



SOLIDProof
Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

MaxxFinance Audit

Security Assessment
08.December,2022

For

MAXX
FINANCE



[SolidProof.io](https://solidproof.io)



[@solidproof_io](https://t.me/solidproof_io)

Disclaimer	2
Description	5
Project Engagement	5
Logo	5
Contract Link	5
Methodology	7
Used Code from other Frameworks/Smart Contracts (direct imports)	8
Tested Contract Files	9
Source Lines	10
Risk Level	10
Capabilities	11
Inheritance Graph	12
CallGraph	13
Scope of Work/Verify Claims	14
Modifiers and public functions	24
Source Units in Scope	26
Critical issues	27
High issues	27
Medium issues	27
Low issues	27
Informational issues	28
Audit Comments	28
SWC Attacks	29

Disclaimer

SolidProof.io reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc’...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof’s position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	26.September,2022	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary
1.1	08.December,2022	<ul style="list-style-type: none">• Reaudit

Network
Polygon

Website
<https://maxx.finance/>

Twitter
<https://twitter.com/MaxxFinance>

Telegram
<https://t.me/maxxfinance>

Discord
<https://discord.com/invite/JtenbACKec>

Reddit
<https://www.reddit.com/r/MaxxFinance>

Medium
<https://maxxfinance.medium.com/>

YouTube
<https://www.youtube.com/MaxxFinance>

Instagram
<https://www.instagram.com/maxxfinance/>

Facebook
<https://www.facebook.com/MaxxFinanceOfficial>

Description

MAXX Finance radically transforms the traditional concept of 'time deposits/certificate of deposits' on the blockchain as a completely fair and transparent DeFi protocol. We stand for trust, transparency, and sustainability of decentralized finance.

The platform will allow participants to earn a high, consistent, and sustainable interest rate by staking their \$MAXX tokens. The interest paid to stakers varies based on the amount staked, duration, and any bonuses used when creating the stake. This allows for larger returns anywhere between 18-80% APY plus additional dividends from the . Once a stake is created, its APY is locked in for the duration, and will not fluctuate. The returns are guaranteed, unlike most other projects.

Project Engagement

During the 26th of September 2022, **Maxx Finance** team engaged Solidproof.io to audit the smart contracts that they created. The engagement was technical in nature and focused on identifying the security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

Logo



Contract Links

v1.0

Provided as files

v1.1

<https://github.com/MaxxFinance/maxx-finance>

Commit: 8009aa9175edcb9f3fe8d5a884beb0bb46e3dd38

:

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
 - ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
2. Testing and automated analysis that includes the following:
 - i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
 - ii) Symbolic execution, which is analyzing 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.

Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:

Dependency / Import Path	Count
@openzeppelin/contracts/access/AccessControl.sol	1
@openzeppelin/contracts/access/IAccessControl.sol	1
@openzeppelin/contracts/access/Ownable.sol	6
@openzeppelin/contracts/security/Pausable.sol	2
@openzeppelin/contracts/security/ReentrancyGuard.sol	2
@openzeppelin/contracts/token/ERC20/ERC20.sol	1
@openzeppelin/contracts/token/ERC20/IERC20.sol	1
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	1
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol	2
@openzeppelin/contracts/token/ERC721/ERC721.sol	3
@openzeppelin/contracts/token/ERC721/IERC721.sol	2
@openzeppelin/contracts/token/ERC721/extensions/ERC721Enumerable.sol	1
@openzeppelin/contracts/utils/Counters.sol	4
@openzeppelin/contracts/utils/cryptography/MerkleProof.sol	1
@openzeppelin/contracts/utils/introspection/ERC165Checker.sol	2
@openzeppelin/contracts/utils/structs/EnumerableSet.sol	1

Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

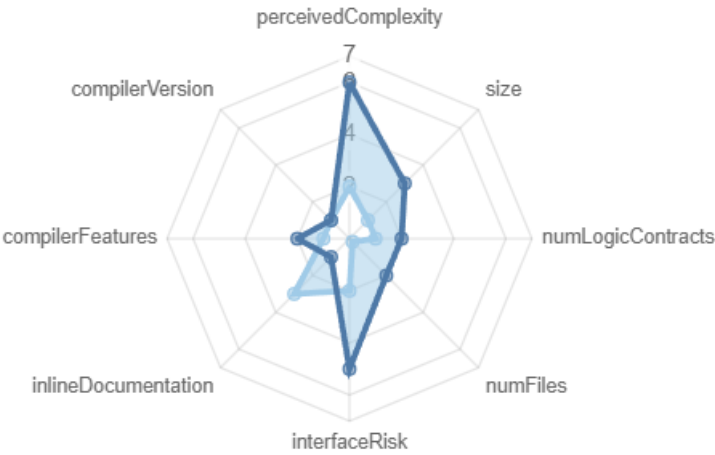
File Name	SHA-1 Hash
contracts/interfaces/IStake.sol	cefb7997ad59efa4b5051b2d8d75c25c103f9741
contracts/interfaces/IMaxxFinance.sol	35a320fca87a5ef3faf135c46d7c90543c7a6be8
contracts/interfaces/IMAXXBoost.sol	6fb1e47ae64d28f8edea4be3f5c6908e1f72058f
contracts/interfaces/ILiquidityAmplifier.sol	d8181d6ab37e8f62678f7968c7b0c8df7c9403d7
contracts/MaxxFinance.sol	e3eeac01771987295f406ac521c5e7aeea7d116f
contracts/LiquidityAmplifier.sol	3db569bcc453cdb9b4889cdc5f60a3e0c08e5984
contracts/Deployer.sol	e11078ccc08cc2c0e3ddf114feb562a508a60630
contracts/FreeClaim.sol	41025b0eb3a630fecc232d44ba6672a60d46ae71
contracts/MAXXGenesis.sol	10e6b73334bb9041e700fce288dc15c369485820
contracts/Marketplace.sol	aff09a688013cc24ddb666af95524bc96850786
contracts/MaxxStake.sol	de30b014675429be7282162c14b46cb734b8bba1
contracts/MAXXBoost.sol	a6d9727d2a9afbd5f28ff3db8dc9f9cd701862f3

Metrics

Source Lines v1.0







Risk Level v1.0



Capabilities

v1.0

Components

 Contracts	 Libraries	 Interfaces	 Abstract
8	0	4	0


Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.













 Public	 Payable
109	5

External	Internal	Private	Pure	View
94	99	0	2	40

StateVariables

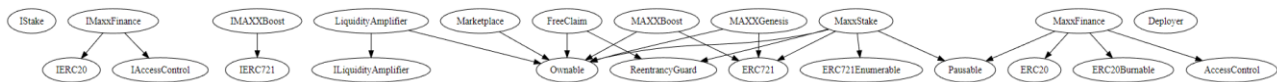
Total	 Public
104	90

Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts	
<input type="text" value="^0.8.0"/>		<input type="text" value="yes"/>	<input type="text" value="yes (1 asm blocks)"/>	<input type="text"/>	
 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRecover	 New/Create/Create2
<input type="text" value="yes"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="yes"/>	<input type="text"/>	<input type="text" value="yes"/> → <input type="text" value="AssemblyCall:Name:create2"/>
 TryCatch	 Unchecked				
<input type="text"/>	<input type="text" value="yes"/>				

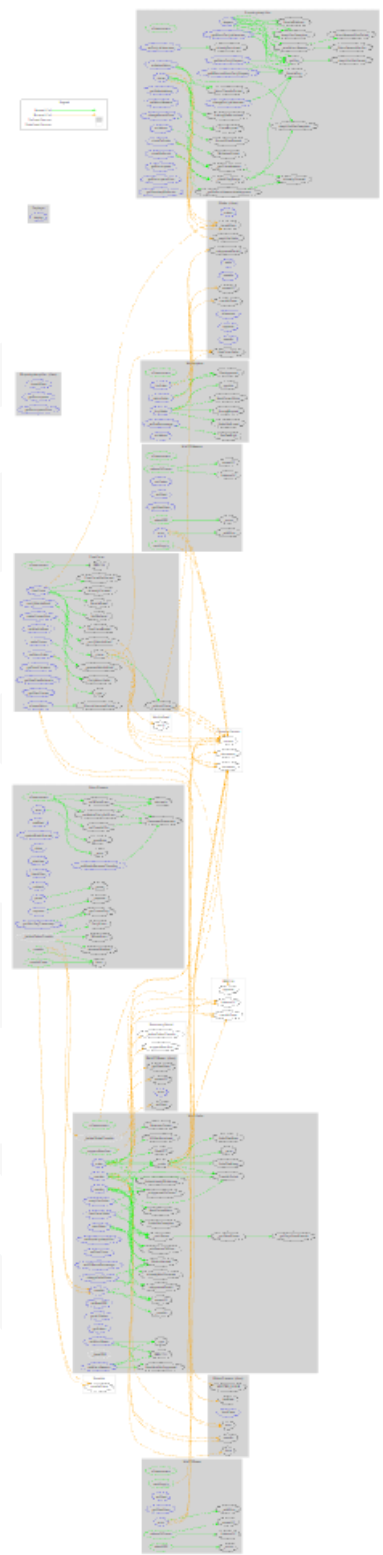
Inheritance Graph

v1.0



Call Graph

v1.0



Scope of Work/Verify Claims

The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Is contract an upgradeable
2. Correct implementation of Token standard
3. Deployer cannot mint any new tokens
4. Deployer cannot burn or lock user funds
5. Deployer cannot pause the contract
6. Deployer can set fees
7. Deployer can blacklist/antisnipe address
8. Overall checkup (Smart Contract Security)

Is contract an upgradeable

Name	
Is contract an upgradeable?	No



Correct implementation of Token standard

ERC20				
Function	Description	Exist	Tested	Verified
totalSupply	Provides information about the total token supply			
balanceOf	Provides account balance of the owner's account			
transfer	Executes transfers of a specified number of tokens to a specified address			
transferFrom	Executes transfers of a specified number of tokens from a specified address			
approve	Allow a spender to withdraw a set number of tokens from a specified account			
allowance	Returns a set number of tokens from a spender to the owner			

Write functions of contracts v1.0

FreeClaim

- ◆ freeClaim
- ◆ allocateMaxx
- ◆ setMaxxStake
- ◆ setMerkleRoot
- ◆ stakeClaims
- ◆ stakeClaimsSlice

MaxxGenesis

- ◆ mint
- ◆ setCodes
- ◆ setUsed

MaxxFinance

- ◆ mint
- ◆ addPool
- ◆ setTransferTax
- ◆ setBlocksBetweenTransfers
- ◆ updateBlockLimited
- ◆ allow
- ◆ disallow
- ◆ blockUser
- ◆ unblock
- ◆ pause
- ◆ unpause
- ◆ transfer
- ◆ transferFrom
- ◆ setGlobalDailySellLimit
- ◆ setWhaleLimit

Marketplace

- ◆ listStake
- ◆ delistStake
- ◆ buyStake 💰
- ◆ setFeePercentage
- ◆ withdraw

LiquidityAmplifier

- ◆ deposit 💰
- ◆ claim
- ◆ claimToStake
- ◆ claimReferrals
- ◆ setStakeAddress
- ◆ setMaxxGenesis
- ◆ setDailyAllocations
- ◆ changeDailyAllocation
- ◆ changeLaunchDate
- ◆ withdraw
- ◆ withdrawMaxx

MaxxStake

- ◆ stake
- ◆ unstake
- ◆ maxShare
- ◆ restake
- ◆ transfer
- ◆ changeStakeName
- ◆ amplifierStake
- ◆ freeClaimStake
- ◆ setLiquidityAmplifier
- ◆ setFreeClaim
- ◆ setNftBonusPercentage
- ◆ setMaxxBoost
- ◆ setMaxxGenesis
- ◆ setBaseURI

Deployer cannot mint any new tokens

Name	Exist	Tested	Status
Deployer cannot mint			
Max / Total Supply	N/A		

Comments:

- Mint function in the MAXXGenesis contract can only be called by ampliferContract which will be set by the owner at the time of deployment.
- Every account with the “MINTER_ROLE” permission granted by owner can mint new tokens and also Maximum supply is also not set.
- Owner can mint NFTs for the lucky winner but not more than Maximum Supply

Deployer cannot burn or lock user funds

Name	Exist	Tested	Status
Deployer cannot lock			
Deployer cannot burn			

Comments:

- Tokens will be burned automatically in the form of tax/penalty.

Deployer cannot pause the contract

Name	Exist	Tested	Status
Deployer cannot pause			

Comments:

- The account owner of the “DEFAULT_ADMIN_ROLE” can pause/unpause the MaxxFinance contract. It is possible by the other authorities for other contracts as well.

Deployer can set fees

Name	Exist	Tested	Status
Deployer can set fees over 25%			
Deployer can set fees to nearly 100% or more			

Comments:

- The fees can't be set to 20% or more by the owner because there is protection against it.

Deployer cannot blacklist/antisnipe addresses

Name	Exist	Tested	Status
Deployer can blacklist/antisnipe addresses			



Overall checkup (Smart Contract Security)

Tested	Verified

Legend

Attribute	Symbol
Verified / Checked	
Partly Verified	
Unverified / Not checked	
Not available	

Modifiers and public functions

v1.0

FreeClaim

- ◆ freeClaim
- Ⓜ nonReentrant
- ◆ allocateMaxx
- Ⓜ onlyOwner
- ◆ setMaxxStake
- Ⓜ onlyOwner
- ◆ setMerkleRoot
- Ⓜ onlyOwner
- ◆ stakeClaims
- ◆ stakeClaimsSlice

MaxxGenesis

- ◆ mint
- ◆ setCodes
- Ⓜ onlyOwner
- ◆ setUsed

MaxxFinance

- ◆ mint
- Ⓜ whenNotPaused
- Ⓜ onlyRole
- ◆ addPool
- Ⓜ onlyRole
- ◆ setTransferTax
- Ⓜ onlyRole
- ◆ setBlocksBetweenTransfers
- Ⓜ onlyRole
- ◆ updateBlockLimited
- Ⓜ onlyRole
- ◆ allow
- Ⓜ onlyRole
- ◆ disallow
- Ⓜ onlyRole
- ◆ blockUser
- Ⓜ onlyRole
- ◆ unblock
- Ⓜ onlyRole
- ◆ pause
- Ⓜ onlyRole
- ◆ unpause
- Ⓜ onlyRole
- ◆ transfer
- Ⓜ whenNotPaused
- ◆ transferFrom
- Ⓜ whenNotPaused
- ◆ setGlobalDailySellLimit
- Ⓜ onlyRole
- ◆ setWhaleLimit
- Ⓜ onlyRole

Marketplace

- ◆ listStake
- ◆ delistStake
- ◆ buyStake 💰
- ◆ setFeePercentage
- Ⓜ onlyOwner
- ◆ withdraw
- Ⓜ onlyOwner

MaxxStake

- ◆ stake
- ◆ unstake
- ◆ maxShare
- ◆ restake
- Ⓜ nonReentrant
- ◆ transfer
- ◆ changeStakeName
- ◆ amplifierStake
- ◆ freeClaimStake
- ◆ setLiquidityAmplifier
- Ⓜ onlyOwner
- ◆ setFreeClaim
- Ⓜ onlyOwner
- ◆ setNftBonusPercentage
- Ⓜ onlyOwner
- ◆ setMaxxBoost
- Ⓜ onlyOwner
- ◆ setMaxxGenesis
- Ⓜ onlyOwner
- ◆ setBaseURI
- Ⓜ onlyOwner

LiquidityAmplifier

- ◆ deposit 💰
- ◆ claim
- ◆ claimToStake
- ◆ claimReferrals
- ◆ setStakeAddress
- Ⓜ onlyOwner
- ◆ setMaxxGenesis
- Ⓜ onlyOwner
- ◆ setDailyAllocations
- Ⓜ onlyOwner
- ◆ changeDailyAllocation
- Ⓜ onlyOwner
- ◆ changeLaunchDate
- Ⓜ onlyOwner
- ◆ withdraw
- Ⓜ onlyOwner
- ◆ withdrawMaxx
- Ⓜ onlyOwner

Comments:

Centralization Features:

- Add maximum allocation and set the Staking contract at any point of time
- Set Merkle Root and Hashed codes that can be used to mint NFTs
- Only maxxStake address can call the stakeClaims function but because the owner can update maxxStake address anytime, this means that owner can call the stakeClaim and stakeClaimsSlice functions because there are no checks to verify if the caller is a contract or not.
- Add Liquidity pool and set blocks between transfers but within a limit
- Include/Exclude contracts and wallets from allowList and also block/unblock users
- Set a global daily sell limit and a whale limit but within a range
- Withdraw the complete balance of the Marketplace and LiquidityAmplifier contracts
- Set new stake and genesis address
- Set/Update Daily Allocations, Maxx Genesis
- Set launch date but not after the initial launch date is passed.
- Set/Update liquidityAmplifier, maxGenesis, maxxBoost, addresses in the MaxxStake contract.

Source Units in Scope

v1.0

File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score
contracts/interfaces/IStake.sol	—————	1	68	20	15	3	27
contracts/interfaces/IMaxxFinance.sol	—————	1	28	15	7	14	13
contracts/interfaces/IMAXXBoost.sol	—————	1	13	8	4	2	9
contracts/interfaces/ILiquidityAmplifier.sol	—————	1	23	7	3	11	7
contracts/MaxxFinance.sol	1	—————	311	279	168	72	130
contracts/LiquidityAmplifier.sol	1	—————	533	508	339	105	289
contracts/Deployer.sol	1	—————	22	22	14	5	28
contracts/FreeClaim.sol	1	—————	346	314	206	56	129
contracts/MAXXGenesis.sol	1	—————	141	131	83	31	61
contracts/Marketplace.sol	1	—————	158	154	90	38	51
contracts/MaxxStake.sol	1	—————	650	598	392	139	223
contracts/MAXXBoost.sol	1	—————	131	121	76	29	53
Totals	8	4	2424	2177	1397	505	1020

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
nSLOC	normalized source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments
Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

Audit Results

AUDIT PASSED

Critical issues

No critical issues

High issues

No high issues

Medium issues

No medium issues

Low issues

No low issues

Informational issues

No Informational issues

Audit Comments

We recommend you to use the special form of comments (NatSpec Format, Follow link for more information <https://docs.soliditylang.org/en/v0.5.10/natspec-format.html>) for your contracts to provide rich documentation for functions, return variables and more. This helps investors to make clear what that variables, functions etc. do.

08. December, 2022:

- There is still an owner (Owner still has not renounced ownership).
- Make sure that the launch date is higher than block.timestamp in the MaxxStake contract

- The value of the “_effectiveMaticDailyDeposits[day]” must not be zero
- Read the whole report and modifiers section for more information.



SWC Attacks

ID	Title	Relationships	Status
SWC-1136	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SWC-1135	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SWC-1134	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SWC-1133	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SWC-1132	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SWC-1131	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED

131			
SWC-130	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SWC-129	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SWC-128	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED
SWC-127	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SWC-125	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SWC-1	Write to Arbitrary	CWE-123: Write-what-where Condition	PASSED

<u>1</u> <u>2</u> <u>4</u>	Storage Location		
<u>S</u> <u>W</u> <u>C</u> : <u>1</u> <u>2</u> <u>3</u>	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
<u>S</u> <u>W</u> <u>C</u> : <u>1</u> <u>2</u> <u>2</u>	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
<u>S</u> <u>W</u> <u>C</u> : <u>1</u> <u>2</u> <u>1</u>	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
<u>S</u> <u>W</u> <u>C</u> : <u>1</u> <u>2</u> <u>0</u>	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
<u>S</u> <u>W</u> <u>C</u> : <u>1</u> <u>1</u> <u>1</u> <u>9</u>	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	PASSED

S W C : 1 1 8	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
S W C : 1 1 7	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED
S W C : 1 1 6	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
S W C : 1 1 5	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
S W C : 1 1 4	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
S W C : 1 1 3	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED

S W C : 1 1 2	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
S W C : 1 1 1	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
S W C : 1 1 0	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
S W C : 1 0 9	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
S W C : 1 0 8	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
S W C : 1 0 7	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED

<div> <div>S</div> <div>W</div> <div>C</div> <div>.</div> <div>1</div> <div>1</div> <div>0</div> <div>0</div> <div>0</div> <div>1</div> </div>	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
--	-----------------------------------	---	--------





SolidProof.io



[@solidproof_io](https://t.me/solidproof_io)

Solid
Proofed

Blockchain Security | Smart Contract Audits | KYC


MADE IN GERMANY