expelee

Building the Futuristic Blockchain Ecosystem

Security Audit Report
FOR

8BitEarn Staking Platform

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

🔍	**Audit Result**	**Passed**
🔍	**KYC Verification**	**Done**
📅	**Audit Date**	**16 Jan 2023**

Audit Passed With No Risk
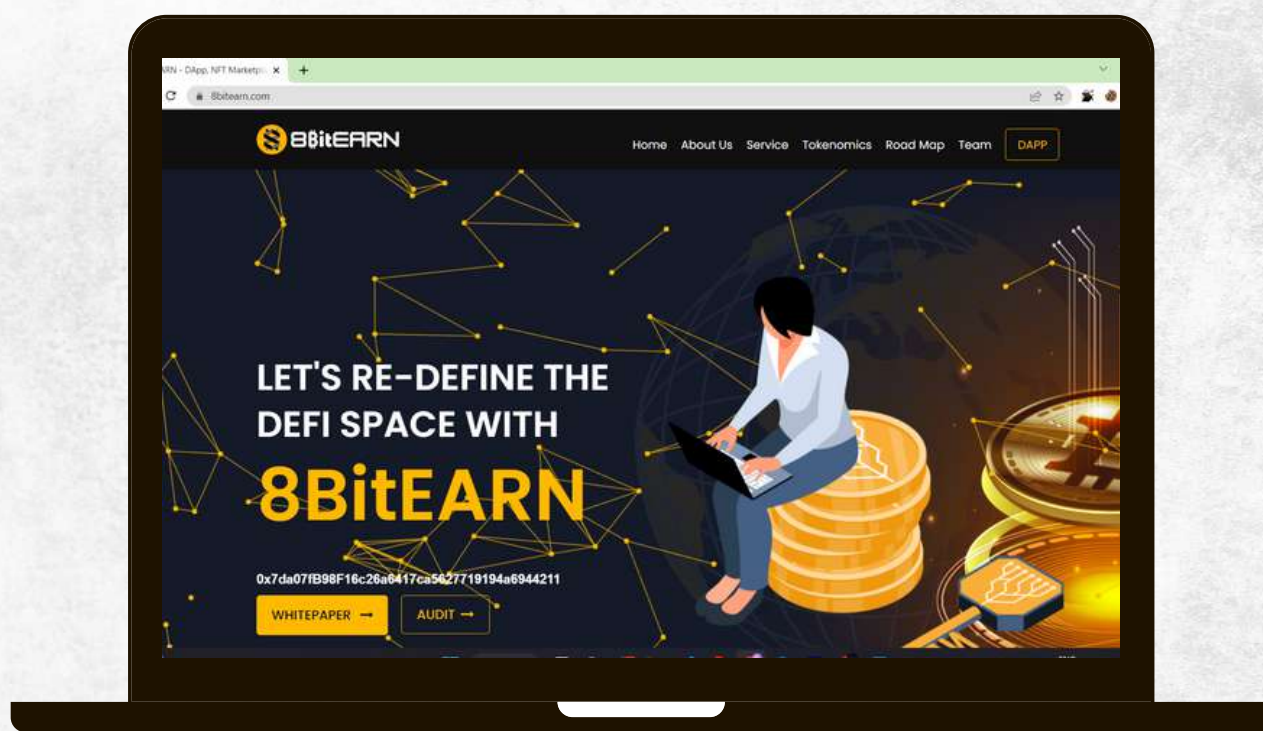
-Team Expelee

PROJECT DESCRIPTION

8BitEARN

$8Bit is a hyper-deflationary BEP-20 native token of the 8BitEARN Ecosystem, that opens numerous passive income streams & benefits to holders by offering BTC Reflection, Staking Rewards, Monthly Diamond Hand Rewards, Quarterly Revenue Distribution, BUSD Credit Facility, Investment Insurance at ProPAD, Farming & Cashback at ProDEX, several DeFi benefits to 8Bit NFT holders with flawless NFT trading at own NFT Marketplace, transparency & integrity through DAO Governance and many more.

Social Media Profiles

8BitEARN

🌐 https://www.8bitearn.com/

✈ https://t.me/official8BitEARN

🐦 https://twitter.com/8BitEARN

It's always good to check the social profiles of the project, before making your investment.

-Team Expelee

AUDIT METHODOLOGY

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:
- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Complier
- Hardhat

FUNCTION OVERVIEW

Can Take Back Ownership	Not Detected
Owner Change Balance	Not Detected
Blacklist	Not Detected
Modify Fees	Not Detected
Proxy	Not Detected
Whitelisted	Not Detected
Anti Whale	Not Detected
Trading Cooldown	Not Detected
Transfer Pausable	Not Detected
Cannot Sell All	Not Detected
Hidden Owner	Not Detected
Mint	Not Detected

VULNERABILITY CHECKLIST

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

AUDIT SUMMARY

Audit Scope

8Bit Staking:

8Bit staking platform has 2 components:
1- Staking contract, for staking 8Bit tokens
2- BUSD credit pool for borrowing BUSD tokens

Contracts are deployed on Binance smart chain, at this addresses:
Staking:
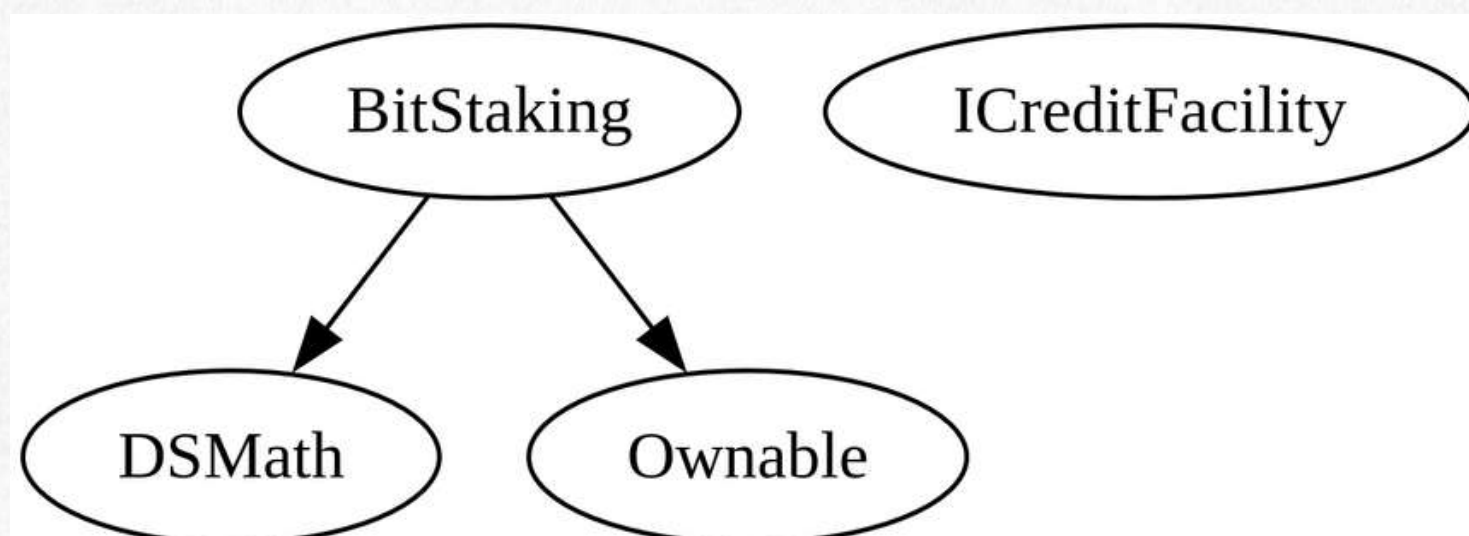0xD44cd24f48dC314f0594EB1D76916f2fDBBE107d
Staking Token (8Bit):
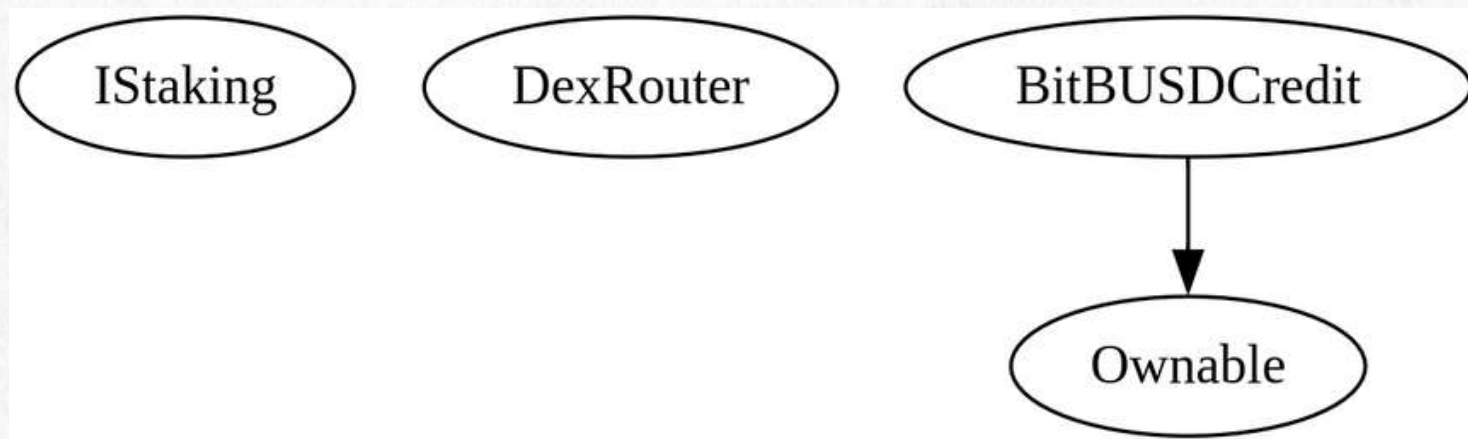0x7da07fB98F16c26a6417ca5627719194a6944211
BUSD credit facility:
0x5ca35ccF048f26b295fEEac1B0473d0a75eB5f3a

Inheritance Trees:

Staking Contract:

BUSD Credit Facility:

Functions:

Staking Contract

BitStaking	Implementation	DSMath, Ownable		
└	<Constructor>	Public ❗	🔴	NO ❗
└	setCreditFacility	Public ❗	🔴	onlyOwner
└	setStakingToken	Public ❗	🔴	onlyOwner
└	setStakingVault	External ❗	🔴	onlyOwner
└	setPenaltyReceiver	External ❗	🔴	onlyOwner
└	StartStaking	External ❗	🔴	onlyOwner
└	changeAPY	External ❗	🔴	onlyOwner
└	changeMinTokensToEnter	External ❗	🔴	onlyOwner
└	AddNFT	External ❗	🔴	onlyOwner
└	removeNFT	External ❗	🔴	onlyOwner
└	StakeTokens	External ❗	🔴	NO ❗
└	Unstake	Public ❗	🔴	NO ❗
└	claimRewards	Public ❗	🔴	NO ❗
└	emergencyWithdraw	Public ❗	🔴	NO ❗
└	penaltyCreditPoolStaker	External ❗	🔴	onlyOwner
└	massPenaltyCreditPoolStakers	External ❗	🔴	onlyOwner
└	getRewards	Public ❗		NO ❗
└	_calculateRewardsTimeRange	Internal 🔒		
└	calculateInteresetInSeconds	Internal 🔒		
└	ratio	Internal 🔒		
└	accrueInterest	Internal 🔒		
└	average	Internal 🔒		
└	findAPYAtTimestamp	Internal 🔒		
└	checkIfHoldsNFT	Public ❗		NO ❗
└	getVolumeAtTimeStamp	External ❗		NO ❗
└	getLastWeekVolume	External ❗		NO ❗
└	getPoolStakedTokens	Public ❗		NO ❗

	└	getTotalStaked	Public ❗			NO ❗	
	└	getStakerEndTime	Public ❗			NO ❗	
	└	getStakerStartTime	Public ❗			NO ❗	
	└	getRemainingStakeTime	Public ❗			NO ❗	
	└	getStakerLastClaimTime	Public ❗			NO ❗	
	└	getAPYCheckPoint	Public ❗			NO ❗	
	└	getTotalClaimed	Public ❗			NO ❗	
	└	getPoolAPY	Public ❗			NO ❗	
	└	getPoolMinToEnter	Public ❗		|NO ❗	|king

BUSD Facility

	BitBUSDCredit	Implementation	Ownable		
	└	<Constructor>	Public ❗		🔴 |NO ❗	
	└	updateDex	External ❗		🔴	onlyOwner
	└	setStakingContract	External ❗		🔴	onlyOwner
	└	setStakingToken	External ❗		🔴	onlyOwner
	└	setBUSDToken	External ❗		🔴	onlyOwner
	└	BorrowBUSD	Public ❗		🔴 |NO ❗	
	└	RepayBUSD	Public ❗		🔴 |NO ❗	
	└	resetBorrower	Public ❗	|^🔴	onlyOwnerOrStaking
	└	getBorrowerStatus	Public ❗		|NO ❗	
	└	setBUSDLimit	External ❗		🔴	onlyOwner
	└	getBorrowTime	Public ❗		|NO ❗	
	└	getTotalBorrowedBUSD	Public ❗		|NO ❗	
	└	getTotalRepaidBUSD	Public ❗		|NO ❗	
	└	getTotalCollateraled8Bit	Public ❗		|NO ❗	
	└	getBorrowStartTime	Public ❗		|NO ❗	
	└	getRepaidTime	Public ❗		|NO ❗	
	└	getNotRepaid	Public ❗		|NO ❗	
	└	getCanBeCollateraled	Public ❗		|NO ❗	

└	getCanBeBorrowedBUSD	Public ❗		NO❗
└	BUSDTo8Bit	Public ❗		NO❗
└	EightBitToBUSD	Public ❗		NO❗
└	getBNBPrice	Public ❗		NO❗
└	get8BitPrice	Public ❗		NO❗
└	withdrawBUSDProtocol	Public ❗	🔴	onlyOwner
└	withdrawStuckTokens	Public ❗	🔴	onlyOwner
└	withdrawStuckBNB	Public ❗	💵	onlyOwner
└	<Receive Ether>	External ❗	💵	NO❗

Features

Staking:

8Bit holders can stake their tokens in 3 different pools:
1- standard pool : not locked
2- nft pool: not locked
3- busd credit pool: locked

NFT pool is only available for 8bit NFT holders. Standard pools are available for all 8bit holders. If holders decide to borrow BUSD token's equal to 30% value of their staked tokens, they should stake their tokens in this pool.

Dynamic APY:

Pools can have different APY which can only be edited by 8Bit owners.

BUSD credit facility:

8Bit holder can borrow equal to 30% value of their staked tokens in busd credit pool.
This borrowed BUSD tokens must be repaid after 30 days:
1- fail on repay after 30 days => APY rewards closed
2- fail to repay on 45 days => staked tokens + APY rewards can be withdrawed by owner

MANUAL AUDIT

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to a methodology based on OWASP standards.

Vulnerabilities are divided into three primary risk categories: high, medium, and low.

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious Input Handling
- Escalation of privileges
- Arithmetic
- Gas use

	Overall Risk Severity			
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
		Likelihood		

FINDINGS

- **High Risk Findings**:0
- **Medium Risk Findings**:0
- **Low Risk Findings**:0
- **Suggestions & discussion**: 1

Suggestions and Improvements

- Repaying BUSD can be unprofitable:

if 8bit price drop below 30% of when BUSD was borrowed, then repaying busd wont be profitable for borrower and this is considered a token loss for 8Bit platform.

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 Start-up. Coping up with numerous solutions for blockchain Security and constructing a Web3 Ecosystem from Deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

🌐 www.expelee.com

🐦 expeleeofficial   Ⓜ expelee

✈ Expelee   in expelee

📷 expelee_official   🐙 expelee-co

expelee

Building the Futuristic **Blockchain Ecosystem**

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always Do your own research and protect yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.