QuillAudits

AUDIT REPORT

January 2025

For

Dabba

Table of Content

Executive Summary

Project Name	Dabba Network
Project URL	https://dabba.com/
Overview	Dabba Inc has deployed thousands of hotspots across India at retail, residential, and commercial locations serving users with super fast, super cheap internet. Demand for data in India is roughly doubling every 18 months and Dabba is building a new data-only network for a data-hungry generation.
Audit Scope	The Scope of the Audit is to analyse the security, code quality and correctness of the DBT Minting Codebase.
Contracts in Scope	https://github.com/wifidabba/dbt-minting
Commit Hash	a60dbf07f10879da85991751a1c4447451912535
Review 1	16th January 2025 - 22th January 2025
Updated Code Received	22nd January 2025
Final Review	23rd January 2025

Number of Issues per Severity

🟥 High	0 (0%)
🟧 Medium	0 (0%)
🟩 Low	1 (100%)
🟪 Informational	0 (0%)

Severity

Issues

	🟥 High	🟧 Medium	🟩 Low	🟪 Informational
Open	0	0	0	0
Resolved	0	0	1	0
Acknowledged	0	0	0	0
Partially Resolved	0	0	0	0

Checked Vulnerabilities

- ☑ Improper Authentication
- ☑ Improper Resource Usage
- ☑ Improper Authorization
- ☑ Insecure File Uploads
- ☑ Insecure Direct Object References
- ☑ Client-Side Validation Issues
- ☑ Rate Limit
- ☑ Input Validation
- ☑ Injection Attacks
- ☑ Cross-Site Scripting (XSS)
- ☑ Cross-Site Request Forgery
- ☑ Security Misconfiguration
- ☑ Broken Access Controls
- ☑ Insecure Cryptographic Storage
- ☑ Insufficient Cryptography
- ☑ Insufficient Session Expiration
- ☑ Insufficient Transport Layer Protection
- ☑ Unvalidated Redirects and Forwards
- ☑ Information Leakage
- ☑ Broken Authentication and Session Management
- ☑ Denial of Service (DoS) Attacks
- ☑ Malware
- ☑ Third-Party Components

And More..

Techniques and Methods

Throughout the pentest of application, care was taken to ensure:

- Information gathering – Using OSINT tools information concerning the web architecture, information leakage, web service integration, and gathering other associated information related to web server & web services.
- Using Automated tools approach for Pentest like Nessus, Acunetix etc.
- Platform testing and configuration
- Error handling and data validation testing
- Encryption-related protection testing

Tools and Platforms used for Pentest:

- **Burp Suite**
- **DNSenum**
- **Dirbuster**
- **SQLMap**
- **Netcat**
- **Acunetix**
- **Neucli**
- **Nabbu**
- **Turbo Intruder**
- **Nessus**
- **Nmap**
- **Metasploit**
- **Horusec**
- **Postman**

And Many more..

Types of Severity

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

🟥 High Severity Issues

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

🟧 Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

🟩 Low Severity Issues

Low-level severity issues can cause minor impact and are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

🟪 Informational

These are four severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

These are the issues identified in the initial audit and have been successfully fixed.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/impact of the security issue, but are not completely resolved.

Low Severity Issues

1. Insecure Handling of mintAuth Private Key

Resolved

Description

The mintAuth private key, which is highly sensitive as it controls the minting of tokens, is:
Loaded into memory during the execution of mintTokens and setMintAuthorityToNull.
Cleared from memory only by assigning null, which does not securely wipe it.

Vulnerable Location

https://github.com/wifidabba/dbt-minting/blob/main/src/helpers/solana.helper.js#L57

https://github.com/wifidabba/dbt-minting/blob/main/src/helpers/solana.helper.js#L31

Recommendation

Wipe mintAuth Securely
After signing the transaction, explicitly overwrite mintAuth in memory to ensure it cannot be retrieved:

```
mintAuth.secretKey.fill(0); // Zero out sensitive data in memory
mintAuth = null;
```

Impact

Authority Hijacking: An attacker could transfer minting authority to another account, making recovery difficult or impossible.

Closing Summary

In this report, we have considered the security of the Dabba Network. We performed our audit according to the procedure described above.

One Low severity Issue was found, which the Dabba Network team has resolved.

Disclaimer

QuillAudits Pentest security audit provides services to help identify and mitigate potential security risks in Wifi Dabba. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of Wifi Dabba. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the Wifi Dabba Team to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a leading name in Web3 security, offering top-notch solutions to safeguard projects across DeFi, GameFi, NFT gaming, and all blockchain layers. With six years of expertise, we've secured over 1000 projects globally, averting over $30 billion in losses. Our specialists rigorously audit smart contracts and ensure DApp safety on major platforms like Ethereum, BSC, Arbitrum, Algorand, Tron, Polygon, Polkadot, Fantom, NEAR, Solana, and others, guaranteeing your project's security with cutting-edge practices.

QuillAudits

6+ Years of Expertise	**1M+** Lines of Code Audited
$30B+ Secured in Digital Assets	**1K+** Projects Secured

Follow Our Journey

AUDIT REPORT

January 2025

For

Dabba

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com audits@quillhash.com