



SMART CONTRACT AUDIT



interfinetwork



hello@interfi.network



<https://interfi.network>

PREPARED FOR

GODMODE TOKEN



INTRODUCTION

| | |
|----------------|---|
| Auditing Firm | InterFi Network |
| Client Firm | GodMode Token |
| Methodology | Automated Analysis, Manual Code Review |
| Language | Solidity |
| | |
| Contract | 0x2063516bA30D69F9075854A9F57d9c29f0C61b59 |
| Blockchain | Ethereum |
| Centralization | Ownership Renounced |
| Commit | d55a6219ec62aa54c291a28d667b64f99456ae42 |
| | |
| Website | http://godmodetoken.io/ |
| Telegram | https://t.me/Godmodetoken_eth/ |
| X (Twitter) | https://x.com/GodMode_eth/ |
| Report Date | May 18, 2024 |

 Verify the authenticity of this report on our website: <https://www.github.com/interfinetwork>



EXECUTIVE SUMMARY

InterFi has performed the automated and manual analysis of solidity codes. Solidity codes were reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

| Status | Critical ● | Major ● | Medium ● | Minor ● | Unknown ● |
|--------------|---|---|--|--|--|
| Open | 0 | 0 | 0 | 0 | 0 |
| Acknowledged | 0 | 0 | 1 | 3 | 1 |
| Resolved | 0 | 0 | 1 | 1 | 0 |

 Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

 Please note that centralization privileges regardless of their inherited risk status – constitute an elevated impact on smart contract safety and security.



TABLE OF CONTENTS

| | |
|-----------------------------|----|
| TABLE OF CONTENTS | 4 |
| SCOPE OF WORK..... | 5 |
| AUDIT METHODOLOGY | 6 |
| RISK CATEGORIES | 8 |
| AUTOMATED ANALYSIS..... | 9 |
| INHERITANCE GRAPH..... | 10 |
| MANUAL REVIEW..... | 11 |
| DISCLAIMERS..... | 19 |
| ABOUT INTERFI NETWORK | 22 |

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL



SCOPE OF WORK

InterFi was consulted by GodMode Token to conduct the smart contract audit of their solidity source codes. The audit scope of work is strictly limited to mentioned solidity file(s) only:

- GodMode.sol

 If source codes are not deployed on the main net, they can be modified or altered before main-net deployment. Verify the contract's deployment status below:

| | |
|---|---------|
| Public Contract Link | |
| https://etherscan.io/token/0x2063516ba30d69f9075854a9f57d9c29f0c61b59#code | |
| | |
| Contract Name | GodMode |
| Compiler Version | 0.8.20 |
| License | MIT |



AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of InterFi's auditing process and methodology:

CONNECT

- The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.

AUDIT

- Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:
 - Remix IDE Developer Tool
 - Open Zeppelin Code Analyzer
 - SWC Vulnerabilities Registry
 - DEX Dependencies, e.g., Pancakeswap, Uniswap
- Simulations are performed to identify centralized exploits causing contract and/or trade locks.
- A manual line-by-line analysis is performed to identify contract issues and centralized privileges.

We may inspect below mentioned common contract vulnerabilities, and centralized exploits:

| | |
|----------------------|---|
| Centralized Exploits | <ul style="list-style-type: none">○ Token Supply Manipulation○ Access Control and Authorization○ Assets Manipulation○ Ownership Control○ Liquidity Access○ Stop and Pause Trading○ Ownable Library Verification |
|----------------------|---|



Common Contract Vulnerabilities

- Integer Overflow
- Lack of Arbitrary limits
- Incorrect Inheritance Order
- Typographical Errors
- Requirement Violation
- Gas Optimization
- Coding Style Violations
- Re-entrancy
- Third-Party Dependencies
- Potential Sandwich Attacks
- Irrelevant Codes
- Divide before multiply
- Conformance to Solidity Naming Guides
- Compiler Specific Warnings
- Language Specific Warnings

REPORT

- The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.
- The client's development team reviews the report and makes amendments to solidity codes.
- The auditing team provides the final comprehensive report with open and unresolved issues.

PUBLISH






- The client may use the audit report internally or disclose it publicly.

 It is important to note that there is no pass or fail in the audit, it is recommended to view the audit as an unbiased assessment of the safety of solidity codes.



RISK CATEGORIES

A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized:






| Risk Type | Definition |
|---|--|
| Critical  | These risks pose immediate and severe threats, such as asset theft, data manipulation, or complete loss of contract functionality. They are often easy to exploit and can lead to significant, irreparable damage. Immediate fix is required. |
| Major  | These risks can significantly impact code performance and security, and they may indirectly lead to asset theft and data loss. They can allow unauthorized access or manipulation of sensitive functions if exploited. Fixing these risks are important. |
| Medium  | These risks may create attack vectors under certain conditions. They may enable minor unauthorized actions or lead to inefficiencies that can be exploited indirectly to escalate privileges or impact functionality over time. |
| Minor  | These risks may include inefficiencies, lack of optimizations, code-style violations. These should be addressed to enhance overall code quality and maintainability. |
| Unknown  | These risks pose uncertain severity to the contract or those who interact with it. Immediate fix is required to mitigate risk uncertainty. |



All statuses which are identified in the audit report are categorized here:

| Status Type | Definition |
|--------------|--|
| Open | Risks are open. |
| Acknowledged | Risks are acknowledged, but not fixed. |
| Resolved | Risks are acknowledged and fixed. |



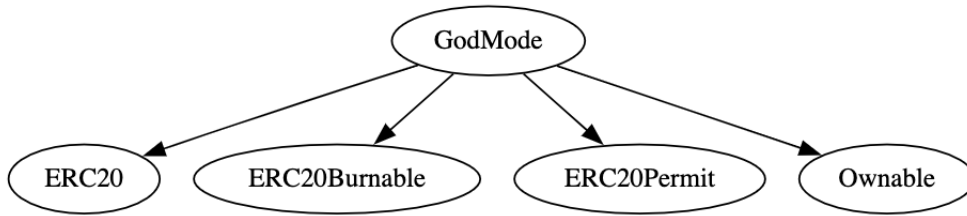
AUTOMATED ANALYSIS

| Symbol | Definition |
|---|-------------------------|
|  | Function modifies state |
|  | Function is payable |
|  | Function is internal |
|  | Function is private |
|  | Function is important |

```
| **GodMode** | Implementation | ERC20, ERC20Burnable, ERC20Permit, Ownable |||  
| L | <Constructor> | Public  |  | ERC20 ERC20Permit Ownable |
```

TERFI
CONFIDENTIALINTERFI
CONFIDENTIAL

INHERITANCE GRAPH



INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL



MANUAL REVIEW

| Identifier | Definition | Severity |
|------------|------------------------|----------|
| CEN-01 | Centralized privileges | Medium ● |

Important onLy0wner centralized privileges are listed below:

```
renounce0wnership()  
transfer0wnership()
```

RECOMMENDATION

Deployers', owners', and all other privileged roles' private-keys/access-keys/admin-keys should be secured carefully. These entities can have a single point of failure that compromises the security of the project. Manage centralized and privileged roles carefully.

- Consider using multi-signature wallets. Multi-sig wallet requires multiple parties to agree on transactions before execution, reducing the risk that a single compromised account could perform unauthorized actions.
- Time-lock sensitive functions: Introduce time-locks for critical functions so that any changes have a mandatory delay period during which users can review and react to proposed actions.

RESOLUTION

GodMode token team has renounced smart contract ownership.



| Identifier | Definition | Severity |
|------------|-------------------------|----------|
| LOG-02 | Potential front-running | Medium 🟡 |

Potential front-running also classified as – sandwich attack happens when an attacker observes a transaction swapping tokens or adding liquidity without setting restrictions on slippage or minimum output amount. The attacker can manipulate the exchange rate by front-running a transaction to purchase assets and make profits by back-running a transaction to sell assets. Standard ERC20 transfer and approve functions can be front-run. For example, if a user is trying to approve a spender for a certain amount, a front-runner could see this and try to transfer tokens from the user if they already have an allowance.

RECOMMENDATION

Use commit-reveal scheme or private transactions.

ACKNOWLEDGEMENT

GodMode token team argued that front-running is a known concern in blockchain environments, particularly on public blockchains like Ethereum. There's no one full-proof way to deter front-runners.



| Identifier | Definition | Severity |
|------------|--|---|
| COD-02 | Timestamp manipulation via <code>block.timestamp</code> and <code>block.chainid</code> | Minor  |

Be aware that the timestamp of the block can be manipulated by a miner. When the contract uses the timestamp to seed a random number, the miner can actually post a timestamp within 15 seconds of the block being validated, effectively allowing the miner to precompute an option more favorable to their chances.

`permit()`

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL

RECOMMENDATION

To maintain block integrity, follow 15 seconds rule, and scale time dependent events accordingly.

ACKNOWLEDGEMENT

GodMode project uses widely accepted *OpenZeppelin* imports in smart contract.



| Identifier | Definition |
|------------|-----------------------------------|
| COD-09 | Lack of contract balance withdraw |

Smart contract may collect tokens, and ethers from external addresses. Add `withdraw()` function to take out tokens and ethers from the contract.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL



| Identifier | Definition | Severity |
|------------|----------------------------------|-----------|
| COD-10 | Direct and indirect dependencies | Unknown 🟤 |

Smart contract is interacting with third party protocols e.g., DEX routers, external contracts, web3 applications, *OpenZeppelin* upgradeable and ERC20 libraries. The scope of the audit treats these entities as black boxes and assumes their functional correctness. However, in the real world, all of them can be compromised, and exploited. Moreover, upgrades in these entities can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT


RECOMMENDATION

Inspect third party dependencies regularly, and mitigate severe impacts whenever necessary.

ACKNOWLEDGEMENT

GodMode token team will inspect third party dependencies regularly, and push updates as required.



| Identifier | Definition | Severity |
|------------|----------------------------------|---|
| COD-11 | Possible signature replay attack | Minor  |

permit() function follows the EIP-2612 standard which is good as it allows for gasless transactions, however **ECDSA** must be implemented properly prevent possible signature replay attacks.


INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL

COMMENT

Checks are set in permit() function to validate signature.

```
address signer = ECDSA.recover(hash, v, r, s);  
if (signer != owner) {  
    revert ERC2612InvalidSigner(signer, owner);  
}
```



| Identifier | Definition | Severity |
|------------|---|---|
| COD-12 | Note regarding keccak256 secure hashing | Minor  |

Note that the keccak256 function is not collision-resistant, and therefore there is a possibility of two different messages producing the same hash. Generating strong random input data, and properly securing and managing keys is recommended for fortification of keccak256.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT

COMMENT

GodMode token team comments that the keccak256 collision has little effect on the functionality as it's related to signed data, except for the storage layout that can be solved by creating test files to check storage slot collisions. keccak256 function is widely adapted in cryptography, and its use is relatively safe.



| Identifier | Definition | Severity |
|------------|----------------------------|----------|
| COM-01 | Floating pragma | Minor ● |
| COM-02 | Multiple pragma directives | |

Compiler is set to ^0.8.20

TERFI
CONFIDENTIALINTERFI
CONFIDENTIAL

RECOMMENDATION

Pragma should be fixed to the version that you're indenting to deploy your contracts with.

RESOLUTION

GodMode token smart contract is deployed using stable compiler.



DISCLAIMERS

InterFi Network provides the easy-to-understand audit of solidity source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. 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. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way



to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, 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, INTERFI NETWORK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, INTERFI NETWORK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, INTERFI NETWORK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT'S OR ANY OTHER INDIVIDUAL'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.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. InterFi Network does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.



LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than InterFi Network. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites' and social accounts' owners. You agree that InterFi Network is not responsible for the content or operation of such websites and social accounts and that InterFi Network shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.

INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI INTERFI
CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL AUDIT REPORT CONFIDENTIAL



ABOUT INTERFI NETWORK

InterFi Network provides intelligent blockchain solutions. We provide solidity development, testing, and auditing services. We have developed 150+ solidity codes, audited 1000+ smart contracts, and analyzed 500,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Velas, Oasis, etc.

InterFi Network is built by engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 4 core members, and 6+ casual contributors.

Website: <https://interfi.network>

Email: hello@interfi.network

GitHub: <https://github.com/interfinetwork>

Telegram (Engineering): <https://t.me/interfiaudits>

Telegram (Onboarding): <https://t.me/interfisupport>



 interfinetwork

 hello@interfi.network

 <https://interfi.network>

SMART CONTRACT AUDITS | SOLIDITY DEVELOPMENT AND TESTING
RELENTLESSLY SECURING PUBLIC AND PRIVATE BLOCKCHAINS