



Smart Contract Security Audit

Project: MEME Exchange

Oct 04, 2023



Contract Address

0x3611a05ed89c751e0F9eFa931b3B64da7A81464e

Table of Contents

1 Disclaimer

2 Audit Review

3 Project Review

4 Smart Contract Vulnerability Checks

5 Manual Code Review

6 Owner Privileges

6.1 Contract Ownership

6.2 Liquidity Overview

7 Tokenomics

8 Social Media Check

9 Website Review

10 Audit Conclusion

Disclaimer

The contents of this report reflect only the CRACKEN TECH audit team's understanding of the current progress and status of the security of the code audited, to verify the integrity of the code provided for the scope of this audit. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit are recommended after the issues covered are fixed. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report.

The review does not address the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from off-chain sources are not extended by this review either.

Audit Review

The source code of the MEME EXCHANGE Token was audited in order to acquire a clear impression of how the project was implemented. The Cracken Tech audit team conducted in-depth research, analysis, and scrutiny, resulting in a series of observations. A detailed list of each issue found, and vulnerabilities in the source code will be included in the audit report. The problems and potential solutions are given in this report, we will identify common sources for such problems and comments for improvement.

The auditing process will follow a routine as special considerations by Cracken:

- Review of the specifications, sources, and instructions provided to Cracken to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Cracken describe.
- Test coverage analysis determines whether the test cases cover the code and how much code is exercised when we run the test cases.
- Symbolic execution is analyzing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

Project Review

Token Summary

Parameter	Result
Token Name	MEME EXCHANGE
Token Symbol	MEME
Token Decimal	18
Total Supply	800,000,000,000
Platform	PEGO
Buy Tax Fee	0%
Sell Tax Fee	0%
Contract Creation Date	September-23-2023 03:08:22 PM +8 UTC
Liquidity Status	Unlocked
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200
Contract Address	<u>0x3611a05ed89c751e0f9efa931b3b64da7a81464e</u>
Deployer Address	0x3735adf84c569A7e5Ccae3aF45d51d887a2a8b2F
Owner Address	0x3735adf84c569a7e5ccae3af45d51d887a2a8b2f

Source Code

CRACKEN was commissioned by MEME EXCHANGE to perform an audit based on the following smart contract:

<https://scan.pegonetwork/address/0x3611a05ed89c751e0f9efa931b3B64da7A81464e>





Smart Contract Vulnerability Checks

Vulnerability	Auto-Scan	Manual-Scan	Result
Unencrypted Private Data On-chain	Completed	Completed	Low/No Risk
Code With No Effects	Completed	Completed	Low/No Risk
Message call with hardcoded gas amount	Completed	Completed	Low/No Risk
Unexpected Ether balanced	Completed	Completed	Low/No Risk
Right-To-Left-Override control character (U+202E)	Completed	Completed	Low/No Risk
Typographical Error	Completed	Completed	Low/No Risk
DoS With Block Gas Limit	Completed	Completed	Low/No Risk
Arbitrary Jump with Function Type Variable	Completed	Completed	Low/No Risk
Insufficient Gas Grieving	Completed	Completed	Low/No Risk
Incorrect Inheritance Order	Completed	Completed	Low/No Risk
Write to Arbitrary Storage Location	Completed	Completed	Low/No Risk
Requirement Violation	Completed	Completed	Low/No Risk
Missing Protection against Signature Replay Attacks	Completed	Completed	Low/No Risk
Weak Sources of Randomness from Chain Attributes	Completed	Completed	Low/No Risk
Authorization through tx.origin	Completed	Completed	Low/No Risk
Delegate call to Untrusted Callee	Completed	Completed	Low/No Risk





Vulnerability	Auto-Scan	Manual-Scan	Result
Use of Deprecated Solidity Functions	Completed	Completed	Low/No Risk
Assert Violation	Completed	Completed	Low/No Risk
Reentrancy	Completed	Completed	Low/No Risk
Unprotected SELF-DESTRUCT Instruction	Completed	Completed	Low/No Risk
Unprotected Ether Withdrawal	Completed	Completed	Low/No Risk
Outdated Compiler Version	Completed	Completed	Low/No Risk
Integer Overflow and Underflow	Completed	Completed	Low/No Risk
Function Default Visibility	Completed	Completed	Low/No Risk

Manual Code Review

Classification of Issues

Severity	Description
 High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
 Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
 Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
 Informational	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
 High-Risk	0
 Medium-Risk	0
 Low-Risk	0
 Informational	0

Privileged Functions onlyOwner

Function Name	Parameters	Visibility
approve	address spender, unit256 amount	External
burn	address account, unit256 amount	Internal
decreaseAllowance	address spender, unit256 subtractedValue	Public
renounceOwnership	None	Public
rescueETH	None	External
rescueToken	address tokenAddress, unit256 tokens	Public
setAddrParam	address _ecologBuildAddr, address _ecologDevelopAddr	External
setBlackList	address account, bool isBlack	Public
setClubAddr	address _clubAddr	Public
setExcludeFromFees	address account, bool excluded	Public
setIsOpenSwap	bool _isOpenSwap	Public
transfer	address to, unit256 amount	External
transferFrom	address from, address to, unit256 amount	External
transferOwnership	address newOwner	Public

Contract Ownership

The contract ownership of MEME EXCHANGE is not renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is [the address 0x3735adf84c569A7e5Ccae3aF45d51d887a2a8b2F](#) which can be viewed: [HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions list above, if the owner's wallet is compromised these privileges could be exploited.

We recommend the team renounce ownership at the right time if possible, or gradually migrate to a time lock with governing functionalities in respect of transparency and safety considerations.

Liquidity Overview

Liquidity Information

The token does not have liquidity at the moment of the audit

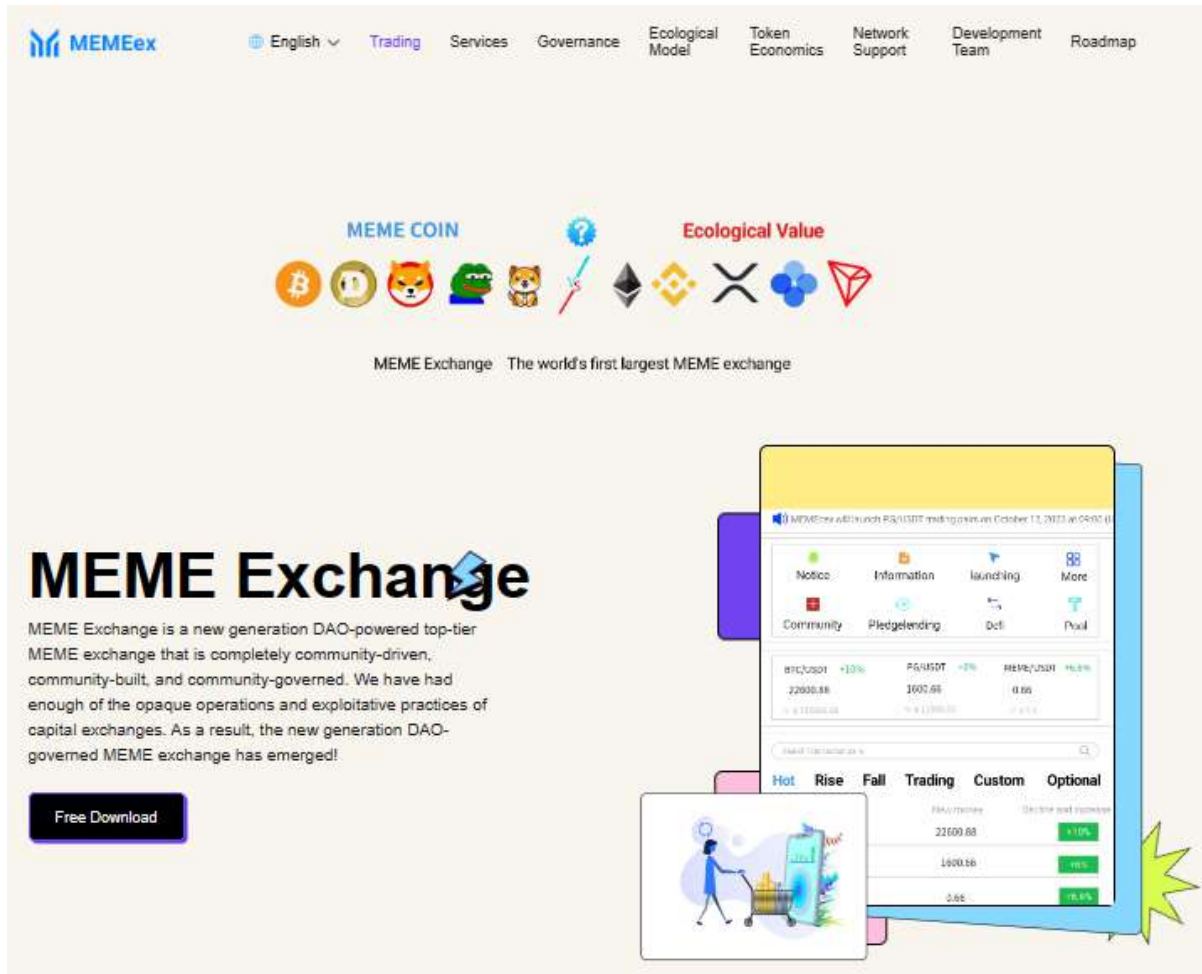
Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x3735adf84c569A7e5Ccae3aF45d51d887a2a8b2F	800,000,000,000	100.00%

Social Media Check

Social Media Type	Link	Result
Website	https://www.bimeme.com	Checked
Twitter	https://twitter.com/MEMEcex	Checked

Website Review



MEME COIN

Ecological Value

MEME Exchange The world's first largest MEME exchange

MEME Exchange

MEME Exchange is a new generation DAO-powered top-tier MEME exchange that is completely community-driven, community-built, and community-governed. We have had enough of the opaque operations and exploitative practices of capital exchanges. As a result, the new generation DAO-governed MEME exchange has emerged!

[Free Download](#)

MEMEex will launch PS/USDT trading pair on October 11, 2023 at 05:00 UTC

Notice Information launching More

Community Pledgeling Defi Pool

Pair	Price	24h Change
BTC/USDT	22600.88	+10%
PS/USDT	1600.88	+2%
MEME/USDT	0.06	+6.5%

Hot Rise Fall Trading Custom Optional

24h Volume: 22600.88 +10%

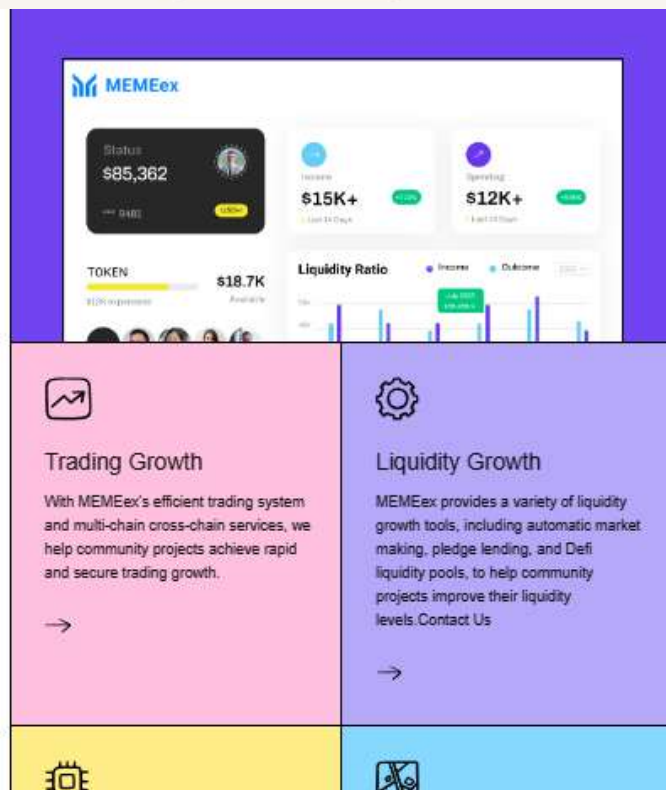
1600.88 +2%

0.06 +6.5%

MEME Services

We provide a comprehensive and transparent governance platform that offers trading growth, liquidity growth, token ecosystem creation, and community development assistance for all top-tier community projects.

No longer serving money, no longer serving relationships, no longer serving exploiters. We will always serve the community, always serve the users, always serve decentralization.



MEMEex

Status: \$85,362

Income: \$15K+

Operating: \$12K+

TOKEN: \$18.7K

Liquidity Ratio

Trading Growth

With MEMEex's efficient trading system and multi-chain cross-chain services, we help community projects achieve rapid and secure trading growth.

[→](#)

Liquidity Growth

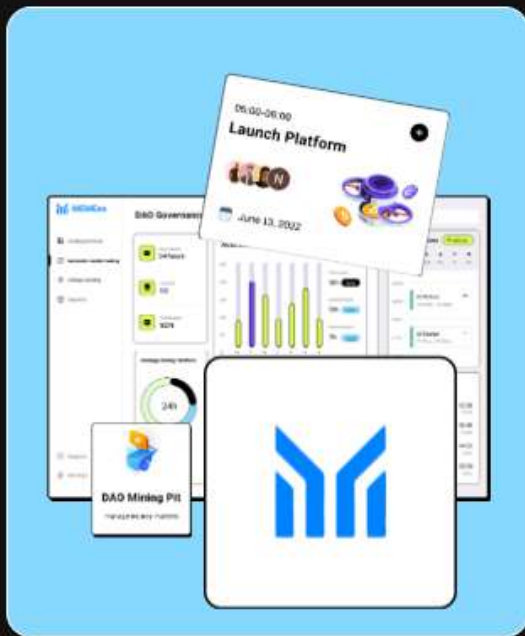
MEMEex provides a variety of liquidity growth tools, including automatic market making, pledge lending, and Defi liquidity pools, to help community projects improve their liquidity levels. Contact Us

[→](#)

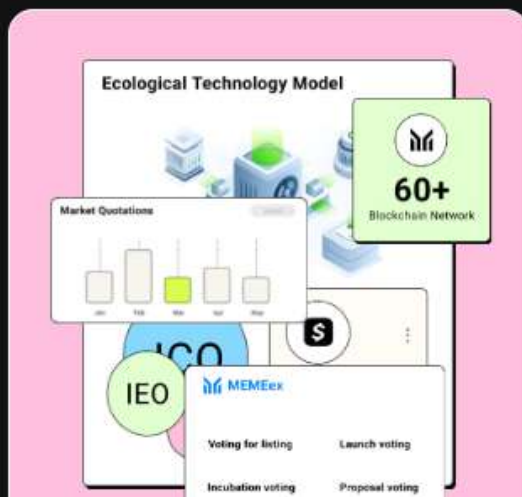
Website Review

DAO Governance Services

MEMEex provides a series of DAO governance services for all top MEME projects and communities, including DAO listing services, DAO launch services, ICO seed financing, IDO public financing, IEO listing financing, financial information, DAO mining pools, ecological community governance, pledge lending, liquidity pool creation governance, wealth management, encrypted transactions, automatic market making, 80+ cross chain services, and custom token quotes



MEME Exchange Ecological Technology Model



✓ Cryptographic token trading, automatic market making

✓ DAO open pit function

✓ Free and open pledge lending

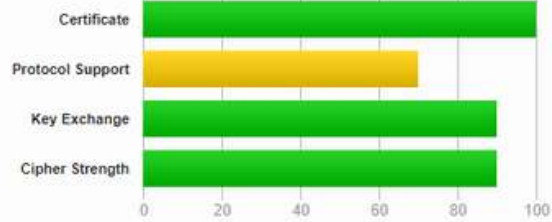
✓ Open self-service lottery pool

✓ Defi liquidity pool, transaction finance

✓ Creation and management of financing functions such as DAO launch pad, ICO, IDO, IEO, etc

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server's certificate chain is incomplete. Grade capped to B.

This server supports TLS 1.1. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA384withRSA)



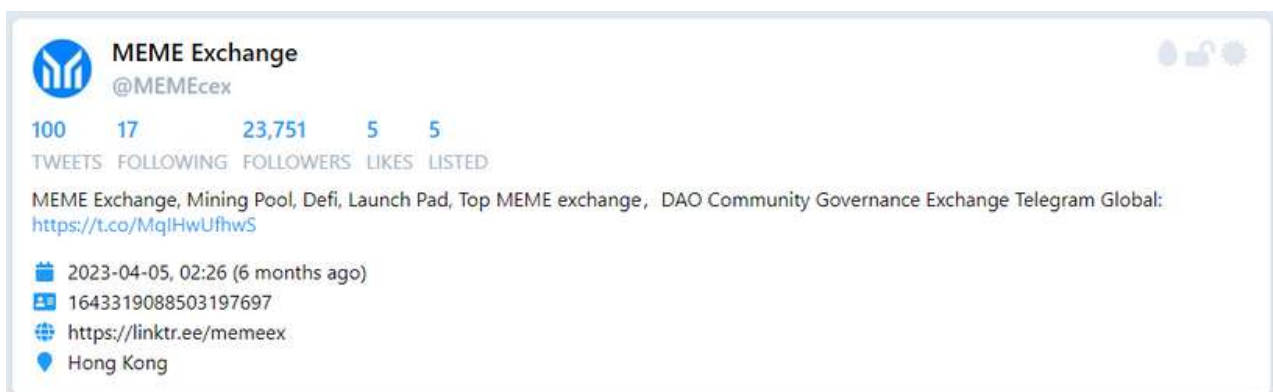
Server Key and Certificate #1



Subject	bimeme.com Fingerprint: SHA256: 0035f5a8b201125bba78b650d50b33ca7ef2a7ebc368bac57ddd0679e347fe Pin: SHA256: LCuGXtxRja1IRKOCJKQskQudPMwRyMSz6rNT6LAH44Ndk=
Common names	bimeme.com
Alternative names	bimeme.com www.bimeme.com
Serial Number	6e8cc98d4ebd8f116403d870ef12dee
Valid from	Fri, 25 Aug 2023 00:00:00 UTC
Valid until	Thu, 23 Nov 2023 23:59:59 UTC (expires in 1 month and 20 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	ZeroSSL RSA Domain Secure Site CA Alt: http://zerossl.crl.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crl
Signature algorithm	SHA384withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://zerossl.ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

- Mobile Friendly
- Contains no code errors
- SSL is secured
- No spelling errors

Twitter Review



- No suspicious activities or events
- No suspicious IP activities.

Audit Conclusion

- The owner cannot pause trading
- The owner cannot mint new token
- The owner cannot blacklist users
- The owner cannot change the max tx amount
- The owner cannot change buy/sell fees up
- The owner can set whitelist wallets.
- The ownership is yet to be renounced.

AUDIT IS PASSED