QuillAudits

AUDIT REPORT

October 2025

For

MNEE

Table of Content

Executive Summary

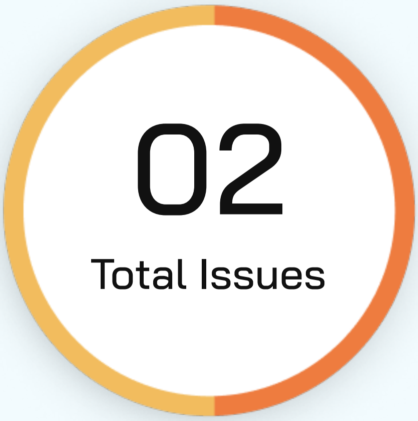
Project Name	MNEE SWAP AND BRIDGE
Protocol Type	Pentest Audit
Project URL	https://dev-swap-user.mnee.net/ https://dev-swap-user.mnee.net/bridge
Overview	MNEE Platform Overview (Bridge + Swap) The MNEE Platform is a cloud-based DeFi ecosystem designed for seamless token swaps and cross-chain bridging between Ethereum (ERC-20) and Bitcoin SV (1Sat Ordinals). It operates as a secure, scalable, and high-availability infrastructure deployed on AWS, integrating multiple blockchain and liquidity protocols to ensure smooth interoperability. The MNEE Bridge enables users to move MNEE tokens between ERC-20 and 1Sat Ordinals formats. It utilizes Fireblocks-managed treasuries on both chains, automating fund release once the source-chain tokens are received. This ensures transparent and custodial fund flow, where MNEE tokens are swapped between pools maintained by the MNEE organization, without direct smart contract dependencies. The MNEE Swap functionality allows users to perform decentralized token exchanges through integrated liquidity sources like Uniswap and Reown, facilitating efficient token conversions across supported chains. Behind the interface, the system uses a multi-layer AWS setup — with load balancers, private app servers, PostgreSQL database, and VPN-secured DevOps access — ensuring end-to-end encryption, real-time monitoring, and operational resilience. The platform architecture follows best practices for network isolation, encrypted communications (HTTPS/SSL/TLS), and role-based access control, enabling a secure, compliant, and high-performance environment for users and partners. In essence, MNEE delivers a unified platform where users can securely bridge and swap tokens between ecosystems, backed by a robust cloud infrastructure and automated treasury-managed flow for efficiency and reliability.

Review 1	12th Oct 2025 - 15th Oct 2025
Updated Code Received	19th Oct 2025
Review 2	22nd Oct 2025 - 24th Oct 2025

Verify the Authenticity of Report on QuillAudits Leaderboard:

https://www.quillaudits.com/leaderboard

Number of Issues per Severity



🟥	Critical	0(0.0%)
🟥	High	0(0.0%)
🟧	Medium	1 (50%)
🟨	Low	1 (50%)
🟪	Informational	0(0.0%)

Severity

Issues

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

Summary of Issues

Issue No.	Issue Title	Severity	Status
1	Lack of Token Address Whitelisting in Swap API Endpoint	Medium	Resolved
2	CORS Misconfiguration Allowing Requests from Unauthorized Origin Domain	Low	Resolved

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
- Client-side and business logic 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 five levels of severity, and each of them has been explained below.

Critical: Immediate and Catastrophic Impact

Critical issues are the ones that an attacker could exploit with relative ease, potentially leading to an immediate and complete loss of user funds, a total takeover of the protocol's functionality, or other catastrophic failures. Critical vulnerabilities are non-negotiable; they absolutely must be fixed.

High (H): Significant Risk of Major Loss or Compromise

High-severity issues represent serious weaknesses that could result in significant financial losses for users, major malfunctions within the protocol, or substantial compromise of its intended operations. While exploiting these vulnerabilities might require specific conditions to be met or a moderate level of technical skill, the potential damage is considerable. These findings are critical and should be addressed and resolved thoroughly before the contract is put into the Mainnet.

Medium (M): Potential for Moderate Harm Under Specific Circumstances

Medium-severity bugs are loopholes in the protocol that could lead to moderate financial losses or partial disruptions of the protocol's intended behavior. However, exploiting these vulnerabilities typically requires more specific and less common conditions to occur, and the overall impact is generally lower compared to high or critical issues. While not as immediately threatening, it's still highly recommended to address these findings to enhance the contract's robustness and prevent potential problems down the line.

Low (L): Minor Imperfections with Limited Repercussions

Low-severity issues are essentially minor imperfections in the smart contract that have a limited impact on user funds or the core functionality of the protocol. Exploiting these would usually require very specific and unlikely scenarios and would yield minimal gain for an attacker. While these findings don't pose an immediate threat, addressing them when feasible can contribute to a more polished and well-maintained codebase.

Informational (I): Opportunities for Improvement, Not Immediate Risks

Informational findings aren't security vulnerabilities in the traditional sense. Instead, they highlight areas related to the clarity and efficiency of the code, gas optimization, the quality of documentation, or adherence to best development practices. These findings don't represent any immediate risk to the security or functionality of the contract but offer valuable insights for improving its overall quality and maintainability. Addressing these is optional but often beneficial for long-term health and clarity.

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.

Severity Matrix

Impact

		🟥 High	🟧 Medium	🟨 Low
Likelihood	🟥 High	Critical	High	Medium
	🟧 Medium	High	Medium	Low
	🟨 Low	Medium	Low	Low

Impact

- **High** - leads to a significant material loss of assets in the protocol or significantly harms a group of users.
- **Medium** - only a small amount of funds can be lost (such as leakage of value) or a core functionality of the protocol is affected.
- **Low** - can lead to any kind of unexpected behavior with some of the protocol's functionalities that's not so critical.

Likelihood

- High - attack path is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount of funds that can be stolen or lost.
- Medium - only a conditionally incentivized attack vector, but still relatively likely.
- Low - has too many or too unlikely assumptions or requires a significant stake by the attacker with little or no incentive.

Medium Severity Issues

Lack of Token Address Whitelisting in Swap API Endpoint

Resolved

Description

A security vulnerability has been identified in the token swap API endpoint at dev-quote-api.mnee.net. The /api/route endpoint accepts user-supplied token addresses for both input (tokenInAddress) and output (tokenOutAddress) parameters without implementing proper whitelist validation. This allows any Ethereum contract address to be specified as a tradeable token, bypassing any intended restrictions on which tokens should be available for swapping through the platform.The endpoint processes swap quote requests for arbitrary ERC-20 token pairs without verifying that the tokens are authorized or supported by the platform. This lack of input validation creates an unrestricted token swap interface that could be exploited for various malicious purposes.

Vulnerable Request/URL

Endpoint: GET /api/route
Host: dev-quote-api.mnee.net

Full Request:

```
GET /api/route?
tokenInAddress=0xdAC17F958D2ee523a2206206994597C13D831ec7&tokenOutAddress=0x8ccedbAe491
6b79da7F3F612EfB2EB93A2bFD6cF&amountIn=10&slippageTolerance=10&deadlineMinutes=1&recipient=
0x435f6c48D57E52Ac47259c856bB8940b94103c94&chainId=1 HTTP/2
```

Vulnerable Parameters:
tokenInAddress - No validation implemented
tokenOutAddress - No validation implemented

Impact

The lack of token address validation exposes the platform and its users to multiple security and operational risks

Recommendation

Implement Token Whitelisting for tokenin and tokenout for only the tokens you want them to select from!

Low Severity Issues

CORS Misconfiguration Allowing Requests from Unauthorized Origin Domain

Resolved

Description

The API endpoint /api/uniswap/save/swap/transaction has a critical CORS (Cross-Origin Resource Sharing) misconfiguration that allows cross-origin requests from an unauthorized domain. The server is accepting and processing requests from https://dev-swap-user.m1nee.net, which appears to be either a typo domain or a potentially malicious origin, when the legitimate application domain is https://dev-swap-user.mnee.net.

The server's CORS policy is incorrectly configured to allow the unauthorized origin:
Legitimate Origin: https://dev-swap-user.mnee.net
Unauthorized Origin Allowed: https://dev-swap-user.m1nee.net (note the “m1” vs “m”)

Vulnerable Request/URL

Endpoint: POST /api/uniswap/save/swap/transaction
Host: dev-swap-api.mnee.net

Impact

- Data Exfiltration
- Compliance and Legal Risks

Recommendation

Validate Origin on Every Request
Strict Origin Whitelist Backend Configuration

Note

The MNEE bridge relies on Fireblocks APIs to facilitate treasury operations and automate token transfers between the ERC-20 and 1Sat Ordinals pools. While this integration streamlines fund movement and enhances operational efficiency, it introduces a dependency and centralization risk. Specifically, any downtime, API malfunction, or custodial control issue within Fireblocks can disrupt the bridge's fund flow, halt bridging operations, or expose users to counterparty and operational risks.

As Fireblocks serves as a centralized intermediary in this architecture, the bridge's functionality and asset custody remain partially dependent on a third-party service, which may conflict with the decentralized principles of cross-chain interoperability.

Closing Summary

In this report, we have considered the security of the MNEE Swap and Bridge. We performed our audit according to the procedure described above.

Some issues of medium and low severity were found. The MNEE team resolved all the issues mentioned.

Disclaimer

At QuillAudits, we have spent years helping projects strengthen their smart contract security. However, security is not a one-time event threats evolve, and so do attack vectors. Our audit provides a security assessment based on the best industry practices at the time of review, identifying known vulnerabilities in the received smart contract source code.

This report does not serve as a security guarantee, investment advice, or an endorsement of any platform. It reflects our findings based on the provided code at the time of analysis and may no longer be relevant after any modifications. The presence of an audit does not imply that the contract is free of vulnerabilities or fully secure.

While we have conducted a thorough review, security is an ongoing process. We strongly recommend multiple independent audits, continuous monitoring, and a public bug bounty program to enhance resilience against emerging threats.

Stay proactive. Stay secure.

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 seven years of expertise, we've secured over 1400 projects globally, averting over $3 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

7+ Years of Expertise	**1M+** Lines of Code Audited
50+ Chains Supported	**1400+** Projects Secured

Follow Our Journey

AUDIT REPORT

October 2025

For

MNEE

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com audits@quillaudits.com