



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

ShibX



Deployer address

0x23df4561bd5167332ae7802045c74b3a95b1cab4



Client contacts:

ShibX team



Blockchain

Binance Smart Chain



Project website:

<http://www.shibxbsc.com/>

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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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

TechRate was commissioned by ShibX to perform an audit of smart contracts:

<https://bscscan.com/address/0xaa357b0f167923efc1d6978a868f81866ca6e98c#code>

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

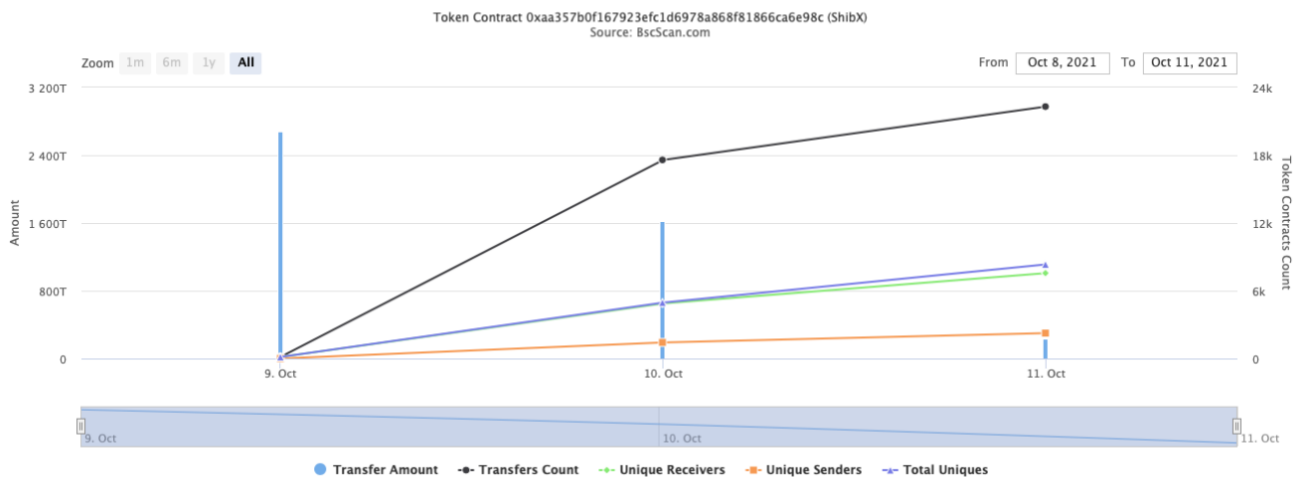
Token contract details for 13.10.2021

Contract name	ShibX
Contract address	0xaA357b0F167923Efc1D6978a868f81866cA6E98c
Total supply	15,279,281,063,578.8805
Token ticker	\$ShibX
Decimals	4
Token holders	9,672
Transactions count	63,981
Top 100 holders dominance	83.87%
Total fee	15
Auto liquidity receiver	0x23df4561bd5167332ae7802045c74b3a95b1cab4
Marketing fee receiver	0x99f3c7388a360eaa292ca653e367301931b4696a
Pair	0x2bd26aab74d0484a905166420b1aae13db6c07bb
Contract deployer address	0x23df4561bd5167332ae7802045c74b3a95b1cab4
Contract's current owner address	0x23df4561bd5167332ae7802045c74b3a95b1cab4


💡 Token Total Supply: 15,279,281,063,578.88 Token | Total Token Holders: 9,672



Sat 9, Oct 2021 - Mon 11, Oct 2021



BASE3 Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	2,868,777,933,966.4555	18.7756%
2	 PancakeSwap V2: \$ShibX	1,064,496,223,637.0118	6.9669%
3	0x99f3c7388a360eaa292ca653e367301931b4696a	930,794,427,807.4045	6.0919%
4	0x7e93b6b0b5caf955364d717b793e097003357e2	305,585,621,271.6731	2.0000%
5	0x351a6a1bb19e1c99cdd9d9b8b8975cb05bdd2b74	207,064,124,581.1398	1.3552%
6	0xd9805b78e60f9da41ff73b9c123932e5dd38317f	197,800,813,737.5767	1.2946%
7	0xafaf03aad1e6d6d50b196bd9614fd0ae0d0765f	180,479,452,079.9179	1.1812%
8	0x62909446288bc48acc5d80f6de690000811ea1be	166,724,011,136.116	1.0912%
9	0x7afd06aa1391f7e6b9aa5680df9bd0c2262f277e	158,000,000,000	1.0341%
10	0xb939304eb2b93c9c95150f816a7c9d0958f0fb5a	152,792,810,635.8843	1.0000%



Contract functions details

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div

+ [Lib] SafeMathInt

- [Int] mul
- [Int] div
- [Int] sub
- [Int] add
- [Int] abs

+ [Int] IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ Auth

- [Pub] <Constructor> #
- [Pub] authorize #
 - modifiers: onlyOwner
- [Pub] unauthorize #
 - modifiers: onlyOwner
- [Pub] isOwner
- [Pub] isAuthorized
- [Pub] transferOwnership #
 - modifiers: onlyOwner

+ [Int] IDEXFactory

- [Ext] createPair #

+ [Int] InterfaceLP

- [Ext] sync #

+ [Int] IDEXRouter

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity #
- [Ext] addLiquidityETH (\$)
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IDividendDistributor

- [Ext] setDistributionCriteria #

- [Ext] setShare #
- [Ext] deposit (\$)
- [Ext] process #
- + DividendDistributor (IDividendDistributor)

- [Pub] <Constructor> #
- [Ext] setDistributionCriteria #
 - modifiers: onlyToken
- [Ext] setShare #
 - modifiers: onlyToken
- [Ext] deposit (\$)
 - modifiers: onlyToken
- [Ext] process #
 - modifiers: onlyToken
- [Int] shouldDistribute
- [Int] distributeDividend #
- [Ext] claimDividend #
- [Pub] getUnpaidEarnings
- [Int] getCumulativeDividends
- [Int] addShareholder #
- [Int] removeShareholder #

+ ShibX (IBEP20, Auth)

- [Pub] rebase_percentage #
 - modifiers: onlyMaster
- [Pub] rebase #
 - modifiers: onlyMaster
- [Pub] <Constructor> #
 - modifiers: Auth
- [Ext] <Fallback> (\$)
- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Pub] balanceOf
- [Ext] allowance
- [Pub] approve #
- [Ext] approveMax #
- [Ext] transfer #
- [Ext] transferFrom #
- [Int] _transferFrom #
- [Int] _basicTransfer #
- [Int] checkTxLimit
- [Int] shouldTakeFee
- [Int] takeFee #
- [Int] shouldSwapBack
- [Ext] clearStuckBalance #
 - modifiers: authorized
- [Ext] clearStuckBalance_sender #
 - modifiers: authorized
- [Ext] set_sell_multiplier #
 - modifiers: onlyOwner
- [Pub] tradingStatus #
 - modifiers: onlyOwner
- [Pub] launchStatus #

- modifiers: onlyOwner
- [Pub] enable_blacklist #
 - modifiers: onlyOwner
- [Pub] manage_blacklist #
 - modifiers: onlyOwner
- [Pub] cooldownEnabled #
 - modifiers: onlyOwner
- [Int] swapBack #
 - modifiers: swapping
- [Ext] setDividendExempt #
 - modifiers: authorized
- [Ext] setFeeExempt #
 - modifiers: authorized
- [Ext] setTxLimitExempt #
 - modifiers: authorized
- [Ext] setTimeLockExempt #
 - modifiers: authorized
- [Ext] setFees #
 - modifiers: authorized
- [Ext] setFeeReceivers #
 - modifiers: authorized
- [Ext] setSwapBackSettings #
 - modifiers: authorized
- [Ext] setTargetLiquidity #
 - modifiers: authorized
- [Ext] manualSync #
- [Ext] setLP #
 - modifiers: onlyOwner
- [Ext] setMaster #
 - modifiers: onlyOwner
- [Ext] isNotInSwap
- [Ext] checkSwapThreshold
- [Ext] setDistributionCriteria #
 - modifiers: authorized
- [Ext] setDistributorSettings #
 - modifiers: authorized
- [Pub] rescueToken #
 - modifiers: onlyOwner
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified
- [Ext] checkMaxWalletToken
- [Ext] checkMaxTxAmount
- [Ext] setMaxWalletPercent_base1000 #
 - modifiers: onlyOwner
- [Ext] setMaxTxPercent_base1000 #
 - modifiers: onlyOwner
- [Ext] multiTransfer #
 - modifiers: onlyOwner
- [Ext] multiTransfer_fixed #
 - modifiers: onlyOwner

(\$) = payable function

= non-constant function

Issues Checking Status

Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
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.	Low issues
10. Methods execution permissions.	Passed
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. Out of gas

Issue:

- The function `manage_blacklist()` uses the loop to change blacklist status of addresses. It also could be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:

Check that the array length is not too big.

Owner privileges (In the period when the owner is not renounced)

- Master can rebase.
- Owner can change sellMultiplier.
- Owner can change trading and launch status.
- Owner can change blacklist mode.
- Owner can change maxRoomRent value.
- Owner can change cooldown settings.
- Owner can change pair address.
- Owner can change master address.
- Owner can withdraw BEP20 tokens.
- Owner can change _maxWalletToken and _maxTxAmount.
- Owner can multiTransfer fixed and listed token amounts.
- Authorized addresses can withdraw contract BNBs.
- Authorized addresses can include in and exclude from dividends.
- Authorized addresses can include in and exclude from fee, timelock and transaction amount.
- Authorized addresses can change fees.
- Authorized addresses can change fee receivers.
- Authorized addresses can change swap threshold and disable/enable swap.
- Authorized addresses can change targetLiquidity.
- Authorized addresses can change distribution criteria.
- Authorized addresses can change distribution GAS.

Conclusion

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

Liquidity locking details provided by the team:

<https://www.pinksale.finance/#/pinklock/record/135?chain=BSC>

TechRate 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.