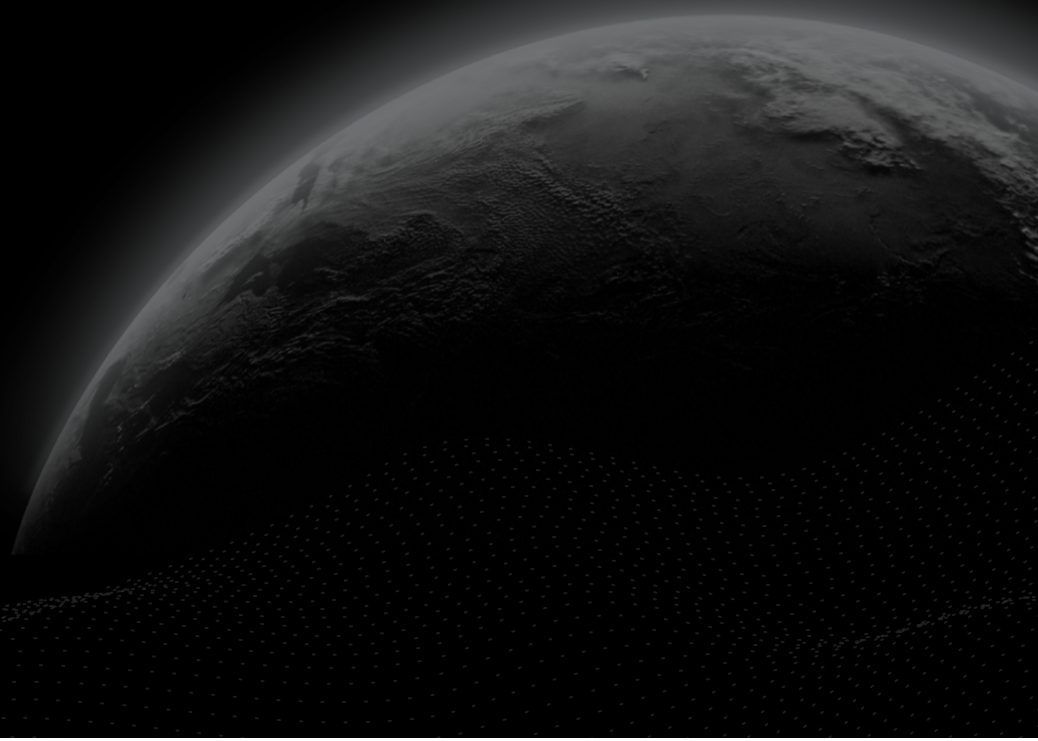
CERTIK

Security Assessment

XMTP - security assessment

CertiK Verified on Feb 6th, 2023



CertiK Verified on Feb 6th, 2023

XMTP - security assessment

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
Messaging Protocol	Web Application	Dynamic Testing
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Golang, JavaScript	Delivered on 02/06/2023	N/A

Vulnerability Summary

2	0	0	0	2	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 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.
1	Low	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 | XMTP - SECURITY ASSESSMENT

APPROACH & METHODS | XMTP - SECURITY ASSESSMENT

This report has been prepared for XMTP to discover issues and vulnerabilities in the application of the XMTP - security assessment project. XMTP (Extensible Message Transport Protocol) is an open network, protocol, and standard for secure messaging between blockchain accounts.

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 attack vectors investigated during the engagement are displayed below, but not limited to:

- **Cryptographic issues**: CertiK investigated the cryptographic mechanisms and algorithms used during multiple phases of the environment, such as the public/private/shared key generations, message encryption/decryption, and envelope signing.
- **API data handling**: the API endpoints were tested for scenarios in which malformed data was submitted in order to observe potential anomalies in the returned HTTP responses.
- **Code Injection Issues**: the API server was tested for potential vulnerabilities through which an attacker could execute arbitrary instructions on the server (Remote Code Execution, Serialization Vulnerabilities, components with known vulnerabilities, etc.)
- **Access Control Mechanisms**: CertiK investigated the Access Control Mechanisms implemented by the API server and the network itself in order to verify that the data stored on the network cannot be retrieved without an appropriate level of authorization.
- **Server misconfigurations**: the testing covered any potential vulnerabilities related to the configuration of the API server, such as debugging/testing ports or endpoints and HTTP parsing issues (HTTP Request Smuggling, CRLF injections, Race Conditions).

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 5 days in January 2023 and yielded 2 security-relevant findings. 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 | XMTP - SECURITY ASSESSMENT

XMTP Labs is a web3 software company that contributes to XMTP (Extensible Message Transport Protocol), an open network, protocol, and standards for secure messaging between blockchain accounts.

An XMTP message API client (client) and the XMTP network cannot (and should not) access a user's blockchain account keys. For this reason, a client generates a set of identity keys to serve as proxies for a user's blockchain account keys.

Blockchain accounts sign and advertise a set of keys that XMTP uses to establish a shared secret for encryption using another account's keys. These keys attest to the authenticity of both accounts and are required to send and retrieve the encrypted message blocks from the nodes.

Both message encryption and decryption are done by first generating a shared secret based on the accounts' keypairs using Diffie-Hellman key exchange. Then, the encryption key is generated from the shared secret using the HKDF key derivation function. Upon decryption but before presentation to the recipient, the client app uses the sender's public key from the message header to verify the sender of the message.

Certik has performed tests on the API endpoints for various attack scenarios. Among the tests performed, we have verified that the server properly sanitizes any user input in the HTTP requests and that no injection attacks are possible. We also verified the API properly handles errors and that generic messages are shown when an unexpected or security-sensitive error occurs and that the application enforces access control rules and if they could be bypassed. Tests were also performed on the XMTP protocol itself, specifically on how the key bundle generation is performed, as well as on the invitation and messaging functionalities.

FINDINGS | XMTP - SECURITY ASSESSMENT

2	0	0	1	1	0
Total Findings	Critical	High	Medium	Low	Informational

This report has been prepared to discover issues and vulnerabilities for XMTP - security assessment. Through this security assessment, we have uncovered 2 issues ranging from different severity levels. Utilizing the techniques of Dynamic Testing to complement rigorous testing process, we discovered the following findings:

ID	Title	Category	Severity	Status
GLOBAL-01	Centralized Risk	Security Misconfiguration	Medium	Acknowledged
GLOBAL-02	Public Access To Communication Metadata	Information Disclosure	Low	Acknowledged

GLOBAL-01 | CENTRALIZED RISK

Category	Severity	Location	Status
Security Misconfiguration	Medium		Acknowledged

Description

Currently all the nodes are operated by the same entity in both the development and production environments. This can also be seen in the documentation brief:

Network

Is the XMTP network decentralized?

Currently, XMTP Labs (the company) operates all of the network nodes in the two available XMTP network environments: `dev` and `production`.

Decentralization of the XMTP network will be achieved by a diverse set of independent third parties operating nodes.

XMTP Labs is working toward a phased decentralization of the network and will share a roadmap in the coming months.

Impact

There is a risk that if a denial of service attack would be performed on the IP location, the network's availability could be affected.

Recommendation

We recommend that the client continues the decentralization efforts by expanding the XMTP network to a diverse set of third party operators.

Alleviation

The XMTP Labs Team acknowledged the risk regarding the current centralization level of the network. XMTP Labs is working towards an decentralization roadmap which is planned to be released soon.

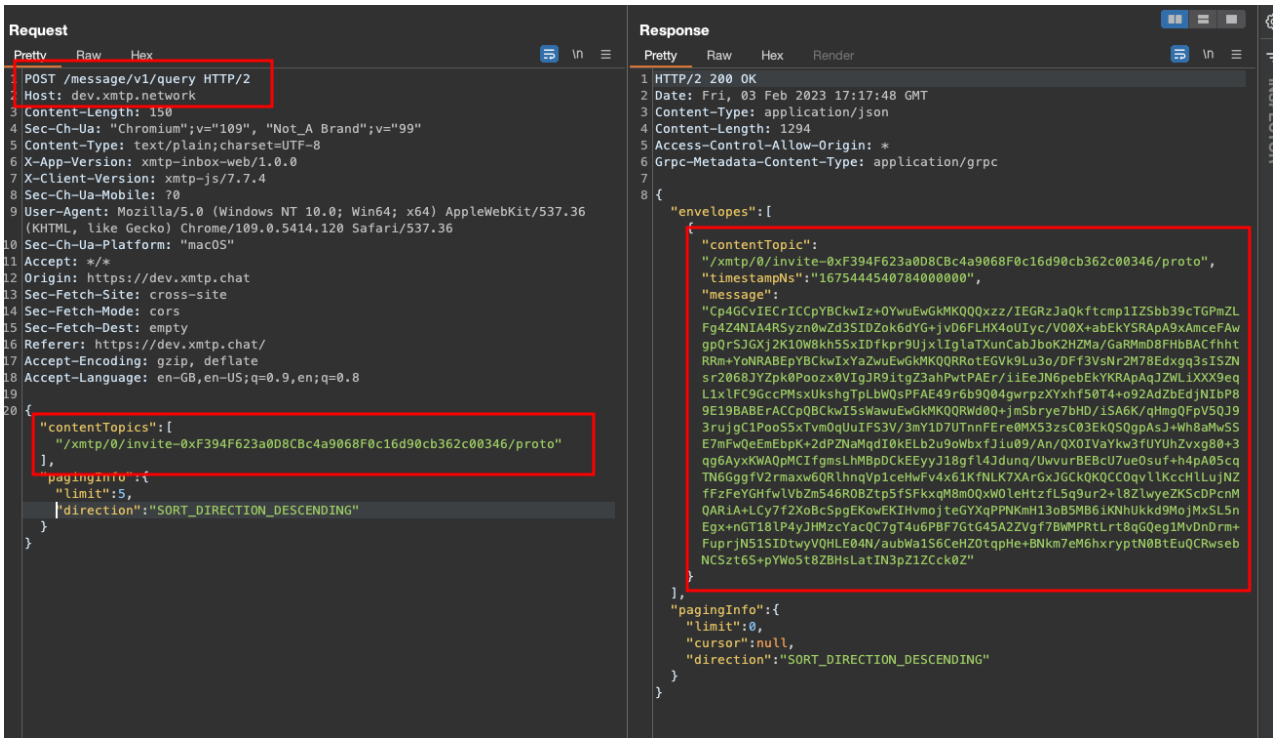
GLOBAL-02 | PUBLIC ACCESS TO COMMUNICATION METADATA

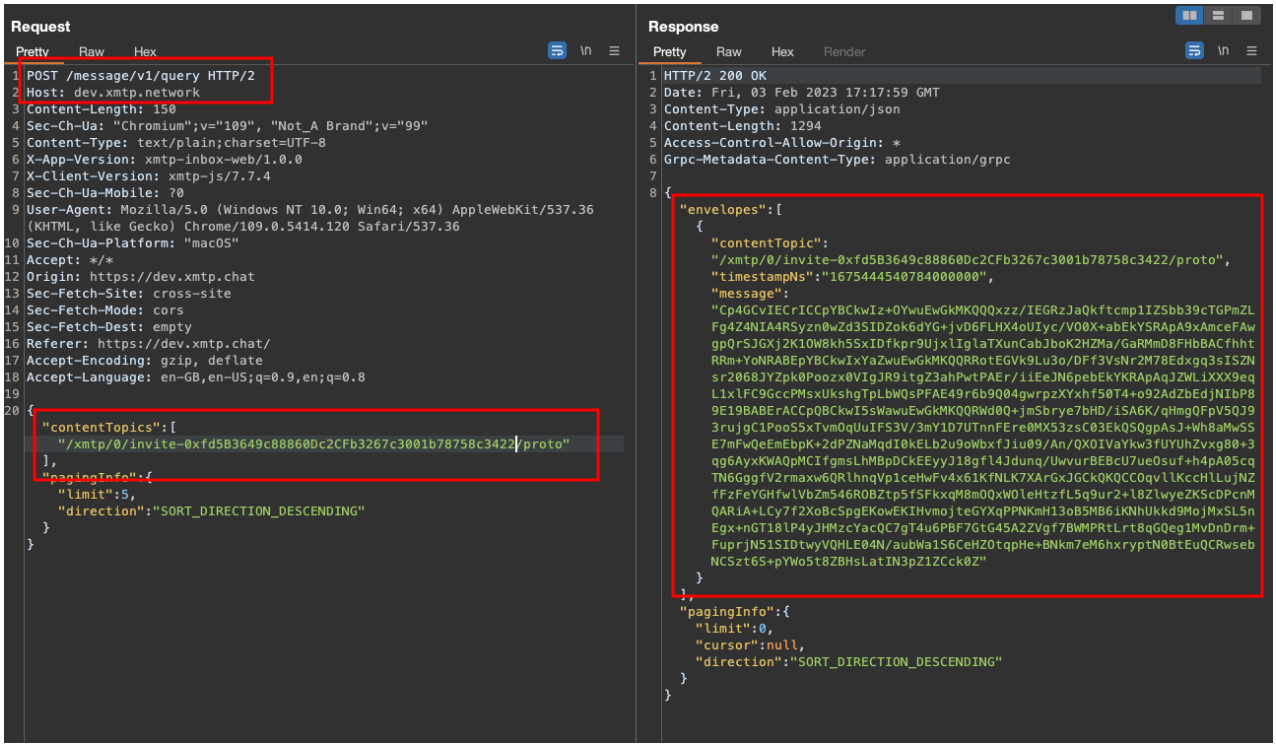
Category	Severity	Location	Status
Information Disclosure	Low		Acknowledged

Description

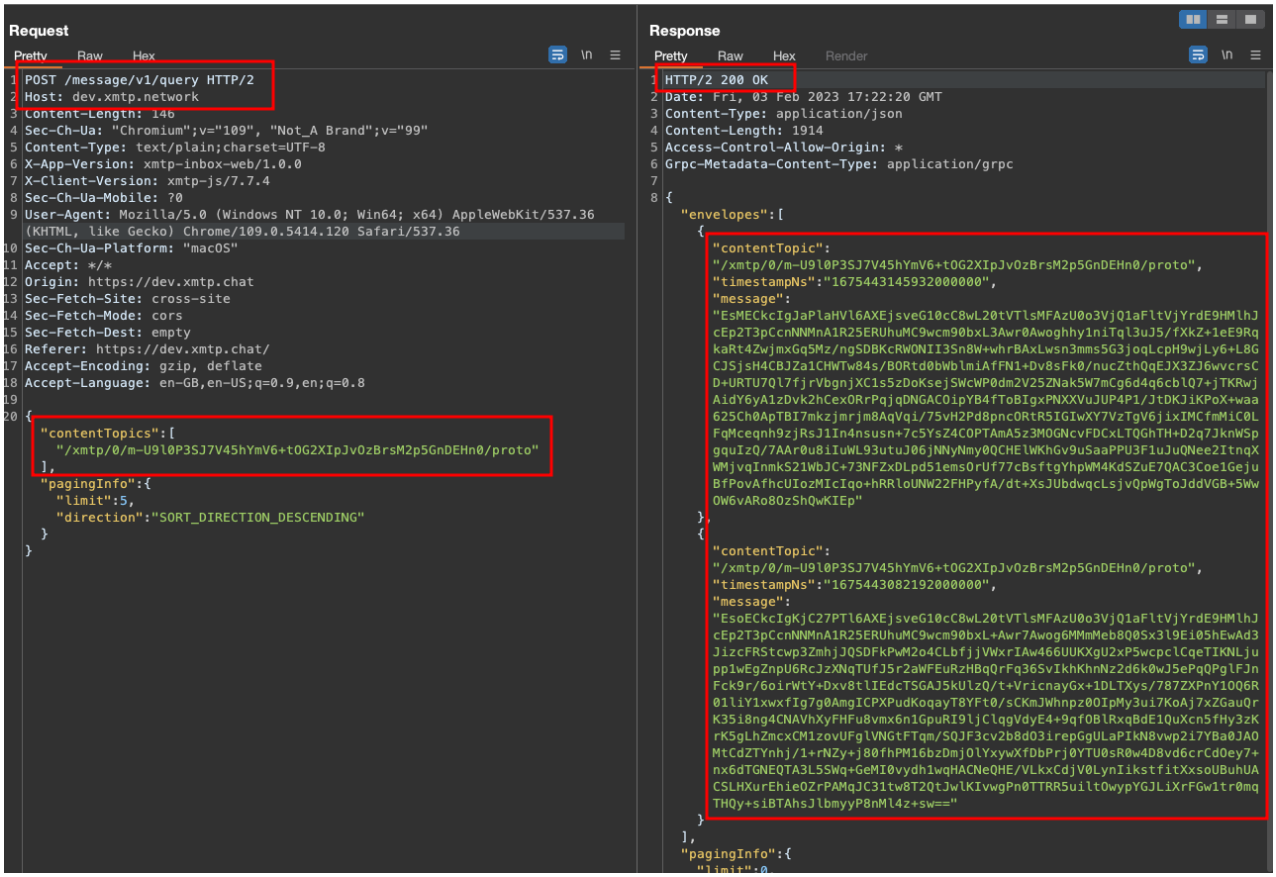
We have noted that details regarding the users' communications can be publicly accessed via API queries sent to the `/message/v1/query` endpoint. While the contents of the messages sent between 2 accounts cannot be decrypted without the private key, any user can retrieve the following interaction metadata, without requiring any Bearer access token:

- **The timestamp and encrypted data of invitations sent between 2 users** (Fig 1,2): by querying the API for invites associated with 2 accounts (`"contentTopics":["xmtp/0/invite-<ADDRESS>/proto"]`), a 3rd party can confirm if 2 accounts have previously interacted, based on the matching values for the timestamp (`timestampNs` JSON value) and the encrypted envelope (`message` JSON value).





- **(Low probability) The timestamp of the messages sent within a topic** (Fig. 3): by querying the API server for the details regarding a topic (`"contentTopic":"/xmtp/0/m-<TOPIC-ID>/proto"`), a 3rd party can observe the timestamps at which the messages have been published on the network. Therefore, an external entity can observe behavioral patterns based on the timestamps of the messages, affecting the privacy of the users interacting with the network. This case presents a low probability of exploitation, as the required topic ID is obtained from a randomly generated byte array, which is encoded in base64. Also, the topic ID is stored in the encrypted envelope of the invitation sent between the 2 accounts. Therefore, the automated enumeration of the existing topic IDs present on the network is highly inefficient.



Impact

An attacker with a list of wallets can query the server and obtain the information needed in order to determine the time of the initial contact between the addresses. Furthermore, in exceptional cases in which an attacker obtains a topic ID, the actor can retrieve the timestamps of the communicated messages.

Recommendation

The auditor would like to verify with the team whether "metadata" is considered sensitive information and whether information leakage is a threat. If so, it is recommended to encrypt the timestamps or include them within the already encrypted message.

Alleviation

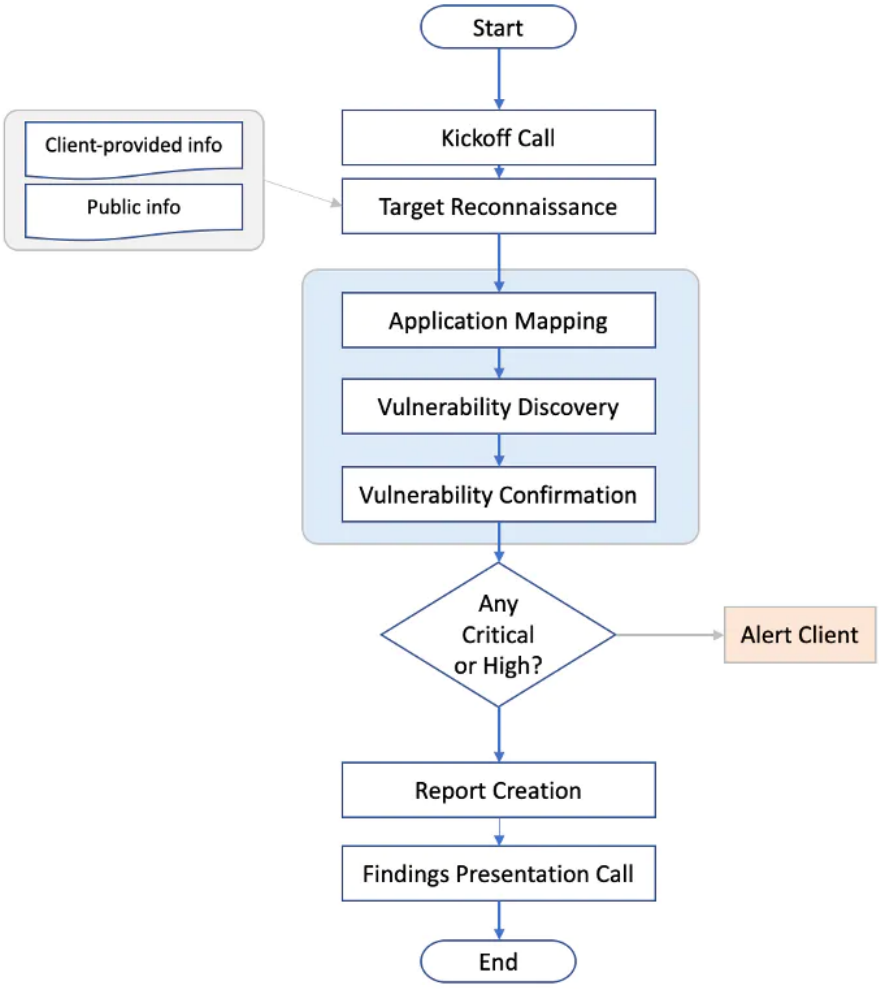
The XMTP Labs Team acknowledged the vulnerability, planning to release a patched version of the API in the future. The fix is not included in the presented testing engagement.

APPENDIX | XMTP - SECURITY ASSESSMENT

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

Web Vulnerability Classes

Class	Items
Insecure Data Storage	• Sensitive Data Store in Plain Text • Use of Public Storage • Logging Sensitive Data
Information Disclosure	• Directory Indexing • Verbose Error Messages • HTML CommentsDefault Content

Class	Items
Account Policy	• Default / Weak Passwords • Unlimited Login Attempts • Password Reset • Insufficient Session Expiration
Session Management	• Session Identifier Prediction • Session Hijacking • Cross-Site Request Forgery • Insufficient Session Expiration
Injection	• SQL Injection • Cross-Site Scripting • HTML Injection • XML Injection • OS Command Injection
Broken Access Control	• Authentication Bypass • Authorization Bypass • Privilege Escalation
Application Resource Handling	• Path Traversal • Predictable Object Identifiers • XML External Entity Expansion • Local & Remote File Inclusion
Logic Flaws	• Abuse of Functionality • Workflow Bypass
Insufficient Cryptography	• Weak Hashing Algorithms • Weak Encryption Algorithms • Hard Coded Cryptographic Key
Denial of Service	• Server-side Denial of Service • Client-side Denial of Service

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.