Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details

Audited project

Zaddy Inu

Deployer address

0x26d90bb6b0f2069b2b15ccc9ca9e370d5d02286b

Client contacts:

Zaddy Inu team

Blockchain

Ethereum

Project website:

https://zaddyinutoken.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 Zaddy Inu to perform an audit of smart contracts:

- https://etherscan.io/address/0x4FfF29D95a8953AD28847278DD6AA11f4c695a24#code
- https://etherscan.io/address/0x7d3Fa0eA83EF907c773dB71890B2858BeD340B84#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 02.11.2021

Contract name	Zaddy Inu
Contract address	0x4FfF29D95a8953AD28847278DD6AA11f4c695a24
Total supply	1,000,000,000,000,000,000
Token ticker	ZADDY
Decimals	18
Token holders	1
Transactions count	1
Top 100 holders dominance	100.00%
Sell fee	80
Buy fee	40
Total fees	0
Uniswap V2 pair	0x0000000000000000000000000000000000000000
Contract deployer address	0x26d90bb6b0f2069b2b15ccc9ca9e370d5d02286b
Contract's current owner address	0x26d90bb6b0f2069b2b15ccc9ca9e370d5d02286b

Contracts Details

Token contract details for 02.11.2021

Contract name	BabyZaddyInu
Contract address	0x7d3Fa0eA83EF907c773dB71890B2858BeD340B84
Total supply	1,000,000,000,000
Token ticker	BZADDY
Decimals	18
Token holders	1
Transactions count	1
Top 100 holders dominance	100.00%
Sell fee	80
Buy fee	40
Total fees	0
Uniswap V2 pair	0x0000000000000000000000000000000000000000
Contract deployer address	0x26d90bb6b0f2069b2b15ccc9ca9e370d5d02286b
Contract's current owner address	0x26d90bb6b0f2069b2b15ccc9ca9e370d5d02286b

Zaddy Inu Token Distribution

The top 100 holders collectively own 100.00% (1,000,000,000,000,000,000.00 Tokens) of Zaddy Inu

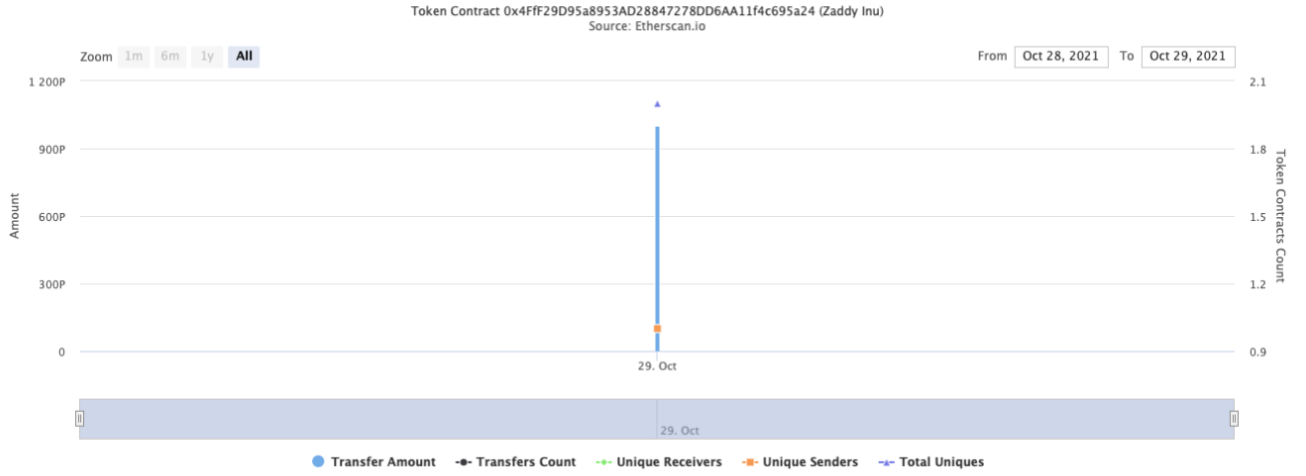
Token Total Supply: 1,000,000,000,000,000,000.00 Token | Total Token Holders: 1

(A total of 1,000,000,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000,000.00 token)

Zaddy Inu Contract Interaction Details

Time Series: Token Contract Overview

Fri 29, Oct 2021 - Fri 29, Oct 2021



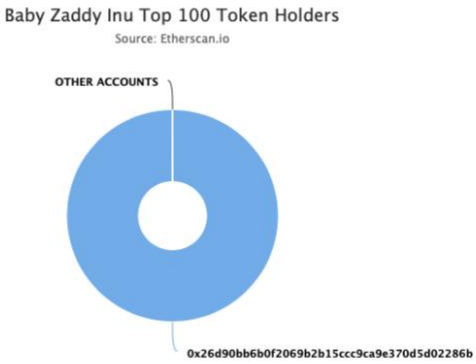
Zaddy Inu Top 10 Token Holders

Rank	Address	Quantity (Token)	Percent
1.	0x26d90bb6b0f2069b2b15ccc9ca9e370d5d02286b	1,000,000,000,000,000,000	100.0000%

Baby Zaddy Inu Token Distribution

The top 100 holders collectively own 100.00% (1,000,000,000,000.00 Tokens) of Baby Zaddy Inu

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 1

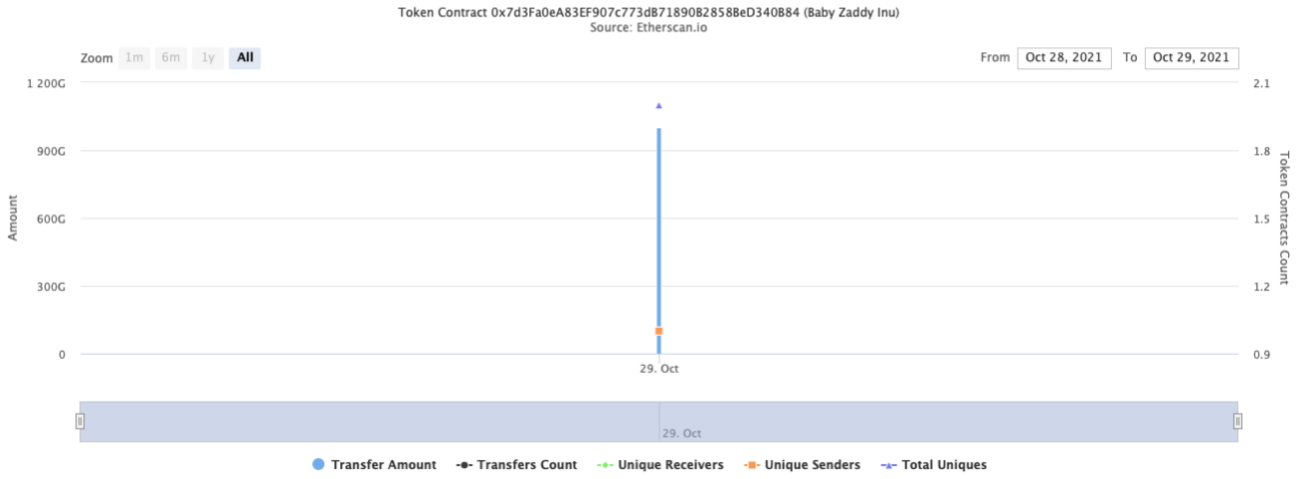


(A total of 1,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

Baby Zaddy Inu Contract Interaction Details

Time Series: Token Contract Overview

Fri 29, Oct 2021 - Fri 29, Oct 2021



Baby Zaddy Inu Top 10 Token Holders

Rank	Address	Quantity (Token)	Percent
1.	0x26d90bb6b0f2069b2b15ccc9ca9e370d5d02286b	1,000,000,000,000	100.0000%

Contract functions details

+ [Int] IERC20
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #
  - [Ext] calculateBonusReflection #
+ Context
  - [Int] _msgSender
  - [Int] _msgData
+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #
+ ZaddyInu (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] reflectionBonusBalance
  - [Pub] getUserToken2Balance
  - [Pub] transfer #
  - [Ext] burn #
    - modifiers: onlyOwner
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] isExcludedFromReward
  - [Pub] totalFees
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner

- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Pub] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] setExcludeFromMaxTx #
  - modifiers: onlyOwner
- [Ext] setFeePercent #
  - modifiers: onlyOwner
- [Ext] setBuyFee #
  - modifiers: onlyOwner
- [Ext] setSellFee #
  - modifiers: onlyOwner
- [Ext] setReflectionFees #
  - modifiers: onlyOwner
- [Pub] changeBonusValues #
  - modifiers: onlyOwner
- [Ext] setLpAddress #
  - modifiers: onlyOwner
- [Ext] setToken2 #
  - modifiers: onlyOwner
- [Ext] startTrading #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _getRate
- [Pub] getTotalFeePerTx
- [Prv] _getCurrentSupply
- [Pub] isExcludedFromFee
- [Pub] isExcludedFromMaxTx
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _tokenTransfer #
- [Pub] calculateBonusReflection #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Int] _takeAllFee #

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

($) = payable function
= non-constant function

Baby Contract functions details

+ [Int] IERC20
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #
  - [Ext] calculateBonusReflection #
+ Context
  - [Int] _msgSender
  - [Int] _msgData
+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #
+ BabyZaddyInu (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] reflectionBonusBalance
  - [Pub] getUserToken2Balance
  - [Pub] transfer #
  - [Ext] burn #
    - modifiers: onlyOwner
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] isExcludedFromReward
  - [Pub] totalFees
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner

- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Pub] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] setExcludeFromMaxTx #
  - modifiers: onlyOwner
- [Ext] setFeePercent #
  - modifiers: onlyOwner
- [Ext] setBuyFee #
  - modifiers: onlyOwner
- [Ext] setSellFee #
  - modifiers: onlyOwner
- [Ext] setReflectionFees #
  - modifiers: onlyOwner
- [Pub] changeBonusValues #
  - modifiers: onlyOwner
- [Ext] setLpAddress #
  - modifiers: onlyOwner
- [Ext] setToken2 #
  - modifiers: onlyOwner
- [Ext] startTrading #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _getRate
- [Pub] getTotalFeePerTx
- [Prv] _getCurrentSupply
- [Pub] isExcludedFromFee
- [Pub] isExcludedFromMaxTx
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _tokenTransfer #
- [Pub] calculateBonusReflection #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Int] _takeAllFee #

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

($) = 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.	High issue
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

1. Out of gas

Issue:

- The function `calculateBonusReflection()` operates only reflection balance without any checking address to be excluded from reward.

Recommendation:
Check that the excluded array length is not too big.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

2. Out of gas

Issue:

- The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function includeInReward(address account⬆) external onlyOwner {
    require(_isExcluded[account⬆], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account⬆) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _rOwned[account⬆] = _tOwned[account⬆].mul(_getRate());
            _tOwned[account⬆] = 0;
            _isExcluded[account⬆] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

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

- Owner can change fees.
- Owner can change the maximum transaction amount.
- Owner can exclude from the fee and maxTx.
- Owner can enable/disable reflection fees.
- Owner can change reflectionInc and pairValue.
- Owner can change Uniswap pair.
- Owner can change token2 address.
- Owner can enable trading.
- Owner can burn token (transfer to burn address).
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

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.

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.