risks	Medium		Resolved

Description

When users want to swap one token for another, the wallet application requires the user to approve the maximal token allowance for the "https://bscscan.com/address/0x02a060a1bb096572b3d6a67e20f8cdf48c92d7d4" contract. The contract is unverified in the blockchain explorer.

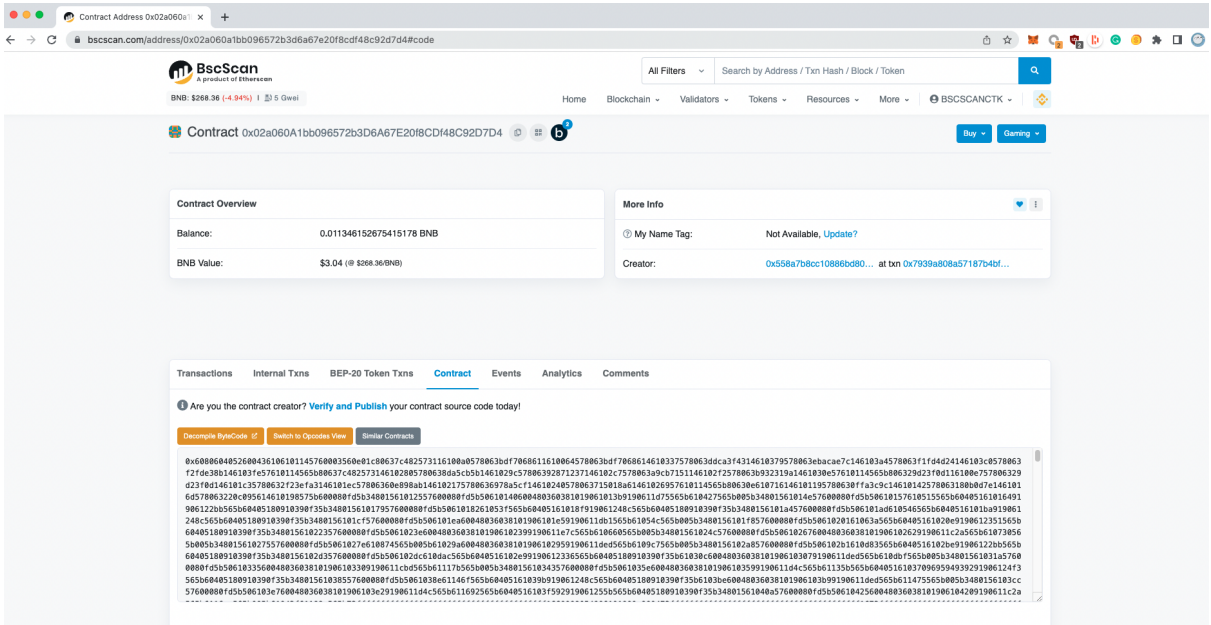
Impact

Approving maximal token allowance is risky as it allows the target contract to spend all the token balance or tokens deposited into the address in the future. Users have no way to perform "do your own research(DYOR)" if the contract is unverified in the blockchain explorer.

Reproduce Steps

Visit https://bscscan.com/address/0x02a060a1bb096572b3d6a67e20f8cdf48c92d7d4#code to view the unverified contract

Proof of Concept



Recommendation

It's highly recommended the team verify the smart contract in the blockchain explorer for the user's trust and transparency.

Alleviation

At the time of the re-test on September 21, 2023, the router contract has been configured as 'https://bscscan.com/address/0x9d9e4f6d93d2baaa8108d6ca32af9f1e27e94c8f#code,' and the contract is verified.

GLOBAL-07 PROBLEMATIC BEHAVIORS WHEN SWAPPING BNB TO WBNB

Category	Severity	Location	Status
Logic Flaws	Medium		Resolved

Description

WBNB is the wrapped version of the native BSC token BNB. BNB should always be able to redeem with a 1-1 ratio for WBNB. The application display a UI claim the BNB to WBNB flow is a "swap" and provides the "SushiSwap/PancakeSwap" as an option.

After selecting one of the DEX options and submitting the transaction, the transaction will always revert.

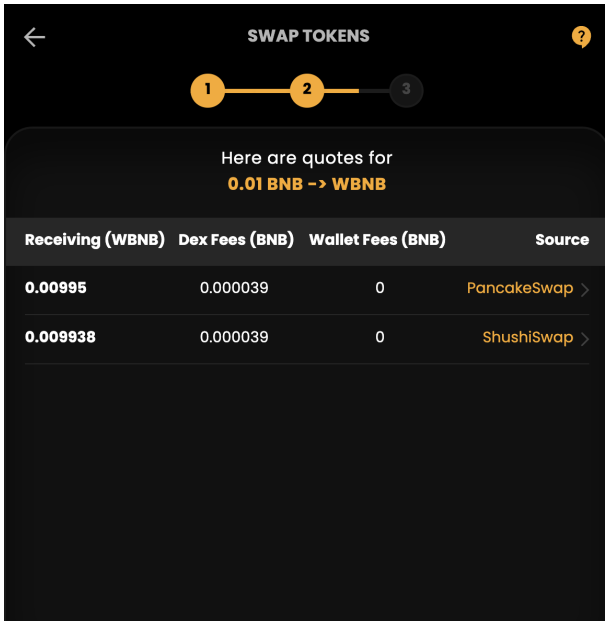
Impact

The UI displays incorrect information when an attempt to swap BNB to WBNB. It also wastes the user's gas because the transaction always fails.

Reproduce Steps

Swap BNB to WBNB in the wallet application

Proof of Concept



Failed transaction:

- https://bscscan.com/tx/0x1a5c794bb913977600ca0b17ccb8a6627822a1941bb2f5b9dc68e8d2616fa73f
- https://bscscan.com/tx/0xb7a80fc5914401fb37ed5577329ce9e5ee294da163457594b6dcbeb9e02c7a41

Recommendation

The wallet should handle the BNB to WBNB swap flow properly. It's also recommended that the team check if the same type of error will happen in edge cases like this.

Alleviation

Fixed in version "Beta 1.0.44"

GLOBAL-08 | ABUSABLE "CLAIM AIRDROP" FEATURE

Category	Severity	Location	Status
Application Resource Handling	Medium		Acknowledged

Description

The application provides the "claim airdrop" feature for new users to claim a small amount of BNB and IM tokens. The feature was exploited before the audit started, and now it's protected with re-captcha and IP-based rate limiting. However, the protection can be easily bypassed, and the attacker will be incentivized to abuse the feature if the airdrop reward is higher than the cost of getting phone numbers to receive an SMS code and an IP rotator.

Impact

The attacker can easily bypass the protection to abuse the "claim airdrop" feature.

Recommendation

As long as the airdrop reward is more than the cost to bypass the protection, the feature is always vulnerable. There is a couple of things to consider to mitigate the risk:

1. Lower the airdrop reward so that the attacker will not be incentivized to perform the attack
2. Require a stronger identity verification than phone number verification, such as a KYC verification.

Alleviation

The client acknowledged this finding.

GLOBAL-09 | VERBOSE ERROR MESSAGE

Category	Severity	Location	Status
Information Disclosure	Low		Resolved

Description

Improper handling of errors can introduce a variety of security problems for an application server. The most common one is the application return detailed stack traces, database dumps, and source code to the user when the server encounters an error. These messages reveal implementation details that should never be revealed. Multiple backend APIs of the internet money application return a verbose error message when receiving a malformed request.

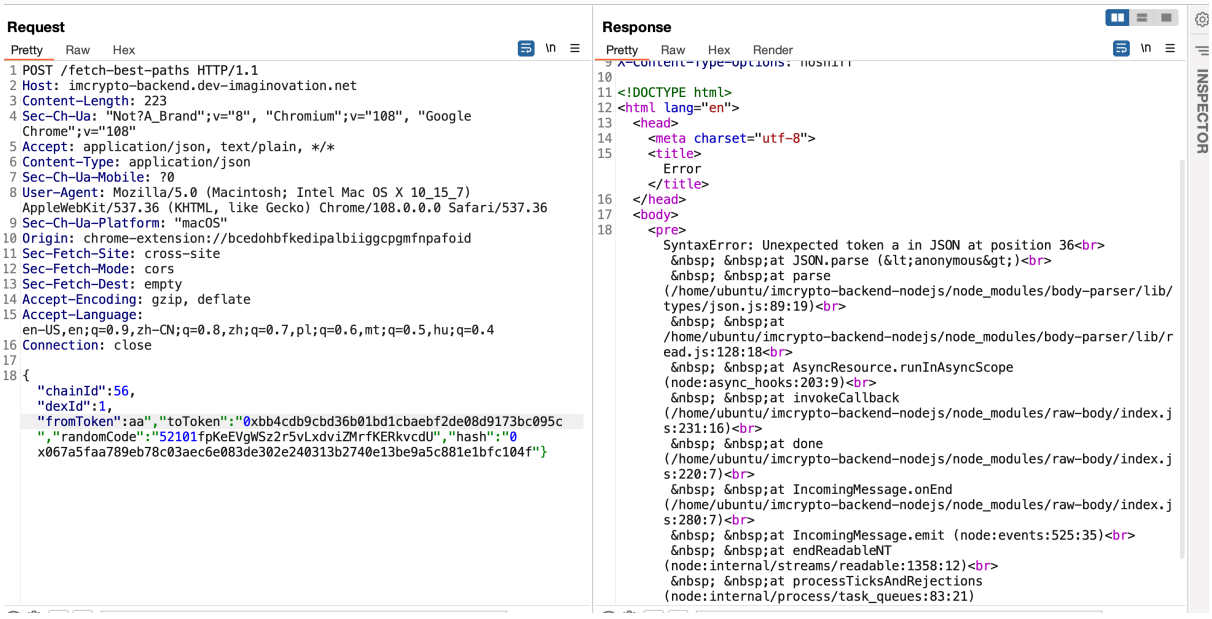
Impact

An attacker can gain important detail on code structure or potential flaws in the application. That information can potentially be used by an attacker to perform more sophisticated attacks. As shown in the evidence section, it leaks the [fixme]

Reproduce Steps

Submit a request with a malformed JSON body.

Proof of Concept



Recommendation

To mitigate this issue, the application server should handle server error properly and return a more generic error message.

GLOBAL-10 NO ROOT OR JAILBREAK DETECTION ON ANDROID/IOS APPLICATION

Category	Severity	Location	Status
Reverse Engineering and Code Tampering	Low		Resolved

Description

No root or jailbreak detection is implemented in the application. This allows an attacker to modify the app on a rooted Android or jailbroken iOS device, which means the attacker can potentially induce behaviors that otherwise would not occur. Examples of the impact include accessing sensitive application data, overwriting critical functions, and an overall wider attack surface.

Impact

A malicious application with root permission can access and modify data belongs to the application.

Recommendation

Implement root and jailbreak detection at the beginning of the runtime of your application. Display a warning message when a user attempts to use the wallet on a rooted or jailbroken device.

Some different methods to check for a jailbroken device are listed below:

Android

Check for existing su binaries, such as:

- /system/bin/su
- /system/xbin/su
- /sbin/su
- /system/su
- /system/bin/.ext/.su Attempt to use the su command directly and compare the current user ID before and after to see if the user was successfully upgraded to root. Utilize SafetyNet by Google. This was developed to try and detect device modifications and will prevent the application from running if the device fails the checks.

iOS

Check for the existence of common files or directories that are associated with a jailbroken device. A list of some of the potential files to check can be seen here:

- /Applications/Cydia.app
- /Applications/FakeCarrier.app
- /Applications/Icy.app
- /Applications/IntelliScreen.app /Applications/MxTube.app

Attempt to write to a file in a location that is outside of the applications virtual sandbox. An example would be to try and write to the /private directory. This attempt would fail on a non-jailbroken device because the application does not have permission to access anything outside of its virtual sandbox, but if the application succeeds in writing to that location, then it can be deduced that it has root permissions, which means that the device is jailbroken.

Alleviation

Fixed in version 1.0 (45)

GLOBAL-11 | LACK OF TOKEN NAME, SYMBOL AND DECIMAL VALIDATION

Category	Severity	Location	Status
Application Resource Handling	Low		Resolved

Description

The extension wallet allows users to import custom tokens, and display the token name and symbol in the wallet UI. The ERC20 token contract standard doesn't have any restrictions on any of the token properties, and anyone can deploy token contracts on the blockchain. Once a token is added, the wallet will fetch the information and display them in it's interface.

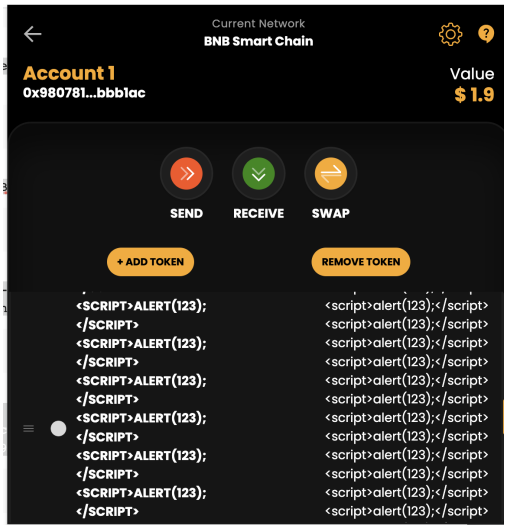
Impact

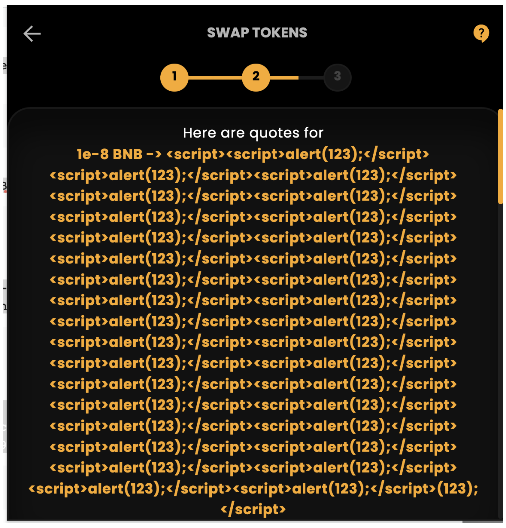
Importing a crafted malicious token can bring a negative user experience to the user, and the attacker can potentially craft a message to perform a phishing attack.

Reproduce Steps

Import the following token "0xe9bb17e159Ff8551e08616Fd310192ea57BBe52b" in the BSC Smart chain.

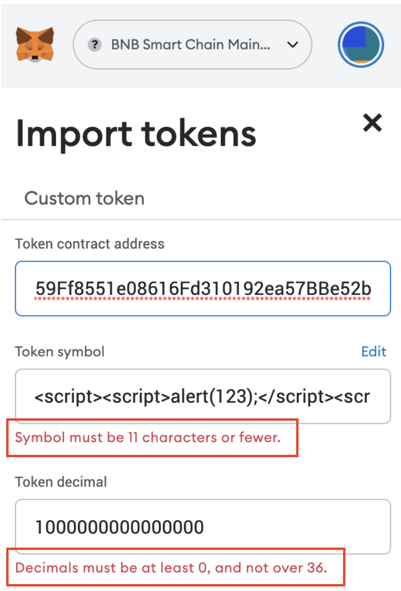
Proof of Concept





Recommendation

It's recommended to place restrictions on the token name, symbol, and decimals similar to the following:



Alleviation

Fixed in version "Beta 1.0.44"

GLOBAL-12 | ATS MISCONFIGURATION

Category	Severity	Location	Status
Security Misconfiguration	Informational	Repositories/imaginovation-imcrypto-mobile_app-react_native-2625263395e8/ios/ImCryptoWallet/Info.plist	Resolved

Description

App Transport Security (ATS) is a set of security checks that the operating system enforces when making connections with NSURLConnection, NSURLSession and CFURL to public hostnames. ATS is enabled by default for applications build on iOS SDK 9 and above.

During the pentest, it is observed that on the iOS App, the App Transport Security restrictions are disabled for all network connections. Disabling ATS means that unsecured HTTP connections are allowed. HTTPS connections are also allowed and are still subject to default server trust evaluation. However, extended security checks like requiring a minimum Transport Layer Security (TLS) protocol version are disabled.

- https://developer.apple.com/documentation/bundleresources/information_property_list/nsapptransportsecurity
- https://cwe.mitre.org/data/definitions/919.html

Impact

Disabling ATS can allow insecure communication with particular servers or allow insecure loads for web views or for media while maintaining ATS protections elsewhere in your app.

Reproduce Steps

Observe that the `NSExceptionAllowsInsecureHTTPLoads` is set to `True`

```
34          <dict>
35              <key>NSExceptionAllowsInsecureHTTPLoads</key>
36              <true/>
37          </dict>
38      </dict>
39  </dict>
```

Recommendation

Set the `NSExceptionAllowsInsecureHTTPLoads` key value to False in `info.plist` file. If it's required to be set to Yes for some functionalities then Implement the following list of App Transport Security Requirements;

- Enable additional security features like Certificate Transparency using the `NSRequiresCertificateTransparency` key.

- Reduce or remove security requirements for communication with particular servers using the `NSExceptionDomains` key.
- Ensure that the X.509 Certificate has a SHA256 fingerprint and must be signed with at least a 2048-bit RSA key or a 256-bit Elliptic-Curve Cryptography (ECC) key.
- Transport Layer Security (TLS) version must be 1.2 or above and must support Perfect Forward Secrecy (PFS) through Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange and AES-256 symmetric ciphers.
- If the application connects to a defined number of domains that the application owner controls, then configure the servers to support the ATS requirements and opt-in for the ATS requirements within the application according to best practices defined by Apple.

Alleviation

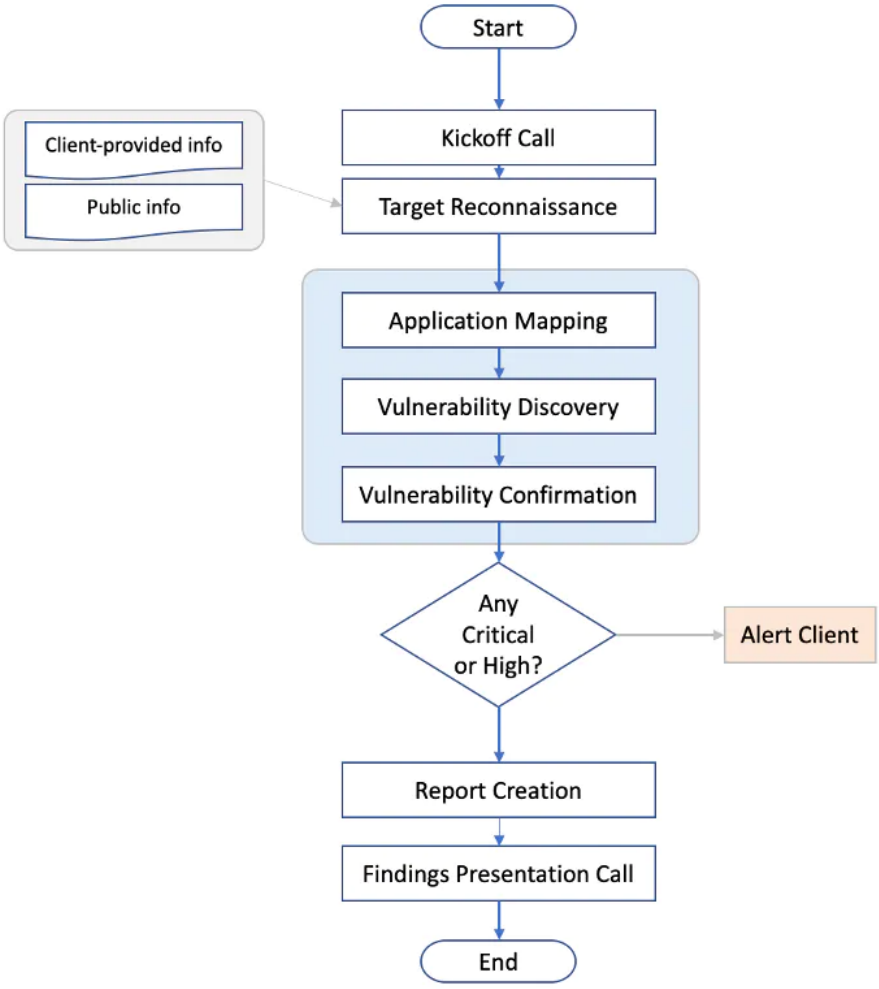
Fix in the version: imaginovation-imcrypto-mobile_app-react_native-fa4a9ca53c1b/ios/ImCryptoWallet/Info.plist

APPENDIX | INTERNET MONEY WALLET

Methodology

CertiK uses a comprehensive penetration testing methodology which adheres to industry best practices and standards in security assessments including from OWASP (Open Web Application Security Project), NIST, PTES (Penetration Testing Execution Standard).

Below is a flowchart of our assessment process:



Coverage and Prioritization

As many components as possible will be tested manually. Priority is generally based on three factors: critical security controls, sensitive data, and the likelihood of vulnerability.

Critical security controls will always receive the top priority in the test. If a vulnerability is discovered in the critical security control, the entire application is likely to be compromised, resulting in a critical-risk to the business. For most applications, critical controls will include the login page, but it could also include major workflows such as the checkout function in an online store.

The Second priority is given to application components that handle sensitive data. This is dependent on business priorities,

but common examples include payment card data, financial data, or authentication credentials.

Final priority includes areas of the application that are most likely to be vulnerable. This is based on CertiK' experience with similar applications developed using the same technology or with other applications that fit the same business role. For example, large applications will often have older sections that are less likely to utilize modern security techniques.

Reconnaissance

CertiK gathers information about the target application from various sources depending on the type of test being performed. CertiK obtains whatever information that is possible and appropriate from the client during scoping and supplements it with relevant information that can be gathered from public sources. This helps provide a better overall picture and understanding of the target.

Application Mapping

CertiK examines the application, reviewing its contents, and mapping out all its functionalities and components. CertiK makes use of different tools and techniques to traverse the entire application and document all input areas and processes. Automated tools are used to scan the application and it is then manually examined for all its parameters and functionalities. With this, CertiK creates and widens the overall attack surface of the target application.

Vulnerability Discovery

Using the information that is gathered, CertiK comes up with various attack vectors to test against the application. CertiK uses a combination of automated tools and manual techniques to identify vulnerabilities and weaknesses. Industry-recognized testing tools will be used, including Burp Suite, Nikto, Metasploit, and Kali. Furthermore, any controls in place that would inhibit the successful exploitation of a particular system will be noted.

Vulnerability Confirmation

After discovering vulnerabilities in the application, CertiK validates the vulnerabilities and assesses its overall impact. To validate, CertiK performs a Proof-of-Concept of an attack on the vulnerability, simulating real world scenarios to prove the risk and overall impact of the vulnerability.

Through CertiK's knowledge and experience on attacks and exploitation techniques, CertiK is able to process all weaknesses and examine how they can be combined to compromise the application. CertiK may use different attack chains, leveraging different weaknesses to escalate and gain a more significant compromise.

To minimize any potential negative impact, vulnerability exploitation was only attempted when it would not adversely affect production applications and systems, and then only to confirm the presence of a specific vulnerability. Any attack with the potential to cause system downtime or seriously impact business continuity was not performed. Vulnerabilities were never exploited to delete or modify data; only read-level access was attempted. If it appeared possible to modify data, this was noted in the list of vulnerabilities below.

Immediate Escalation of High or Critical Findings

If critical or high findings are found whereby application elements are compromised, client's key security contacts will be notified immediately.

Risk Assessment

Risk Level	CVSS Score	Impact	Exploitability
Critical	9.0-10.0	Root-level or full-system compromise, large-scale data breach	Trivial and straightforward
High	7.0-8.9	Elevated privilege access, significant data loss or downtime	Easy, vulnerability details or exploit code are publicly available, but may need additional attack vectors (e.g., social engineering)
Medium	4.0-6.9	Limited access but can still cause loss of tangible assets, which may violate, harm, or impede the org's mission, reputation, or interests.	Difficult, requires a skilled attacker, needs additional attack vectors, attacker must reside on the same network, requires user privileges
Low	0.1-3.9	Very little impact on an org's business	Extremely difficult, requires local or physical system access
Informational	0.0	Discloses information that may be of interest to an attacker.	Not exploitable but rather is a weakness that may be useful to an attacker should a higher risk issue be found that allows for a system exploit

DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

CertiK | Securing the Web3 World

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.