

# SMART CONTRACT SECURITY AUDIT DAY OF DEFEAT



SMART CONTRACT AUDIT | TEAM KYC | PROJECT EVALUATION

RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 

# Summary

<b>Auditing Firm</b>	InterFi Network
<b>Architecture</b>	InterFi "Echelon" Auditing Standard
<b>Smart Contract Audit Approved By</b>	Chris   Blockchain Specialist at InterFi Network
<b>Project Overview Approved BY</b>	Albert   Project Specialist at InterFi Network
<b>Platform</b>	Solidity
<b>Audit Check (Mandatory)</b>	Static, Software, Auto Intelligent & Manual Analysis
<b>Project Check (Optional)</b>	KYC, Website & Socials Analysis (Not Applicable)
<b>Consultation Request Date</b>	October 03, 2021
<b>Report Date</b>	October 11, 2021

## Audit Summary

### Smart Contract Security Audit

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

- ❖ **Day Of Defeat's smart contract source codes has MEDIUM RISK SEVERITY.**
- ❖ **Day Of Defeat utilizes "takeoutTokenInCase" function which allows the owner to transfer any amount tokens to any address on the network. According to the project team, this token will be utilized only if there's any remaining BUSD left in the fund pool at the end of the project.**

For the detailed understanding of risk severity, source code vulnerability, and functional test, kindly refer to the audit.



# Table Of Contents

## **Project Information**

Overview .....	4
----------------	---

## **InterFi “Echelon” Audit Standard**

Audit Scope & Methodology .....	7
InterFi’s Risk Classification.....	9

## **Smart Contract Risk Assessment**

Contract Overview .....	10
Static Analysis.....	11
Software Analysis .....	13
Manual Analysis.....	16
SWC Attacks.....	18
Risk Status & Radar Chart.....	20

## **Report Summary**

Auditor’s Verdict .....	21
-------------------------	----

## **Legal Advisory**

Important Disclaimer .....	22
About InterFi Network.....	23



# Project Overview

InterFi was consulted by Day of Defeat on October 03, 2021 to conduct a smart contract security audit of their token source code.

DOD (Day of Defeat) is a token issued on the Binance Smart Chain. It is first and exciting social experiment on this planet, with a radical deflationary mathematical model which will keep the price of DOD token rising continuously. The team of DOD has fixed the first and final price in the smart contract mathematically. Therefore, all final holders will get 2,300,000X gains.

A prize fund pool will be controlled by the smart contract. At the end of project, the prize fund pool will reach 100,000,000 BUSD while 1,000,000,000 DOD token left. At that point, all token holders can swap their DOD for BUSD at the rate 1 DOD = 0.1 BUSD. Therefore, the project will be able to deliver projected 2,300,000X gains.

<b>Project</b>	DAY OF DEFEAT
<b>Blockchain</b>	Binance Smart Chain / Binance Blockchain Explorer
<b>Language</b>	Solidity
<b>Contract</b>	0xc709878167Ed069Aea15FD0bD4E9758CEb4Da193
<b>Website</b>	<a href="https://www.dayofdefeat.io/">https://www.dayofdefeat.io/</a>
<b>Twitter</b>	<a href="https://twitter.com/dayofdefeatbsc">https://twitter.com/dayofdefeatbsc</a>
<b>Telegram</b>	<a href="https://t.me/DayOfDefeatBSC">https://t.me/DayOfDefeatBSC</a>
<b>Reddit</b>	<a href="https://www.reddit.com/r/DayOfDefeatBSC/">https://www.reddit.com/r/DayOfDefeatBSC/</a>



## **Token Logo**



## **Project Logo**



# InterFi

Smart Contract  
Security Audit

## **Solidity Source Code On InterFi GitHub**

<https://github.com/interfinetwork/audited-codes/blob/main/DayOfDefeat.sol>

## **GitHub Commits**

Solidity source code committed at: a36cdf010e129b56c562ef8658fbc7ed75ceeb59



**Contract Source Code On Blockchain (BscScan Verified With Exact Match)**

<https://bscscan.com/address/0xc709878167ed069aea15fd0bd4e9758ceb4da193#code#L1>

Contract Name: DODToken

Compiler Version: v0.6.12+commit.27d51765

Optimization Enabled: Yes with 200 runs

InterFi

.....

Smart Contract  
Security Audit



# Audit Scope & Methodology

The scope of this report is to audit the smart contract source code of Day of Defeat. The source code can be viewed in its entirety on

<https://github.com/interfinetwork/audited-codes/blob/main/DayOfDefeat.sol>

InterFi has scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

## Category

---

### Smart Contract Vulnerabilities

- ❖ Re-entrancy (RE)
- ❖ Unhandled Exceptions (UE)
- ❖ Transaction Order Dependency (TO)
- ❖ Integer Overflow (IO)
- ❖ Unrestricted Action (UA)
- ❖ Ownership Takeover
- ❖ Gas Limit and Loops

### Source Code Review

- ❖ Deployment Consistency
- ❖ Repository Consistency
- ❖ Data Consistency
- ❖ Token Supply Manipulation
- ❖ Access Control and Authorization
- ❖ Operations Trail and Event Generation

### Functional Assessment

- ❖ Assets Manipulation
- ❖ Liquidity Access



## **InterFi's Echelon Audit Standard**

The aim of InterFi's "Echelon" standard is to analyze the smart contract and identify the vulnerabilities and the hacks in the smart contract. Mentioned are the steps used by ECHELON-1 to assess the smart contract:

1. Solidity smart contract source code reviewal:
  - ❖ Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, scope, and functionality of the smart contract.
  - ❖ Manual review of code, which is the process of reading source code line-byline to identify potential vulnerabilities.
2. Static, Manual, and Automated AI analysis:
  - ❖ Test coverage analysis, which is the process of determining whether the test cases are covering the code and how much code is exercised when we run those test cases.
  - ❖ Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts

## **Automated 3P frameworks used to assess the smart contract vulnerabilities**

- ❖ Slither
- ❖ Consensys MythX
- ❖ Consensys Surya
- ❖ Open Zeppelin Code Analyzer
- ❖ Solidity Code Compiler





# InterFi's Risk Classification

Smart contracts are generally designed to manipulate and hold funds denominated in ETH/BNB. This makes them very tempting attack targets, as a successful attack may allow the attacker to directly steal funds from the contract. Below are the typical risk levels of a smart contract:

**Vulnerable:** A contract is vulnerable if it has been flagged by a static analysis tool as such. As we will see later, this means that some contracts may be vulnerable because of a false-positive.

**Exploitable:** A contract is exploitable if it is vulnerable and the vulnerability could be exploited by an external attacker. For example, if the "vulnerability" flagged by a tool is in a function which requires to own the contract, it would be vulnerable but not exploitable.

**Exploited:** A contract is exploited if it received a transaction on the main network which triggered one of its vulnerabilities. Therefore, a contract can be vulnerable or even exploitable without having been exploited.

Risk severity	Meaning
<b>! Critical</b>	This level vulnerabilities could be exploited easily, and can lead to asset loss, data loss, asset manipulation, or data manipulation. They should be fixed right away.
<b>! High</b>	This level vulnerabilities are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to critical risk severity
<b>! Medium</b>	This level vulnerabilities are should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution.
<b>! Low</b>	This level vulnerabilities can be ignored. They are code style violations, and informational statements in the code. They may not affect the smart contract execution







# Smart Contract – Overview

## Contract information
















Query	Result
<b>Name</b>	Day Of Defeat
<b>Symbol</b>	DOD
<b>Decimals</b>	18
<b>Total Supply</b>	100,000,000,000,000
<b>Owner</b>	0x98ac817934eb66de820bfac7fc7b478b69d6895d
<b>Total Fees</b>	19
<b>Deployer Address (D)</b>	0x98aC817934eb66dE820bfac7FC7b478B69d6895D
<b>Team Address (T)</b>	0xE74A502705737F9DaFACd53e5f69bC7A5ECa277C
<b>Partner Address (P)</b>	0x5F348d70d5d1319BBc63D78b5cc81BC732797D87
<b>Consultant Address (C)</b>	0x9DF117Fd6153DCE120bE2655caAb1534b1fbA369
<b>Airdrop Address (AD)</b>	0x9a76E45d054F4C07B89F48f54635771AD7b75Ac8
<b>Transition Address (A)</b>	0xD9b8F8A4602047C67F99CD11a6e1671819446Db3
<b>Marketing Address (M)</b>	0xE0541091e68cae9BEBC988B6a642Beb039e8BA0a
<b>BUSD Address</b>	0xe9e7CEA3DedcA5984780Bafc599bD69ADd087D56



# Smart Contract – Static Analysis

Symbol	Meaning
	Function can be modified
	Function is payable
	Function is locked
	Function can be accessed
!	Important functionality

```

| **IBEP20** | 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 ! |
| | | |
| **SafeMath** | Library |   |
| L | add | Internal  |   |
| L | sub | Internal  |   |
| L | sub | Internal  |   |
| L | mul | Internal  |   |
| L | div | Internal  |   |
| L | div | Internal  |   |
| | | |
| **Context** | Implementation |   |
| L | _msgSender | Internal  |   |
| | | |
| **Address** | Library |   |
| L | isContract | Internal  |   |
| | | |
| **Ownable** | Implementation | Context |
| L | <Constructor> | Internal  |  |
| L | owner | Public ! |   |NO ! |
| L | renounceOwnership | Public ! |  | onlyOwner |
| L | transferOwnership | Public ! |  | onlyOwner |
| | | |
| **BEP20** | Implementation | Context, Ownable, IBEP20 |
| 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 | increaseAllowance | Public ! | ● | NO ! |
| L | decreaseAllowance | Public ! | ● | NO ! |
| L | checklock | Internal 🔒 | ● | |
| L | swap | Public ! | ● | NO ! |
| L | _transfer | Internal 🔒 | ● | |
| L | _approve | Internal 🔒 | ● | |
|||||
| **BEP20Detailed** | Implementation | BEP20 |||
| L | <Constructor> | Internal 🔒 | ● | |
| L | name | Public ! | | NO ! |
| L | symbol | Public ! | | NO ! |
| L | decimals | Public ! | | NO ! |
|||||
| **D00Token** | Implementation | BEP20Detailed |||
| L | <Constructor> | Public ! | ● | BEP20Detailed |
| L | takeOutTokenInCase | Public ! | ● | onlyOwner |

```

## Smart Contract Security Audit



# Smart Contract – Software Analysis

## Function Signatures

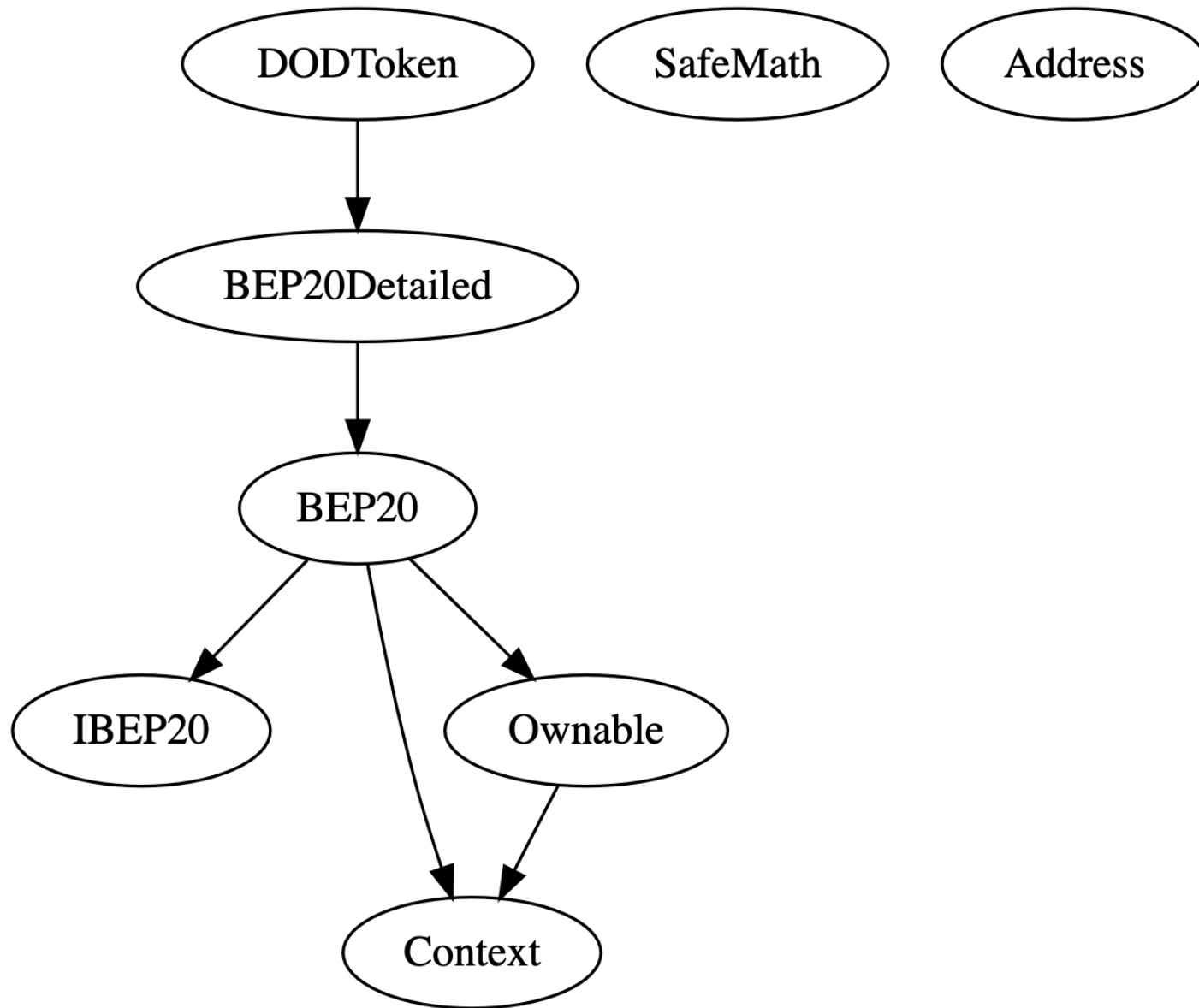
```

16279055 => isContract(address)
39509351 => increaseAllowance(address,uint256)
18160ddd => totalSupply()
70a08231 => balanceOf(address)
a9059cbb => transfer(address,uint256)
dd62ed3e => allowance(address,address)
095ea7b3 => approve(address,uint256)
23b872dd => transferFrom(address,address,uint256)
771602f7 => add(uint256,uint256)
b67d77c5 => sub(uint256,uint256)
e31bdc0a => sub(uint256,uint256,string)
c8a4ac9c => mul(uint256,uint256)
a391c15b => div(uint256,uint256)
b745d336 => div(uint256,uint256,string)
119df25f => _msgSender()
8da5cb5b => owner()
715018a6 => renounceOwnership()
f2fde38b => transferOwnership(address)
a457c2d7 => decreaseAllowance(address,uint256)
f9aae68c => checklock()
94b918de => swap(uint256)
30e0789e => _transfer(address,address,uint256)
104e81ff => _approve(address,address,uint256)
06fdde03 => name()
95d89b41 => symbol()
313ce567 => decimals()
8c76dc93 => takeOutTokenInCase(address,uint256,address)

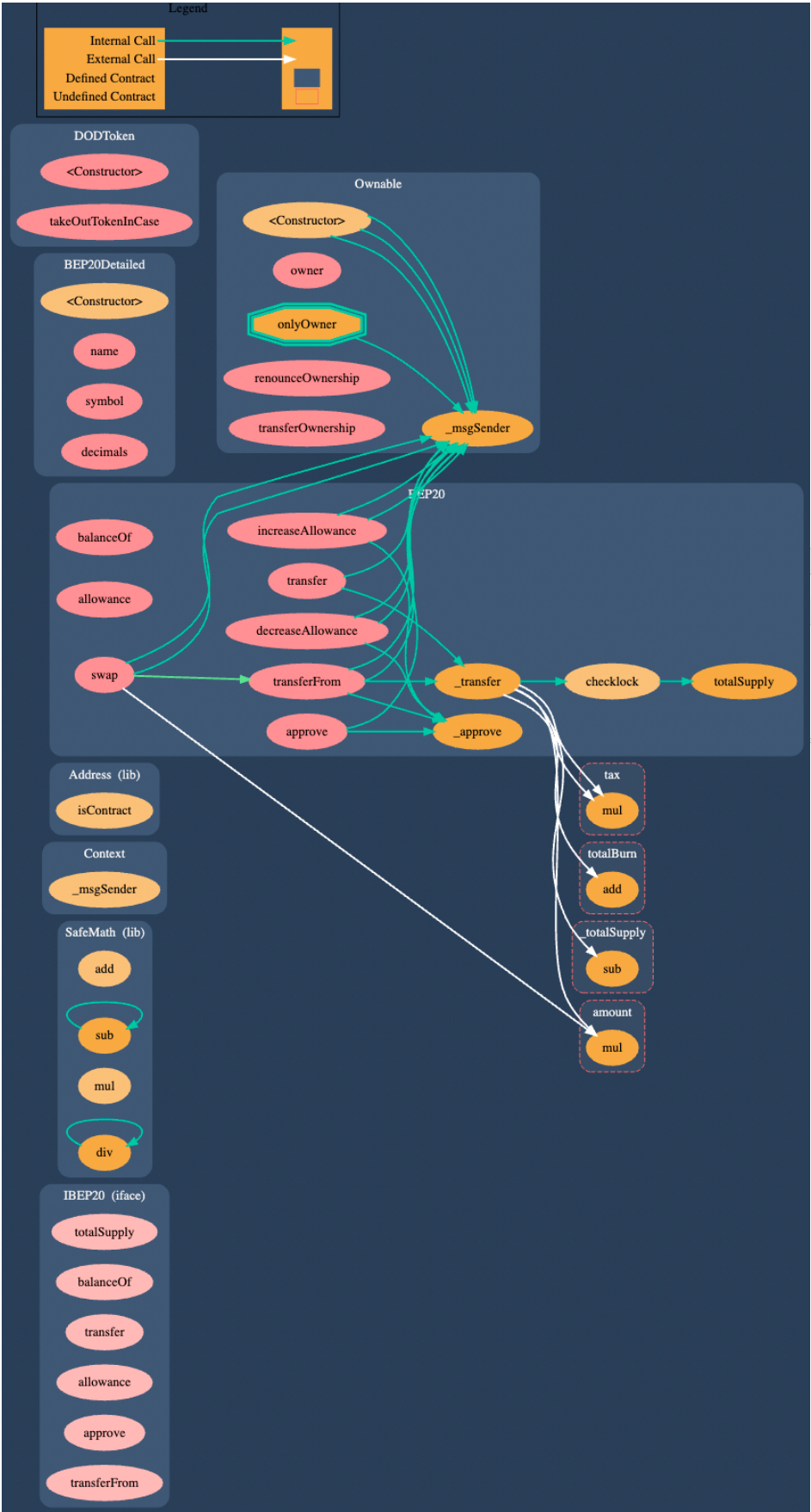
```



## Inheritance Graph



Callout Graph



# Smart Contract – Manual Analysis

Function	Description	Tested	Verdict
<b>TotalSupply</b>	provides information about the total token supply	Yes	<b>Passed</b>
<b>BalanceOf</b>	provides account balance of the owner's account	Yes	<b>Passed</b>
<b>Transfer</b>	executes transfers of a specified number of tokens to a specified address	Yes	<b>Passed</b>
<b>TransferFrom</b>	executes transfers of a specified number of tokens from a specified address	Yes	<b>Passed</b>
<b>Approve</b>	allow a spender to withdraw a set number of tokens from a specified account	Yes	<b>Passed</b>
<b>Allowance</b>	returns a set number of tokens from a spender to the owner	Yes	<b>Passed</b>
<b>burn</b>	executes transfers of a specified number of tokens to a burn address	Yes	<b>Passed</b>

## Verified

Active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.

- ❖ Active Owner: 0x98ac817934eb66de820bfac7fc7b478b69d6895d
- ❖ Owner can mint tokens at token launch.
- ❖ Owner can-not lock or burn user assets.
- ❖ Owner uses "takeOutTokenInCase" function. According to the project team, this token will be utilized only if there's any remaining BUSD left in the fund pool at the end of the project.





## Important Information

Day of Defeat smart contract utilizes the “SafeMath” to prevent known vulnerabilities.

```
string private _name = 'Day Of Defeat';
string private _symbol = 'DOD';
uint8 private _decimals = 18;

library SafeMath {
function add(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a + b;
    require(c >= a, 'SafeMath: addition overflow');

    return c;
}
function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    return sub(a, b, 'SafeMath: subtraction overflow');
}
uint256 c = a * b;
require(c / a == b, 'SafeMath: multiplication overflow');

    return c;
}
}
```

## Smart Contract

Day of Defeat uses “takeOutTokenInCase” function. According to the project team, this token will be utilized only if there’s any remaining BUSD left in the fund pool at the end of the project.

```
function takeOutTokenInCase(address _token, uint256 _amount, address _to) public onlyOwner {
    require(!isLocked, "Token contract is locked");
    IBEP20(_token).transfer(_to, _amount);
}
}
```

Day of Defeat smart contract has 1 low severity issues which may or may not create any functional vulnerability.

- ❖ "Expected pragma, import directive or contract/interface/library definition"



# Smart Contract – SWC Attacks

SWC ID	Description	Verdict
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	! Low
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Withdrawal	! Low
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
SWC-107	Re-entrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegate Call to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-116	Block values as a proxy for time	Passed
SWC-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed

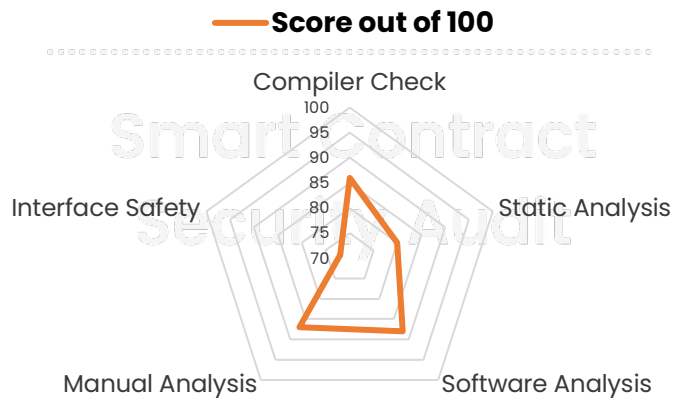


<b>SWC-119</b>	Shadowing State Variables	<b>Passed</b>
<b>SWC-120</b>	Weak Sources of Randomness from Chain Attributes	<b>Passed</b>
<b>SWC-121</b>	Missing Protection against Signature Replay Attacks	<b>Passed</b>
<b>SWC-122</b>	Lack of Proper Signature Verification	<b>Passed</b>
<b>SWC-123</b>	Requirement Violation	<b>Passed</b>
<b>SWC-124</b>	Write to Arbitrary Storage Location	<b>Passed</b>
<b>SWC-125</b>	Incorrect Inheritance Order	<b>Passed</b>
<b>SWC-126</b>	Insufficient Gas Griefing	<b>Passed</b>
<b>SWC-127</b>	Arbitrary Jump with Function Type Variable	<b>Passed</b>
<b>SWC-128</b>	DoS With Block Gas Limit	<b>Passed</b>
<b>SWC-129</b>	Typographical Error	<b>Passed</b>
<b>SWC-130</b>	Right-To-Left-Override control character (U+202E)	<b>Passed</b>
<b>SWC-131</b>	Presence of unused variables	<b>Passed</b>
<b>SWC-132</b>	Unexpected Ether balance	<b>Passed</b>
<b>SWC-133</b>	Hash Collisions With Multiple Variable Length Arguments	<b>Passed</b>
<b>SWC-134</b>	Message call with hardcoded gas amount	<b>Passed</b>
<b>SWC-135</b>	Code With No Effects (Irrelevant/Dead Code)	<b>Passed</b>
<b>SWC-136</b>	Unencrypted Private Data On-Chain	<b>Passed</b>



# Smart Contract - Risk Status & Radar Chart

Risk Severity	Status
<b>! Critical</b>	None critical severity issues identified
<b>! High</b>	None high severity issues identified
<b>! Medium</b>	None medium severity issues identified
<b>! Low</b>	2 Low severity issues identified
<b>Passed</b>	40 functions and instances verified and passed



Compiler Check 86

Static Analysis 80

Software Analysis 88

Manual Analysis 87

Interface Safety 72



## Auditor's Verdict

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks.

**Day Of Defeat's token smart contract source code has MEDIUM RISK SEVERITY.**

# InterFi

## Smart Contract Security Audit

### **NOTE:**

- ❖ **Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.**
- ❖ **Owner or developer KYC isn't checked and verified due to out of scope.**
- ❖ Project's liquidity pair isn't checked and verified due to out of scope.
- ❖ Project website is not checked due to out of scope. The website hasn't been reviewed for SSL and lighthouse report.



# Important Disclaimer

InterFi Network provides contract auditing and project verification services for blockchain projects. The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project. **This report should not be transmitted, disclosed, referred to, or relied upon by any person for any purposes without InterFi's prior written consent.**

InterFi provides the easy-to-understand assessment of the project, and the smart contract (otherwise known as the source code). The audit makes no statements or warranties on the security of the code. It also cannot be considered as an enough assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have used all the data at our disposal to provide the transparent analysis, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. **Be aware that smart contracts deployed on a blockchain aren't resistant from external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security. Therefore, InterFi does not guarantee the explicit security of the audited smart contract.**

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.

**This report should not be considered as an endorsement or disapproval of any project or team.**

The information provided on this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. Do conduct your own due diligence and consult your financial advisor before making any investment decisions.



# About InterFi Network

InterFi Network provides intelligent blockchain solutions. InterFi is developing an ecosystem that is seamless and responsive. Some of our services: Blockchain Security, Token Launchpad, NFT Marketplace, etc. **InterFi's mission is to interconnect multiple services like Blockchain Security, DeFi, Gaming, and Marketplace under one ecosystem that is seamless, multi-chain compatible, scalable, secure, fast, responsive, and easy-to-use.**

InterFi is built by a decentralized team of UI experts, contributors, engineers, and enthusiasts from all over the world. Our team currently consists of 6+ core team members, and 10+ casual contributors. **InterFi provides manual, static, and automatic smart contract analysis, to ensure that project is checked against known attacks and potential vulnerabilities.**

To learn more, visit <https://interfi.network>

To view our audit and KYC portfolio, visit <https://github.com/interfinetwork>

To book an audit or KYC, message <https://t.me/interfiaudits>





**@INTERFINETWORK**

**RELENTLESSLY SECURING THE PUBLIC BLOCKCHAIN | MADE IN CANADA 🇨🇦**