Star Wars Token

RugfreeCoins Verified on December 26th, 2023

Overview

✅ No mint function found, the owner cannot mint tokens after initial deployment.

✅ The owner can't set a max transaction limit.

✅ The owner can't pause trading once it's enabled

✅ The owner can't change fees over 6%.

✅ The owner can't blacklist wallets.

✅ The owner can't set a max wallet limit

✅ The owner can't claim the contract's balance of its own token.

❗ HIGH SEVERITY ISSUES

The owner can adjust the swap point up to the total supply. If the owner sets the swap point to a significantly large amount, the swap may fail due to price impact issues.

```solidity
function updateSwapTokensAtAmount(
    uint256 _swapTokensAtAmount
) external onlyOwner returns (bool) {
    require(
        _swapTokensAtAmount < totalSupply(),
        "Swap amount cannot be higher than total supply."
    );
    require(
        _swapTokensAtAmount >= (totalSupply() * 1) / 100000,
        "Swap amount cannot be lower than 0.001% total supply."
    );
    swapTokensAtAmount = _swapTokensAtAmount;
    return true;
}
```

Contents

Audit details

Audited project

Star Wars Token

Contract Address

0xE5b3e8C88ADE3cfe393051078CB59854953faa22

Client contact

Star Wars Token Team

Blockchain

Binance Smart chain

Project website

https://starwar.app/

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

RugfreeCoins was commissioned by the **Star Wars Token Team** to perform an audit of the smart contract.

https://bscscan.com/token/0xe5b3e8c88ade3cfe393051078cb59854953faa22

This audit focuses on verifying that the smart contract is secure, resilient, and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, and long-term sustainability, and as a guide to improving the smart contract's security posture by remediating the identified issues.

Tokenomics

▲ 3% tax when buying & selling

3% of trade goes to the marketing wallet in BNB

Target market and the concept

- Anyone who's interested in the Crypto space with long-term investment plans.
- Anyone who's ready to earn a passive income by holding tokens.
- Anyone who's interested in trading tokens.
- Anyone who's interested in taking part in the Star Wars token ecosystem.
- Anyone who's interested in taking part in the future plans of Star Wars Token.
- Anyone who's interested in making financial transactions with any other party using Star Wars Token as the currency.

Potential to grow with score points

⚡ Project efficiency	8 / 10
🌟 Project uniqueness	8 / 10
📊 Information quality	8 / 10
👆 Service quality	8 / 10
💻 System quality	8 / 10
🌍 Impact on the community	8 / 10
💼 Impact on the business	9 / 10
🔮 Preparing for the future	8 / 10
🔒 Smart contract security	9/ 10
🛠️ Smart contract functionality assessment	9 / 10
🏆 **Total Score**	**8.3**/ **10**

Contract details

Token contract details for 26th of December 2023

Contract name	**Star Wars**
Contract address	**0xE5b3e8C88ADE3cfe393051078CB59854953faa22**
Token supply	**1,000,000,000**
Token ticker	**STW**
Decimals	**18**
Token holders	**1**
Transaction count	**1**
Contract deployer address	**0x349BB193Cf7588cA07233Cf80d964885B73FaBa2**
Contract's current owner address	**0x349BB193Cf7588cA07233Cf80d964885B73FaBa2**
Fee wallet	**0x349BB193Cf7588cA07233Cf80d964885B73FaBa2**

Contract code function details

Nº	Category	Item	Result
1	Coding conventions	ERC20 Token standards	PASS
		Compile errors	PASS
		Compiler version security	PASS
		Visibility specifiers	PASS
		Gas consumption	PASS
		SafeMath features	PASS
		Fallback usage	PASS
		tx.origin usage	PASS
		Deprecated items	PASS
		Redundant code	LOW
		Overriding variables	PASS
2	Function call audit	Authorization of function call	PASS
		Low level function (call/delegate call) security	PASS
		Returned value security	PASS
		Self destruct function security	PASS
3	Business security & centralisation	Access control of owners	HIGH
		Business logics	PASS
		Business implementation	PASS
4	Integer overflow/underflow		PASS
5	Reentrancy		PASS
6	Exceptional reachable state		PASS
7	Transaction ordering dependence		PASS
8	Block properties dependence		PASS
9	Pseudo random number generator (PRNG)		PASS
10	DoS (Denial of Service)		PASS
11	Token vesting implementation		PASS
12	Fake deposit		PASS
13	Event security		PASS

Contract description table

The below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions, and implementations with their visibility and mutability.

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
IERC20Errors	**Interface**			
IERC721Errors	**Interface**			
IERC1155Errors	**Interface**			
IERC20	**Interface**			
L	totalSupply	External ❗		NO ❗
L	balanceOf	External ❗		NO ❗
L	transfer	External ❗	🛑	NO ❗
L	allowance	External ❗		NO ❗
L	approve	External ❗	🛑	NO ❗
L	transferFrom	External ❗	🛑	NO ❗
IERC20Metadata	**Interface**	**IERC20**		
L	name	External ❗		NO ❗
L	symbol	External ❗		NO ❗
L	decimals	External ❗		NO ❗
Context	**Implementation**			
L	_msgSender	Internal 🔒		
L	_msgData	Internal 🔒		

L	_contextSuffixLength	Internal 🔒		
ERC20	**Implementation**	**Context, IERC20, IERC20 Metadata, IERC20 Errors**		
L		Public ❗	🛑	NO ❗
L	name	Public ❗		NO ❗
L	symbol	Public ❗		NO ❗
L	decimals	Public ❗		NO ❗
L	totalSupply	Public ❗		NO ❗
L	balanceOf	Public ❗		NO ❗
L	transfer	Public ❗	🛑	NO ❗
L	allowance	Public ❗		NO ❗
L	approve	Public ❗	🛑	NO ❗
L	transferFrom	Public ❗	🛑	NO ❗
L	_transfer	Internal 🔒	🛑	
L	_update	Internal 🔒	🛑	
L	_mint	Internal 🔒	🛑	
L	_burn	Internal 🔒	🛑	
L	_approve	Internal 🔒	🛑	
L	_approve	Internal 🔒	🛑	
L	_spendAllowance	Internal 🔒	🛑	
Ownable	**Implementation**	**Context**		
L		Public ❗	🛑	NO ❗
L	owner	Public ❗		NO ❗
L	_checkOwner	Internal 🔒		
L	renounceOwnership	Public ❗	🛑	onlyOwner
L	transferOwnership	Public ❗	🛑	onlyOwner

L	_transferOwnership	Internal 🔒	🛑	
IUniswapV2 Router01	**Interface**			
L	factory	External ❗		NO ❗
L	WETH	External ❗		NO ❗
L	addLiquidity	External ❗	🛑	NO ❗
L	addLiquidityETH	External ❗	💵	NO ❗
L	removeLiquidity	External ❗	🛑	NO ❗
L	removeLiquidityETH	External ❗	🛑	NO ❗
L	removeLiquidityWithPermit	External ❗	🛑	NO ❗
L	removeLiquidityETHWithPermit	External ❗	🛑	NO ❗
L	swapExactTokensForTokens	External ❗	🛑	NO ❗
L	swapTokensForExactTokens	External ❗	🛑	NO ❗
L	swapExactETHForTokens	External ❗	💵	NO ❗
L	swapTokensForExactETH	External ❗	🛑	NO ❗
L	swapExactTokensForETH	External ❗	🛑	NO ❗
L	swapETHForExactTokens	External ❗	💵	NO ❗
L	quote	External ❗		NO ❗
L	getAmountOut	External ❗		NO ❗
L	getAmountIn	External ❗		NO ❗
L	getAmountsOut	External ❗		NO ❗
L	getAmountsIn	External ❗		NO ❗
IUniswapV2 Router02	**Interface**	**IUniswapV2 Router01**		
L	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
L	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
L	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗

L	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO ❗
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
IUniswapV2 Factory	**Interface**			
L	feeTo	External ❗		NO ❗
L	feeToSetter	External ❗		NO ❗
L	getPair	External ❗		NO ❗
L	allPairs	External ❗		NO ❗
L	allPairsLength	External ❗		NO ❗
L	createPair	External ❗	🛑	NO ❗
L	setFeeTo	External ❗	🛑	NO ❗
L	setFeeToSetter	External ❗	🛑	NO ❗
StarWarsToken	**Implementation**	**ERC20, Ownable**		
L		Public ❗	🛑	ERC20 Ownable
L		External ❗	💵	NO ❗
L	_update	Internal 🔒	🛑	
L	swapTokensForEth	Private 🔐	🛑	lockTheSwap
L	sendETHToFee	Private 🔐	🛑	
L	updateFeeWallet	External ❗	🛑	onlyOwner
L	_updateFeeWallet	Private 🔐	🛑	
L	updateFees	Public ❗	🛑	onlyOwner
L	_updateFees	Private 🔐	🛑	
L	excludeFromFees	Public ❗	🛑	onlyOwner
L	_excludeFromFees	Private 🔐	🛑	
L	excludeFromMaxTransactionAmount	Public ❗	🛑	onlyOwner

L	_excludeFromMaxTransactionAmount	Private 🔐	🛑	
L	setAutomatedMarketMakerPair	Public ❗	🛑	onlyOwner
L	_setAutomatedMarketMakerPair	Private 🔐	🛑	
L	updateSwapTokensAtAmount	External ❗	🛑	onlyOwner

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Security issue checking status

❖ High severity issues

The owner can adjust the swap point up to the total supply. If the owner sets the swap point to a significantly large amount, the swap may fail due to price impact issues.

```solidity
function updateSwapTokensAtAmount(
    uint256 _swapTokensAtAmount
) external onlyOwner returns (bool) {
    require(
        _swapTokensAtAmount < totalSupply(),
        "Swap amount cannot be higher than total supply."
    );
    require(
        _swapTokensAtAmount >= (totalSupply() * 1) / 100000,
        "Swap amount cannot be lower than 0.001% total supply."
    );
    swapTokensAtAmount = _swapTokensAtAmount;
    return true;
}
```

❖ Medium severity issues

No medium severity issues found

❖ Low severity issues

The contract does not check for maximum transaction limits, rendering all functions related to the maximum transaction limit redundant.

```solidity
_excludeFromMaxTransactionAmount(address(0xdead), true);
_excludeFromMaxTransactionAmount(address(this), true);
_excludeFromMaxTransactionAmount(address(_uniswapV2Router), true);
_excludeFromMaxTransactionAmount(address(uniswapV2Pair), true);
_excludeFromMaxTransactionAmount(owner(), true);
```

Owner privileges

❖ Owner can change fee wallet

```
function updateFeeWallet(address _feeWallet) external onlyOwner {
    _updateFeeWallet(_feeWallet);
}
```

❖ Owner can change buy and sell fees up-to to 6% (each 3%)

```
function updateFees(uint256 _buyFee, uint256 _sellFee) public onlyOwner {
    _updateFees(_buyFee, _sellFee);
}

function _updateFees(uint256 _buyFee, uint256 _sellFee) private {
    require(_buyFee <= 30 && _sellFee <= 30, "Invalid fees"); // _buyFee and
_sellFee <= 3%
    buyFee = _buyFee;
    sellFee = _sellFee;
}
```

❖ Owner can include/exclude wallets from fees

```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    _excludeFromFees(account, excluded);
}
```

❖ Owner can add/remove new lp pairs

```
function setAutomatedMarketMakerPair(
    address pair,
    bool value
) public onlyOwner {
    require(
        pair != uniswapV2Pair,
        "The pair cannot be removed from automatedMarketMakerPairs"
    );
    require(pair != address(0), "Zero address");

    _excludeFromMaxTransactionAmount(pair, value);
    _setAutomatedMarketMakerPair(pair, value);
}
```

❖ Owner can change swap point

```
function updateSwapTokensAtAmount(
    uint256 _swapTokensAtAmount
) external onlyOwner returns (bool) {
    require(
        _swapTokensAtAmount < totalSupply(),
        "Swap amount cannot be higher than total supply."
    );
    require(
        _swapTokensAtAmount >= (totalSupply() * 1) / 100000,
        "Swap amount cannot be lower than 0.001% total supply."
    );
    swapTokensAtAmount = _swapTokensAtAmount;
    return true;
}
```

Audit conclusion

RugFreeCoins team has performed in-depth testing, line-by-line manual code review, and automated audit of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, manipulations, and hacks. According to the smart contract audit.

Smart contract functional Status:	PASS ▾
Smart contract security Status:	HIGH ISSUES ▾
Number of risk issues:	2
Solidity code functional issue level:	PASS ▾
Number of owner privileges:	5
Centralization risk correlated to the active owner:	HIGH ▾
Smart contract active ownership:	ACTIVE ▾