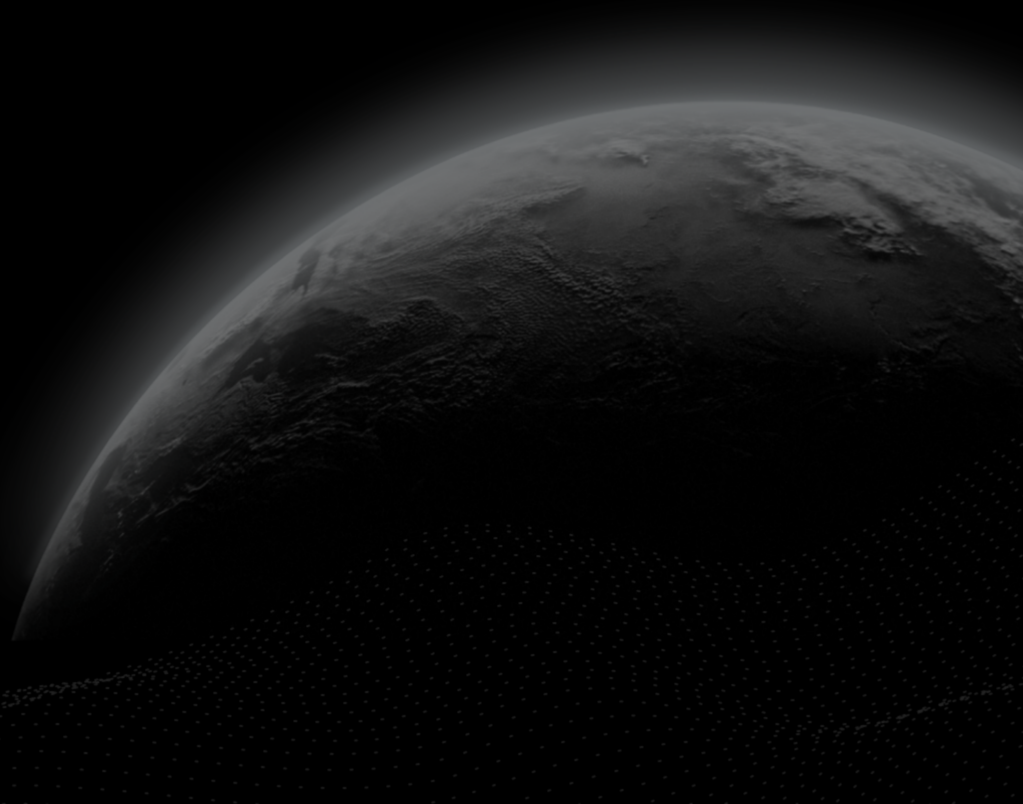
Security Assessment

StarShell - Pentest

CertiK Verified on Jan 25th, 2023



CertiK Verified on Jan 25th, 2023

StarShell - Pentest

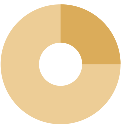
The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
Others	Cosmos (ATOM)	Dynamic Testing, Manual Review

LANGUAGE	TIMELINE	KEY COMPONENTS
TypeScript	Delivered on 01/25/2023	N/A

Vulnerability Summary



4	3	0	0	1	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

🟥	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.
🟨	1	Medium	1 Resolved	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	2 Resolved, 1 Acknowledged	Low risks can be any of the above, but on a smaller impact. They generally do not compromise the overall integrity of the project.
🟦	0	Informational		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 | STARSHELL - PENTEST

SCOPE | STARSHELL - PENTEST

StarShell extension wallet	Version Beta 0.7.0
Source code	https://github.com/SolarRepublic/starshell-beta/tree/dcc2021eeccd08a3086ba6948dc9f4261b98db88

APPROACH & METHODS | STARSHELL - PENTEST

This report has been prepared for StarShell to discover issues and vulnerabilities in the application of the StarShell - Pentest project. Starshell is a privacy-preserving, free, and open-source Web3 wallet built for the Secret Network and Cosmos ecosystem.

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 10 days in December 2022 and January 2023 and yielded 4 security-relevant findings. The most significant vulnerabilities are Weak password policy and Lack of "disconnect" option.

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 | STARSHELL - PENTEST

Wallet secret and password storage

The user password, private key, account information, providers and all sensitive information are stored in `chrome.storage.local`. Wallet creates a special vault that encrypts values. Depending on the importance of the information, the vault also encrypts keys in the `chrome.storage.local`

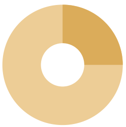
Vault encryption happens as below:

- Wallet first takes a passphrase from the user.
- Wallet then generates 128 bits of secure random values and calls it entropy.
- After generating the entropy, the wallet generates 128 bits of a secure random nonce value.
- Wallet then generates root keys `eg:(root0)` with Argon2 key derivation function.
    - Specs: Iteration:48, User supplied passphrase, Nonce generated at the beginning, type: Argon2id
- Wallet then generates `dk_key` from `root0` using HKDF key derivation function. This key is used for encrypt/decrypt value in the local storage. For encryption in the local storage wallet, it uses AES-GCM 256 bits.
- Wallet generates a signature using HMAC SHA-256 and saves it in the local storage. When the user wants to unlock the wallet, the wallet generates a new signature from user supplied password and verifies it with the previous one.

List of features included in the wallet but are not tested due to not being fully functional during the testing period

- Agents
- Tokens - Send(The "TO" field is not available)
- Backup and import private key
- Submitting proposal on SecretNodes

FINDINGS | STARSHELL - PENTEST



4	0	0	1	3	0
Total Findings	Critical	High	Medium	Low	Informational

This report has been prepared to discover issues and vulnerabilities for StarShell - Pentest. Through this security assessment, we have uncovered 4 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	Lack Of "Disconnect" Option	Logic Flaws	Medium	● Resolved
GLOBAL-02	Weak Password Policy	Account Policy	Low	● Resolved
GLOBAL-03	Missing Security Headers	Security Misconfiguration	Low	● Acknowledged
GLOBAL-04	Lack Of Disable Access Option	Logic Flaws	Low	● Resolved

GLOBAL-01 | LACK OF "DISCONNECT" OPTION

Category	Severity	Location	Status
Logic Flaws	● Medium		● Resolved

Description

The wallet has a window pop-up that asks for user permission when the user wants to connect to the Dapps for the first time. Connected Dapps can obtain user wallet address information and send messages/transactions for the wallet to sign. The wallet doesn't provide the option for users to revoke the permission.

Impact

If a Dapp is compromised and the users don't want the wallet to be connected to the Dapp anymore, users have no easy way to do so.

Recommendation

It's recommended the wallet add an option for the user to disconnect from a Dapp and remove the permission for the Dapp to connect automatically.

Alleviation

The team heeded the advice and resolved the finding in the commit hash d4d6bb573503eb2bb578e375b13249f89463c181.

GLOBAL-02 | WEAK PASSWORD POLICY

Category	Severity	Location	Status
Account Policy	● Low		● Resolved

Introduction

An authentication mechanism is only as strong as its credentials. For this reason, it is important to require users to have strong passwords. Lack of password complexity significantly reduces the search space when trying to guess the user's passwords, making brute-force attacks easier.

Description

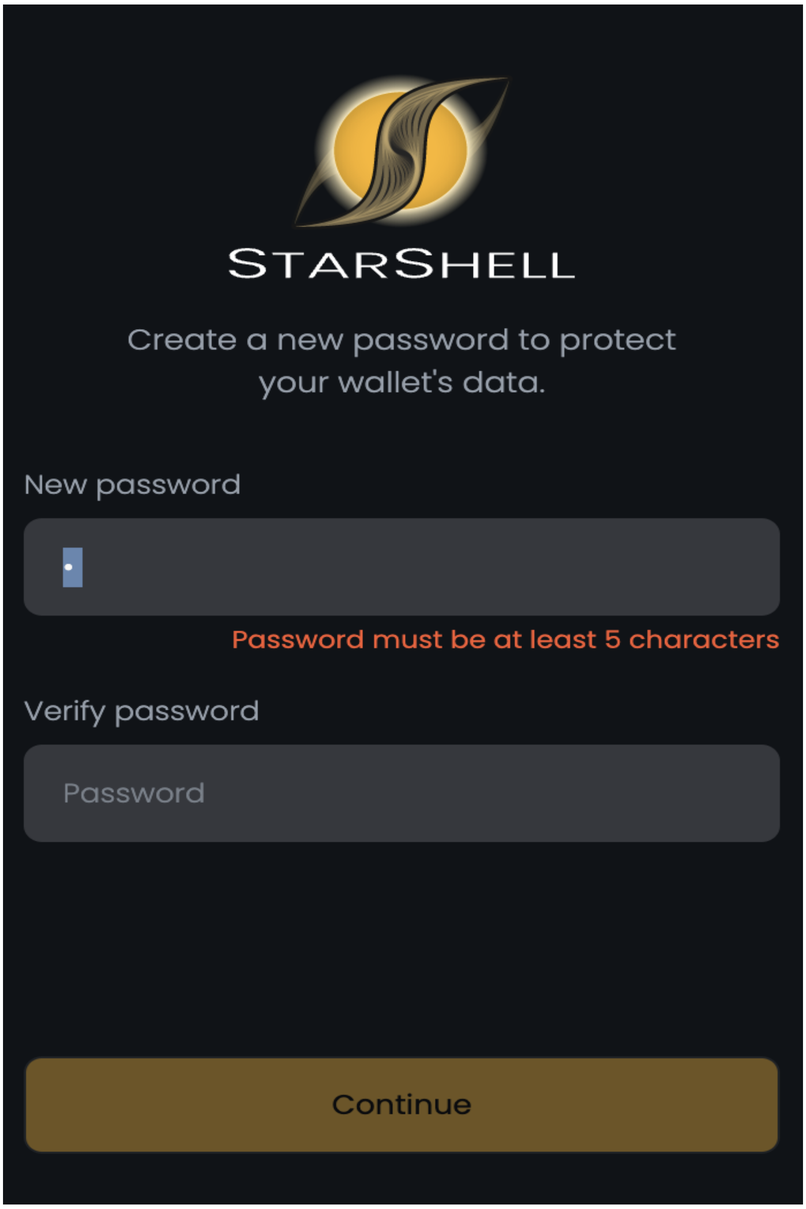
The currently implemented password policy is permissive regarding the requirements related to the password length and complexity, as it allows 5 character strings and doesn't require the use of special characters.

Impact

Weak password policies may allow users to create an easy-to-guess password. An attacker with local access can gain unauthorized access to the wallet by brute-forcing the weak password.

Reproduce Steps

After installing the app or resetting the wallet, the extension requests the user to set a password. Upon submitting a weak password, the extension displays the currently implemented password policy, which requires the string to contain at least 5 characters, it not having any requirements regarding the use of special characters:



Create a new password to protect your wallet's data.

New password

•

Password must be at least 5 characters

Verify password

Password

Recommendation

It's recommended to implement a stronger password policy for the user accounts. Strong password policies should include at least eight characters, containing uppercase and lowercase letters, numbers, and special characters.

Alleviation

The team heeded the advice and resolved the finding in the commit hash 67b518511a29e93cdba0d56d772a7e6f108bb301.

GLOBAL-03 | MISSING SECURITY HEADERS

Category	Severity	Location	Status
Security Misconfiguration	● Low	https://faucet.starshell.net/ https://launch.starshell.net/	● Acknowledged

Description

HTTP headers are well known and their implementation can make your application more versatile and secure. Modern browsers support many HTTP headers that can improve web application security to protect against clickjacking, cross-site scripting, and other common attacks. The important ones are missing and should be added to the response headers. They are listed below.

- `Content-Security-Policy` - Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
- `X-Frame-Options` - X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
- `HSTS` - HTTP Strict Transport Security (also named HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS. It also prevents HTTPS click through prompts on browsers.

Note that not all headers will be relevant for each endpoint, but security best practices stipulate that these headers should be set for all server responses, regardless of content.

Impact

- The lack of `X-Frame-Options` header could make the application vulnerable to Clickjacking / UI Redressing attacks.
- The lack of `X-Content-Type-Options` header enables a browser to perform MIME sniffing when the Content-Type header is not set or its value seems inappropriate. It can lead to severe issues such as an XSS attack in certain circumstances.
- The lack of `Content-Security-Policy` header could make the application vulnerable to Cross-Site Scripting (XSS), clickjacking, and other code injection attacks that rely on executing malicious content in the context of a trusted web page.
- `Permissions-Policy` ensures user privacy by limiting or specifying the features of the browsers can be used by the web resources.

Reproduce Steps

Visit https://faucet.starshell.net/:

```
HTTP/2 200
accept-ranges: bytes
content-length: 1113
content-type: text/html; charset=utf-8
last-modified: Mon, 02 Jan 2023 09:55:19 GMT
date: Tue, 03 Jan 2023 13:56:42 GMT
```

Visit https://launch.starshell.net/:

```
HTTP/2 200
server: openresty
date: Thu, 05 Jan 2023 09:31:10 GMT
content-type: text/html; charset=UTF-8
content-length: 12331
vary: Accept-Encoding
last-modified: Thu, 29 Sep 2022 22:57:22 GMT
vary: Accept-Encoding
etag: "633622d2-302b"
x-frame-options: sameorigin
x-cache: MISS
x-service: pixie-sh
accept-ranges: bytes
```

Recommendation

It is recommended to set the missing Security HTTP response headers. Following are the examples to securely implement them. (Note: `X-XSS-Protection` Header is Deprecated now)

- `X-Frame-Options: Deny`
- `Content-Security-Policy: default-src 'self'` (Note: Content Security Policy has a significant impact on how the browser renders pages, so careful tuning is required.)
- HSTS header set the "max-age-header" to at least 1 year.

Reference: OWASP Secure Headers Project https://owasp.org/www-project-secure-headers/ https://developers.cloudflare.com/ssl/edge-certificates/additional-options/http-strict-transport-security.

Alleviation

The client acknowledged this finding and will fix the finding in the future.

GLOBAL-04 | LACK OF DISABLE ACCESS OPTION

Category	Severity	Location	Status
Logic Flaws	● Low		● Resolved

Description

The StarShell wallet aims to protect user privacy; for this reason, it does not register Keplr API on the web pages automatically. Users need to enable Keplr API so Dapps can access the wallet. Because the API is not registered automatically, webpages will not know if the user has a wallet. The wallet doesn't provide the option for users to revoke access to Keplr API.

Impact

If a Dapp is compromised or the users don't want to permit that Dapp to use Keplr API anymore, users have no easy way to do so.

Recommendation

It's recommended the wallet add an option for the user to disable access to Keplr API for selected the Dapp.

Alleviation

The team heeded the advice and resolved the finding in the commit hash d4d6bb573503eb2bb578e375b13249f89463c181.

APPENDIX | STARSHELL - PENTEST

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.