ITISH

Audit Details

Audited project

Endless Burn TOKEN

Deployer address

0x56a8870768260180faf146d91e332643326b1b13

Client contacts:

Endless Burn TOKEN Team

Blockchain

Binance Smart Chain

Project website:

Not Provided By Endless Burn TOKEN Team

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Itish and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Itish) owe no duty of care towards you or any other person, nor does Itish make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Itish hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Itish hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Itish, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

Itish was commissioned by Endless Burn TOKEN to perform an audit of smart contracts:

https://bscscan.com/token/0x56a8870768260180faf146d91e332643326b1b13

The purpose of the audit was to achieve the following:

- **Ensure that the smart contract functions as intended.**
- **Identify potential security issues with the smart contract.**

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

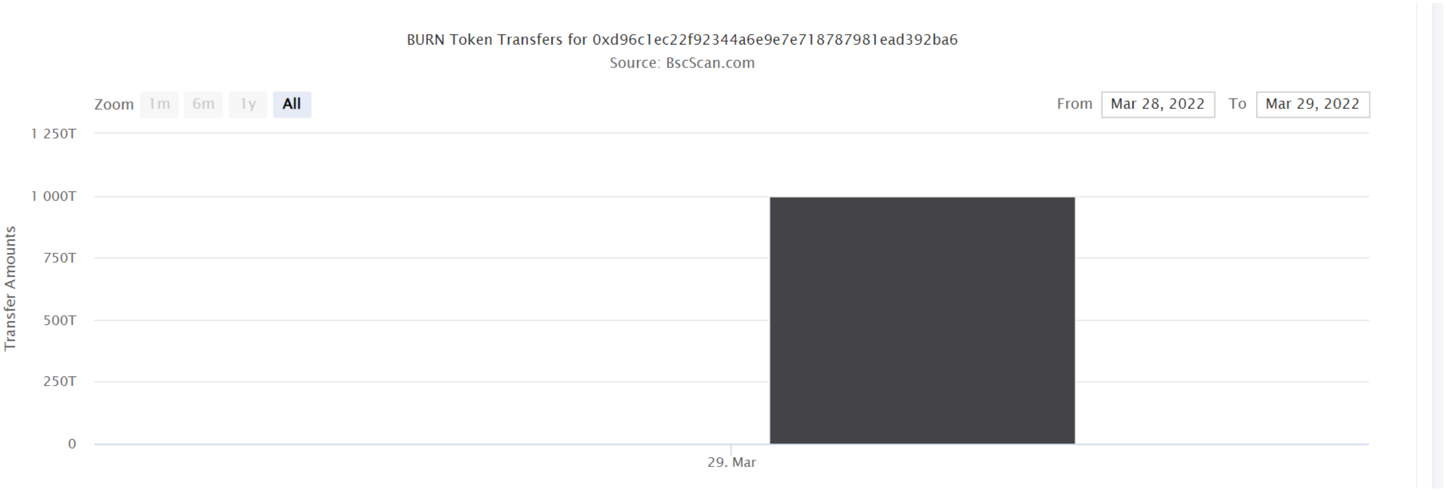
Contracts Details

Token contract details for 24.04.2022

Contract name	Endless Burn TOKEN
Contract address	0x56a88707682601 80faf146d91e332643326b1b13
Total supply	1,000,000,000,000,000
Token	Burn
Decimal Endless Burn	18
Token holders	1
Transactions count	4
Top 100 holders dominance	100.00%

Token Creator 0x0ac6f46afc05b06a5ce4a799336c8caad62cd92794eb4ccdec586aff794eabd7

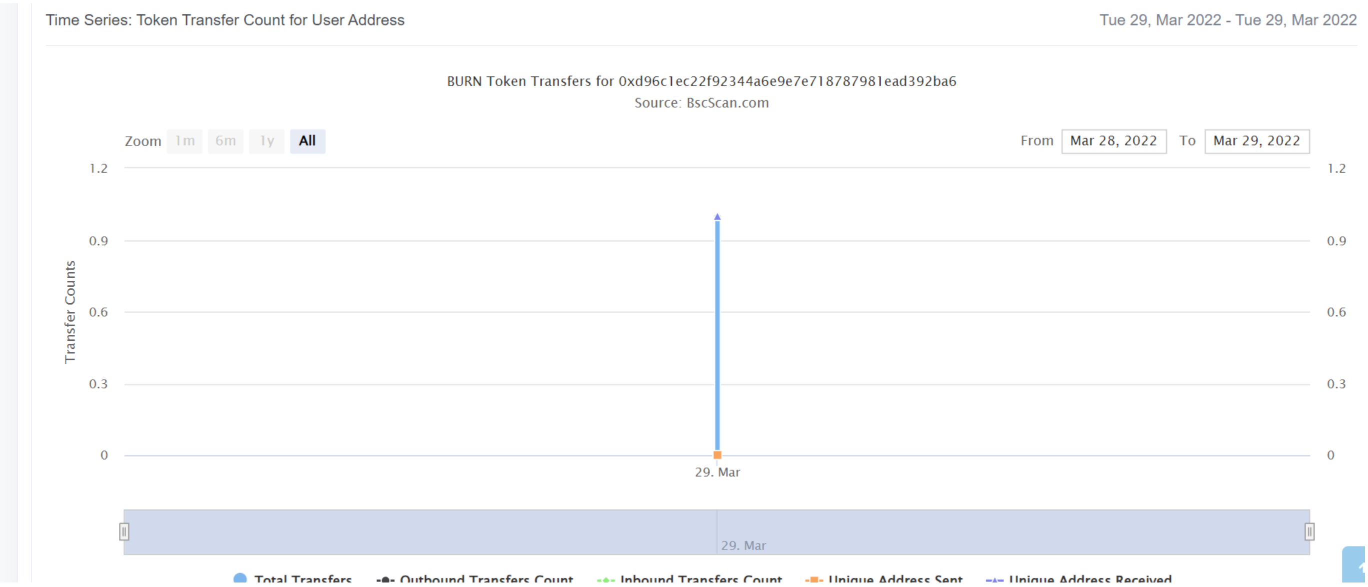
Endless Burn TOKEN Distribution



BURN Token Transfers for 0xd96c1ec22f92344a6e9e7e718787981ead392ba6

Source: BscScan.com

Endless Burn TOKEN Contract Interaction Details



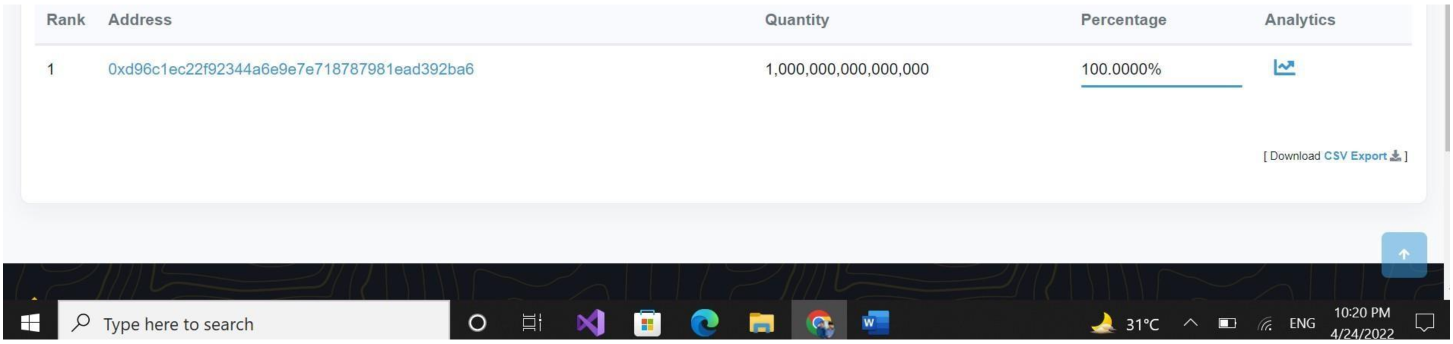
Time Series: Token Transfer Count for User Address

Tue 29, Mar 2022 - Tue 29, Mar 2022

BURN Token Transfers for 0xd96c1ec22f92344a6e9e7e718787981ead392ba6

Source: BscScan.com

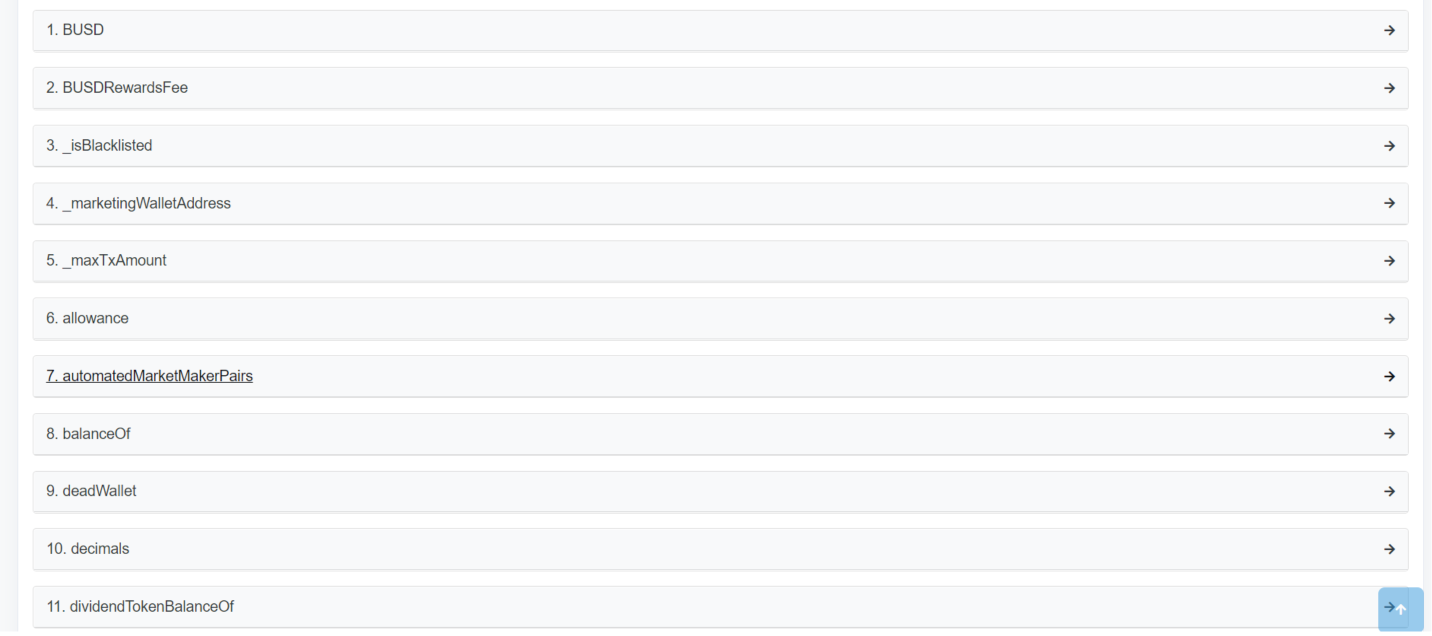
Endless Burn TOKEN Top 10 Token Holders



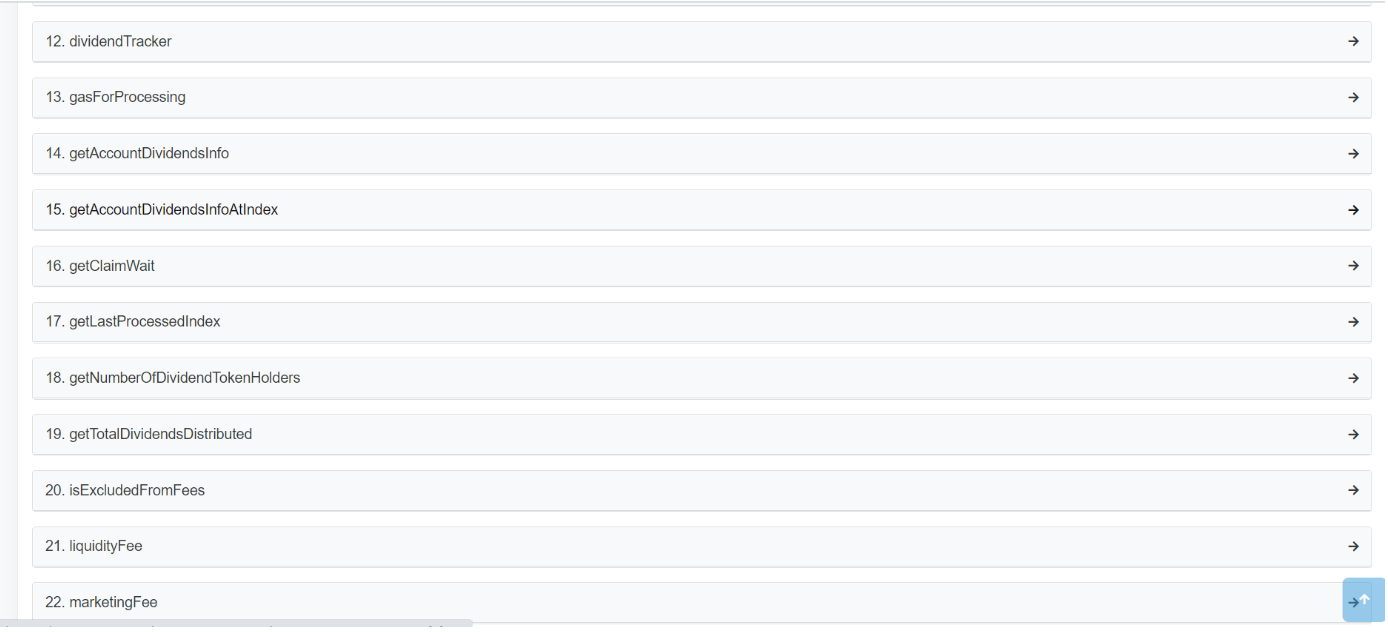
Rank	Address	Quantity	Percentage	Analytics
1	0xd96c1ec22f92344a6e9e7e718787981ead392ba6	1,000,000,000,000,000	100.0000%	

[Download CSV Export]

Contract Functions Details



1. BUSD
2. BUSDRewardsFee
3. _isBlacklisted
4. _marketingWalletAddress
5. _maxTxAmount
6. allowance
7. automatedMarketMakerPairs
8. balanceOf
9. deadWallet
10. decimals
11. dividendTokenBalanceOf



12. dividendTracker
13. gasForProcessing
14. getAccountDividendsInfo
15. getAccountDividendsInfoAtIndex
16. getClaimWait
17. getLastProcessedIndex
18. getNumberOfDividendTokenHolders
19. getTotalDividendsDistributed
20. isExcludedFromFees
21. liquidityFee
22. marketingFee

23. maxWalletToken →

24. name →

25. owner →

26. swapTokensAfAmount →

27. symbol →

28. totalFees →

29. totalsupply →

30. uniswapV2Pair →

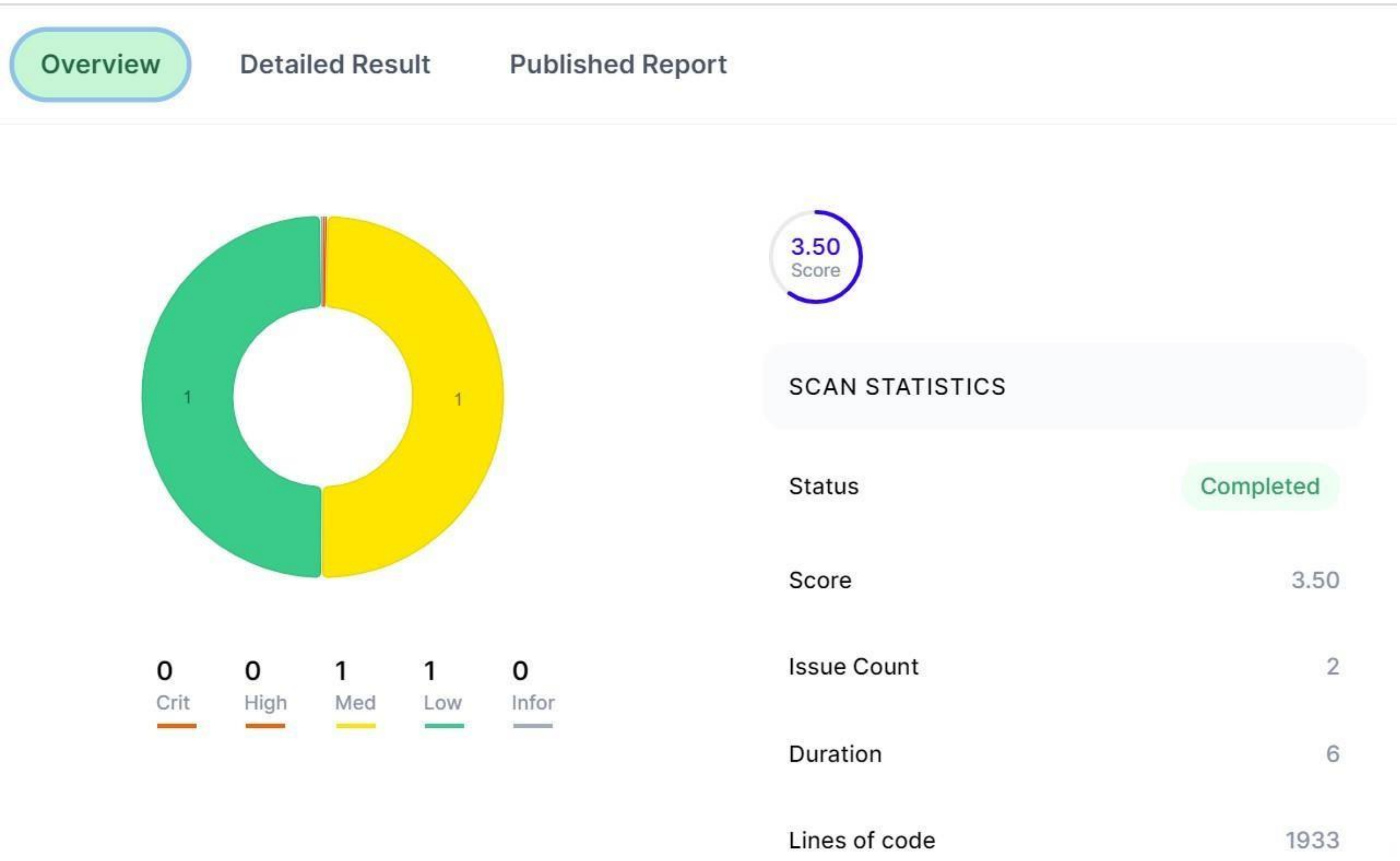
31. uniswapV2Rou ter →

32. withdrawableDividendOl →

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Compiler Compatibilities	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Moderate
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Moderate
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Severe
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Moderate
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Moderate
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Failed

Security Issues



0	0	1	1	0
Crit	High	Med	Low	Infor

SCAN STATISTICS

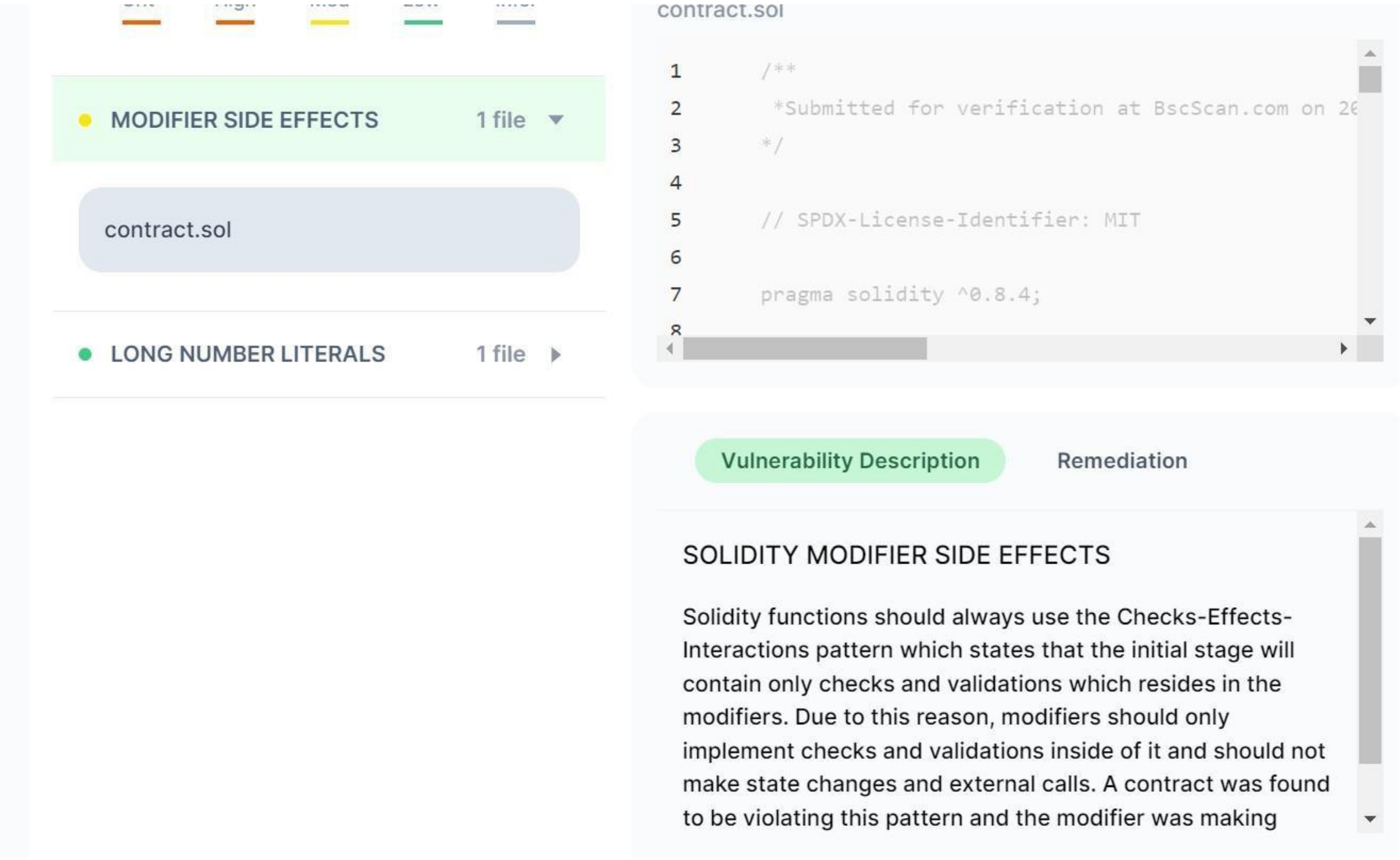
Status	Completed
Score	3.50
Issue Count	2
Duration	6
Lines of code	1933

High Severity Issues

NO high severity issues found.

Medium Severity Issues

One medium severity issues found.


● MODIFIER SIDE EFFECTS 1 file
contract.sol
● LONG NUMBER LITERALS 1 file
contract.sol
Vulnerability Description
Remediation

```
/**
 *Submitted for verification at BscScan.com on 20
*/

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.4;
```

SOLIDITY MODIFIER SIDE EFFECTS

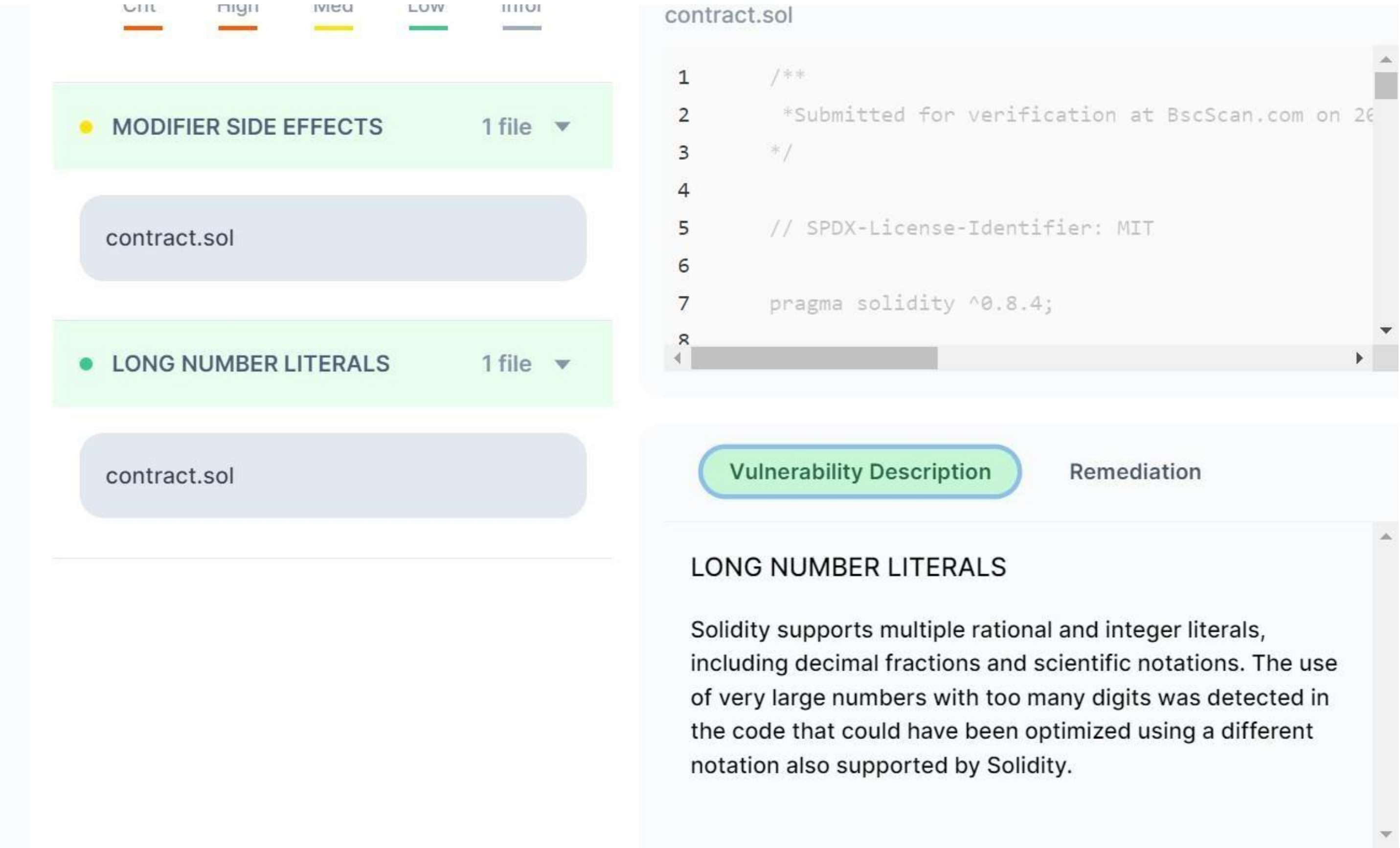
Solidity functions should always use the Checks-Effects-Interactions pattern which states that the initial stage will contain only checks and validations which resides in the modifiers. Due to this reason, modifiers should only implement checks and validations inside of it and should not make state changes and external calls. A contract was found to be violating this pattern and the modifier was making

REMEDIATION METHOD :

Only use modifiers for implementing checks and validations. Do not make external calls or state changing actions inside modifiers.

Low Severity Issues

One Low severity issues found.


Crit
High
Med
Low
Infor
MODIFIER SIDE EFFECTS 1 file
contract.sol
LONG NUMBER LITERALS 1 file
contract.sol
contract.sol
Vulnerability Description
Remediation

```
/**
 *Submitted for verification at BscScan.com on 2
*/

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.4;
```

LONG NUMBER LITERALS

Solidity supports multiple rational and integer literals, including decimal fractions and scientific notations. The use of very large numbers with too many digits was detected in the code that could have been optimized using a different notation also supported by Solidity.

REMEDIATION METHOD :

Scientific notation in the form of 2e10 is also supported, where the mantissa can be fractional but the exponent has to be an integer. The literal MeE is equivalent to M * 10**E. Examples include 2e10, 2e10, 2e-10, 2.5e1, as suggested in official solidity documentation https://docs.soliditylang.org/en/latest/types.html#rational-and-integer-l

Conclusion

Smart contracts contain High severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details NOT provided by the team.

Itish note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.