# Shumi

2230101

hash 93c80b52ae0fb477dff2d0e8be2c4dcd6b64f7ce3d9039836fcd865b2465573d

url bscscan.com/address/0x1cABcd4B66d86D703866050f6430eA86b66188BB#code#F1#L793

solidity

# Introduction

Checks The Contract Code For Security Vulnerabilities And Bad Practices

## Vulnerability analysis

### High Severity Issues

✅ No high severity issues found

### Medium Severity Issues

✅ No medium severity issues found

### Low Severity Issues

⚠️ Old version of Solidity v0.8.0 and Low issues table presented below

finteh.org recommended

Upgrade to the current version v0.8.17

## Specific functionality of contract

1. Tokens will be burned while tx
2. Deployer can enable/disable following state variable of ShumiToken:
   a. antisnipeDisable

   b. AntisnipeAddress
   c. marketingWallet
   d. TaxFeePercent
   e. LiquidityFeePercent
   f. MarketingFeePercent
   g. BurnFeePercent
   h. SellBurnFeePercent
   i. SellMarketingFeePercent
   j. SellLiquidityFeePercent
   k. SellTaxFeePercent
   l. MaxHoldingPercents
   m. SwapAndLiquifyEnabled
   n. AntiWhale
   o. AntiBot
   p. _isExcludedFromFee
   q. _isExcluded
   r. _excluded
   s. _included

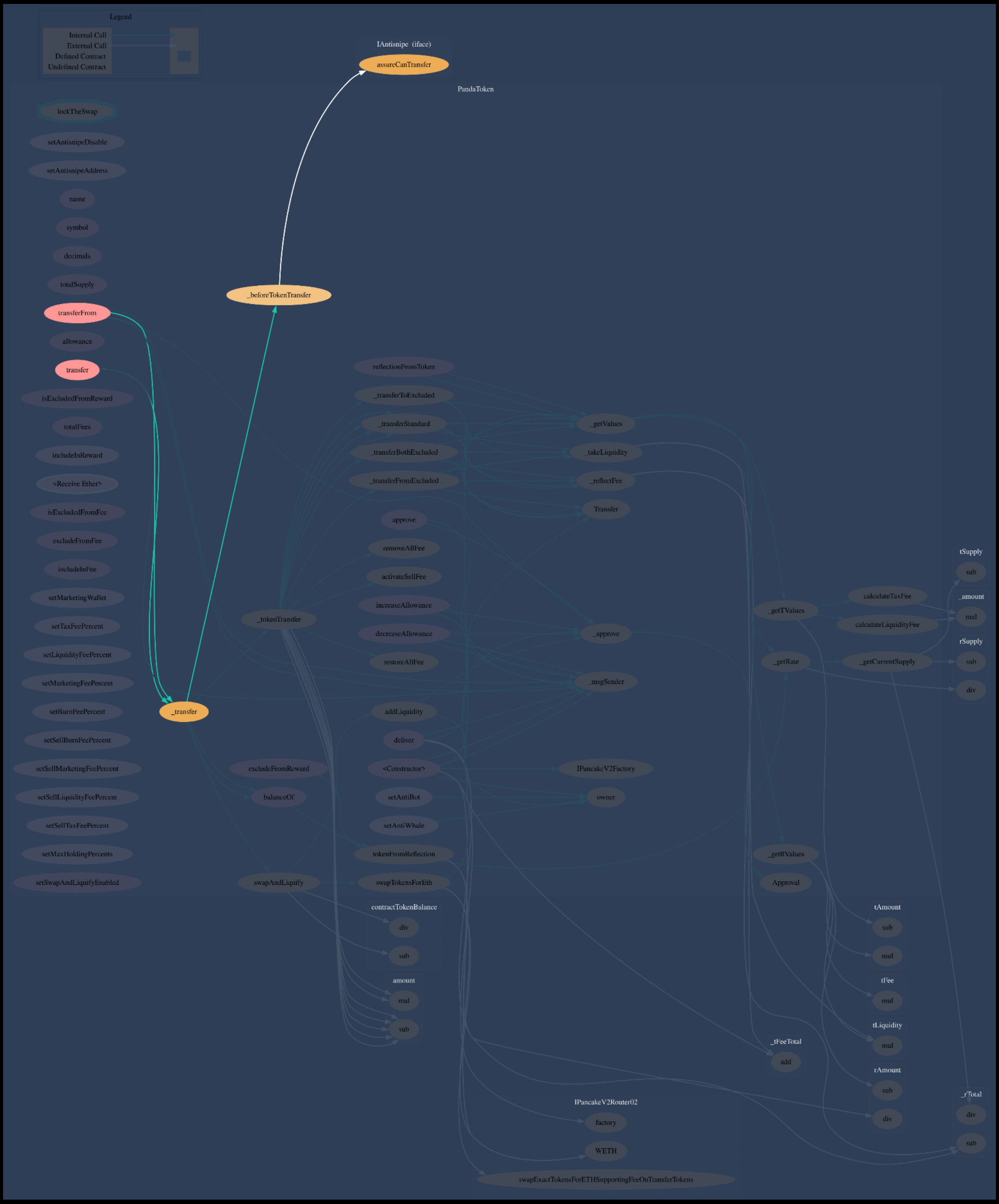
3. Deployer can set following addresses of ShumiToken:
   a. IPancakeV2Pair.sol
   b. IPancakeV2Router
   c. IPancakeV2Factory

4. Existing Modifiers:
    a. onlyRegistered
    b. lockTheSwap
5. If an address is excluded from reward it cannot call the deliver function
6. Liquidity will be added to the owner

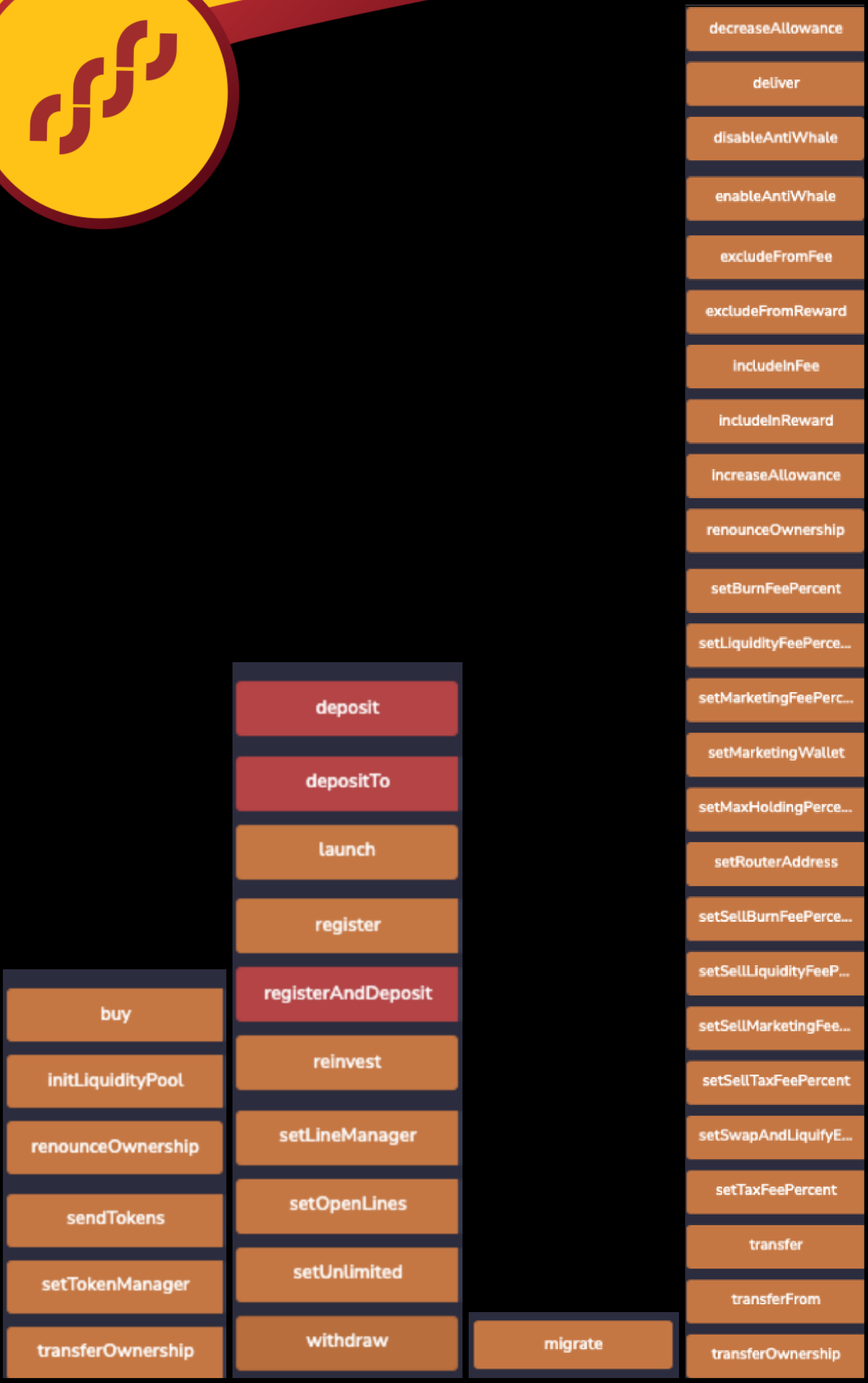
## Low issues

| Issue | File | Type | Description |
|---|---|---|---|
| 1 | All | A floating pragma is set | The current pragma Solidity directive is not a certain one. |
| 2 | ShumiToken | Missing Zero Address Validation (missing-zero-check) | Check that the address is not zero |
| 3 | ShumiToken | State variable visibility is not set | It is best practice to set the visibility of state variables explicitly |
| 4 | ShumiToken | Local variables shadowing | Rename the local variables that shadow another component |
| 5 | ShumiToken | Missing Events Arithmetic | Emit an event for critical parameter changes |

Table 1.1



1.1 Main scheme of contract Shumi



1.2 Write functions of contract

## SWC Attacks

| ID | Title | Relationships | Passed |
|---|---|---|---|
| SWC-136 | Unencrypted Private Data On-Chain | CWE-767: Access to Critical Private Variable via Public Method | ✅ |
| SWC-135 | Code With No Effects | CWE-1164: Irrelevant Code | ✅ |
| SWC-134 | Message call with hardcoded gas amount | CWE-655: Improper Initialization | ✅ |
| SWC-133 | Hash Collisions With Multiple Variable Length Arguments | CWE-294: Authentication Bypass by Capture-replay | ✅ |
| SWC-132 | Unexpected Ether balance | CWE-667: Improper Locking | ✅ |
| SWC-131 | Presence of unused variables | CWE-1164: Irrelevant Code | ✅ |
| SWC-130 | Right-To-Left-Override control character (U+202E) | CWE-451: User Interface (UI) Misrepresentation of Critical Information | ✅ |
| SWC-129 | Typographical Error | CWE-480: Use of Incorrect Operator | ✅ |
| SWC-128 | DoS With Block Gas Limit | CWE-400: Uncontrolled Resource Consumption | ✅ |
| SWC-127 | Arbitrary Jump with Function Type Variable | CWE-695: Use of Low-Level Functionality | ✅ |
| SWC-126 | Insufficient Gas Griefing | CWE-691: Insufficient Control Flow Management | ✅ |

Table 2.1

| ID | Title | Relationships | Passed |
|---|---|---|---|
| SWC-125 | Incorrect Inheritance Order | CWE-696: Incorrect Behaviour Order | ✅ |
| SWC-124 | Write to Arbitrary Storage Location | CWE-123: Write-what-where Condition | ✅ |
| SWC-123 | Requirement Violation | CWE-573: Improper Following of Specification by Caller | ✅ |
| SWC-122 | Lack of Proper Signature Verification | CWE-345: Insufficient Verification of Data Authenticity | ✅ |
| SWC-121 | Missing Protection against Signature Replay Attacks | CWE-347: Improper Verification of Cryptographic Signature | ✅ |
| SWC-120 | Weak Sources of Randomness from Chain Attributes | CWE-330: Use of Insufficiently Random Values | ✅ |
| SWC-119 | Shadowing State Variables | CWE-710: Improper Adherence to Coding Standards | ⛔ |
| SWC-118 | Incorrect Constructor Name | CWE-665: Improper Initialization | ✅ |
| SWC-117 | Signature Malleability | CWE-347: Improper Verification of Cryptographic Signature | ✅ |
| SWC-116 | Block values as a proxy for time | CWE-829: Inclusion of Functionality from Untrusted Control Sphere | ✅ |
| SWC-115 | Authorization through tx.origin | CWE-477: Use of Obsolete Function | ✅ |
| SWC-114 | Transaction Order Dependence | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronisation ('Race Condition') | ✅ |
| SWC-113 | DoS with Failed Call | CWE-703: Improper Check or Handling of Exceptional Conditions | ✅ |

Table 2.2

| ID | Title | Relationships | Passed |
|---|---|---|---|
| SWC-112 | Delegatecall to Untrusted Callee | CWE-829: Inclusion of Functionality from Untrusted Control Sphere | ✅ |
| SWC-111 | Use of Deprecated Solidity Functions | CWE-477: Use of Obsolete Function | ✅ |
| SWC-110 | Assert Violation | CWE-670: Always-Incorrect Control Flow Implementation | ✅ |
| SWC-109 | Uninitialized Storage Pointer | CWE-824: Access of Uninitialized Pointer | ✅ |
| SWC-108 | State Variable Default Visibility | CWE-710: Improper Adherence to Coding Standards | ⛔ |
| SWC-107 | Reentrancy | CWE-841: Improper Enforcement of Behavioural Workflow | ✅ |
| SWC-106 | Unprotected SELF DESTRUCT Instruction | CWE-284: Improper Access Control | ✅ |
| SWC-105 | Unprotected Ether Withdrawal | CWE-284: Improper Access Control | ✅ |
| SWC-104 | Unchecked Call Return Value | CWE-252: Unchecked Return Value | ✅ |
| SWC-103 | Floating Pragma | CWE-664: Improper Control of a Resource Through its Lifetime | ⛔ |
| SWC-102 | Outdated Compiler Version | CWE-937: Using Components with Known Vulnerabilities | ✅ |
| SWC-101 | Integer Overflow and Underflow | CWE-682: Incorrect Calculation | ✅ |
| SWC-100 | Function Default Visibility | CWE-710: Improper Adherence to Coding Standards | ✅ |

Table 2.3

**Backdoor for investor funds can be withdrawn by not owner**

**Bugs allowing to steal money from the contract**

**were not detected in this code**

Non-governmental organization
FINTEH
FINTECH ASSOCIATION
Warsaw