



**SOLID**Proof  
*Bring trust into your projects*

**Blockchain Security | Smart Contract Audits | KYC**

MADE IN GERMANY

**v1.0: 24. November, 2021**

# Audit

**Security Assessment**  
**04. December, 2021**

**For**



Disclaimer	3
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
Scope of Work	13
Inheritance Graph	13
Verify Claims	14
OnlyOwner functions	21
CallGraph	23
Source Units in Scope	24
Critical issues	25
High issues	25
Medium issues	25
Low issues	25
Informational issues	25
Audit Comments	26
SWC Attacks	27

# 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	24. November 2021	<ul style="list-style-type: none"><li>• Layout project</li><li>• Automated- /Manual-Security Testing</li><li>• Summary</li></ul>
1.1	04. December 2021	<ul style="list-style-type: none"><li>• Reaudit</li></ul>

## **Network**

Binance Smart Chain (BEP20)

## **Website**

<https://pyrrhodefifi.com/>



## Description

TBA

## Project Engagement

During the 22nd of November 2021, **Pyrrho Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

## Logo



## Contract Link

### v1.0

<https://bscscan.com/address/0x557fd23cfd40db3bcc2066da2ad625d41087834b#code>

### v1.1

<https://bscscan.com/address/0xe6DF015f66653EcE085A5FBBa8d42C356114ce4F#code>

# 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)
<b>Critical</b>	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.
<b>High</b>	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.
<b>Medium</b>	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.
<b>Low</b>	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.
<b>Informational</b>	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 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.

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

Imported packages:

```
Context  
IERC20  
IUniswapV2Factory  
IUniswapV2Pair  
IUniswapV2Router01  
IUniswapV2Router02  
AntiSnipe
```



## 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

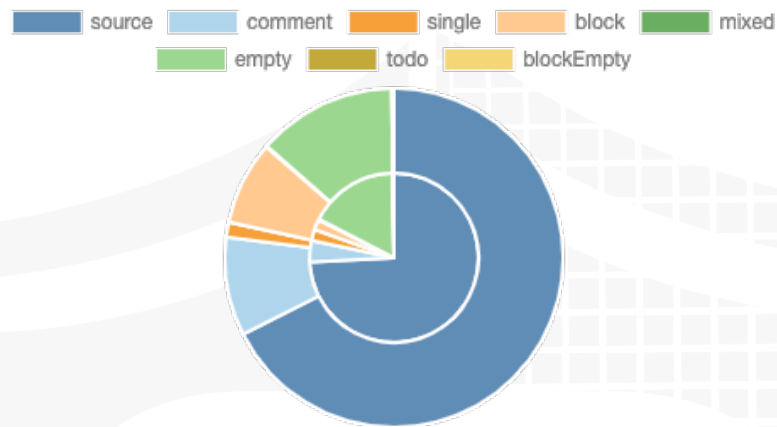
File Name	SHA-1 Hash
contracts/pyrrho.sol	3bd53ad4da18e761b9d57888d2a0b8c18a6cadf5

### v1.1

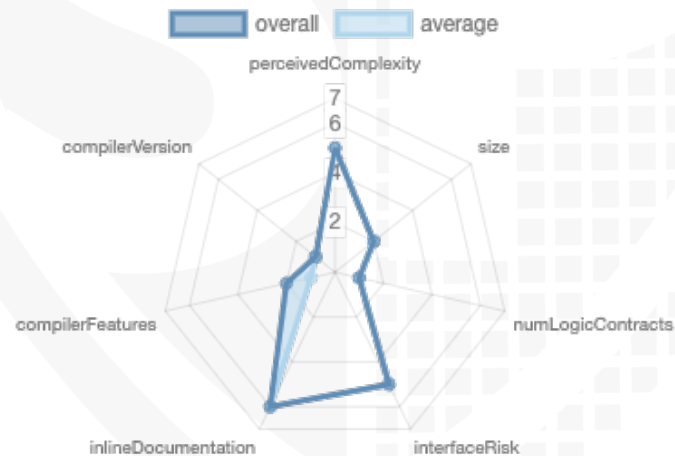
File Name	SHA-1 Hash
contracts/pyrrho.sol	157adf15a58cf610bd0e08dae64d0606c9ce8333

# Metrics

## Source Lines v1.0



## Risk Level v1.0



## Capabilities

### Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	1	0	6	1
1.1	1	0	5	1

### Exposed Functions

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

Version	Public	Payable
1.0	112	6
1.1	52	4

Version	External	Internal	Private	Pure	View
1.0	95	68	5	12	40
1.1	35	36	5	6	20

## State Variables

Version	Total	Public
1.0	42	13
1.1	38	14

## Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	<code>&gt;=0.6.0</code> <code>&lt;0.9.0</code>		yes	**** (0 asm blocks)	
1.1	<code>&gt;=0.8.0</code>		yes		

Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	ECRecover	New/Create/Create2
1.0	yes					

## Scope of Work

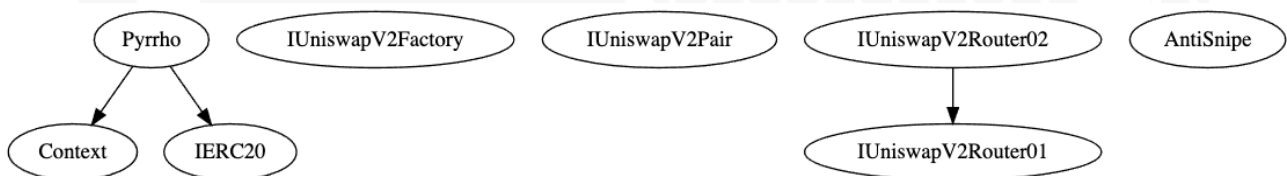
The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

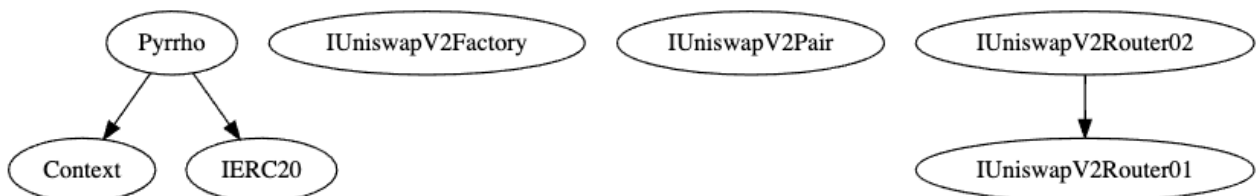
1. Correct implementation of Token standard
2. Deployer cannot mint any new tokens
3. Deployer cannot burn or lock user funds
4. Deployer cannot pause the contract
5. Overall checkup (Smart Contract Security)

## Inheritance Graph

v1.0



v1.1



## Verify Claims

### Correct implementation of Token standard

Tested	Verified
✓	✓

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 contract v1.0

1. approve	→
2. approveContractContingency	→
3. decreaseAllowance	→
4. excludePresaleAddresses	→
5. increaseAllowance	→
6. renounceOwnership	→
7. setContractSwapEnabled	→
8. setExcludedFromFees	→
9. setExcludedFromSellLimits	→
10. setExcludedFromWalletSize	→
11. setGasPriceLimit	→
12. setInitializer	→
13. setLpPair	→
14. setMaxWalletSell	→
15. setNewRouter	→
16. setProtectionSettings	→
17. setRatios	→
18. setSwapSettings	→
19. setTaxes	→
20. sweepContingency	→
21. transfer	→
22. transferFrom	→
23. transferOwner	→

## v1.1

1. approve

2. approveContractContingency

3. decreaseAllowance

4. excludePresaleAddresses

5. increaseAllowance

6. renounceOwnership

7. setContractSwapEnabled

8. setExcludedFromFees

9. setExcludedFromSellLimits

10. setExcludedFromWalletSize

11. setLpPair

12. setMaxWalletSell

13. setNewRouter

14. setRatios

15. setSwapSettings

16. setTaxes

17. setWallets

18. sweepContingency

19. transfer

20. transferFrom

21. transferOwner



## Deployer cannot mint any new tokens

Name	Exist	Tested	Verified	File
Deployer cannot mint	✓	✓	✓	Main
Comment	Line: -			

Max / Total Supply: 5.000.000.000



## Deployer cannot burn or lock user funds

Name	Exist	Tested	Verified
Deployer cannot lock	✓	✓	✓
Deployer cannot burn	✓	✓	✓

Comments:

### v1.0

- ~~Deployer can lock user funds with antiSnipe.checkUser~~

```
795         if (_hasLimits(from↑, to↑)) {
796             bool checked;
797             try antiSnipe.checkUser(from↑, to↑, amount↑) returns (bool check) {
798                 checked = check;
799             } catch {
800                 revert();
801             }
802
803             if(!checked) {
804                 revert();
805             }
806         }

```

```
298     interface AntiSnipe {
299         function checkUser(address from, address to, uint256 amt) external returns (bool);
300         function setLaunch(address _initialLpPair, uint32 _liqAddBlock, uint64 _liqAddStamp) external;
301         function setLpPair(address pair, bool enabled) external;
302         function setProtections(bool _ag) external;
303         function setGasPriceLimit(uint256 gas) external;
304         function removeSniper(address account) external;
305         function isBlacklisted(address account) external view returns (bool);
306         function setBlacklistEnabled(address account, bool enabled) external;
307     }

```

~~antiSnipe contract was not provided to solidproof, please do your own research~~

### v1.1

- Lines above were removed
  - Deployer cannot lock user funds anymore

## Deployer cannot pause the contract

Name	Exist	Tested	Verified
Deployer cannot pause	—	—	—



## Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

### Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	⚠
Unverified / Not checked	✗
Not available	—

# OnlyOwner functions

## V1.0

```
transferOwner
renounceOwnership
approveContractContingency
setNewRouter
setLpPair
setExcludedFromFees
setExcludedFromWalletSize
setExcludedFromSellLimits
setInitializer
setProtectionSettings
setGasPriceLimit
setTaxes
setRatios
setMaxWalletSell
setSwapSettings
setContractSwapEnabled
excludePresaleAddresses
sweepContingency
```

### Comments:

- Deployer can set antiSnipe address with setInitializer function
  - antiSnipe contract was not provided to solidproof, please do your own research
- setProtectionSettings
  - Deployer can enable/disable protections anytime
- setTaxes
  - Deployer can set \_taxRates.buyFee lower than 500
  - Deployer can set \_taxRates.sellFee lower than 500
- setSwapSettings
  - Check that thresholdDivisor and amountDivisor not to be 0
  - swapThreshold and swapAmount can be set without any limitations

## V1.1

**transferOwner**

**renounceOwnership**

**approveContractContingency**

**setNewRouter**

**setLpPair**

**setExcludedFromFees**

**setExcludedFromWalletSize**

**setExcludedFromSellLimits**

**setTaxes**

**setRatios**

**setMaxWalletSell**

**setWallets**

**setSwapSettings**

**setContractSwapEnabled**

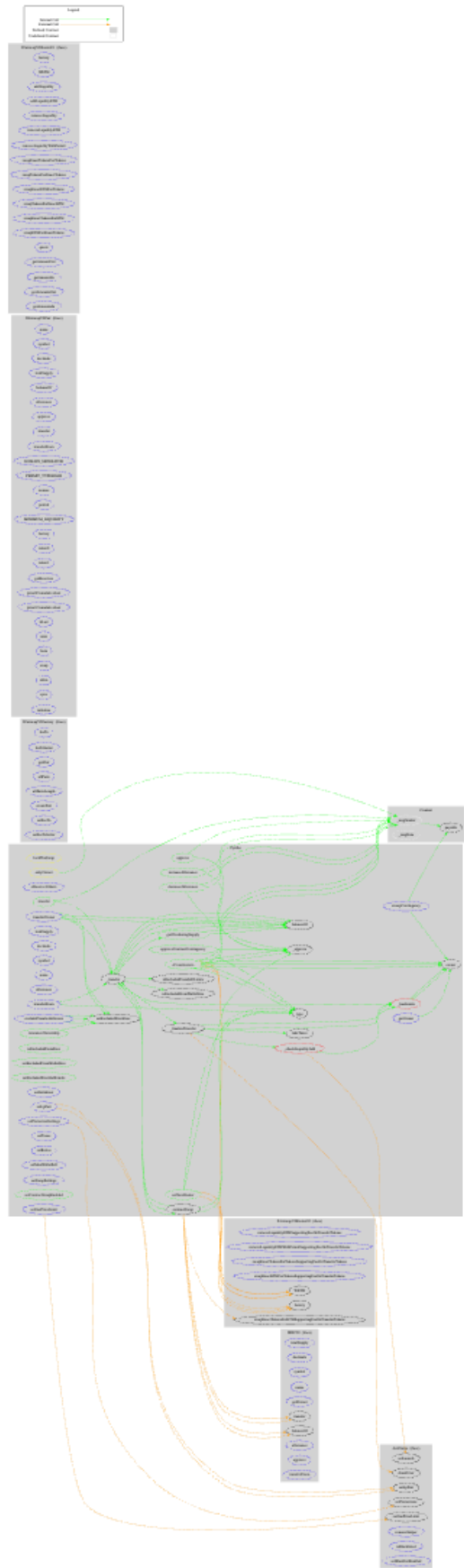
**excludePresaleAddresses**

**sweepContingency**

Comments





See above comments

# CallGraph







## Source Units in Scope

### v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/pyrrho.sol	2	6	831	577	451	87	554	
	<b>Totals</b>	<b>2</b>	<b>6</b>	<b>831</b>	<b>577</b>	<b>451</b>	<b>87</b>	<b>554</b>	

### V1.1

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/pyrrho.sol	2	5	642	537	416	87	396	
	<b>Totals</b>	<b>2</b>	<b>5</b>	<b>642</b>	<b>537</b>	<b>416</b>	<b>87</b>	<b>396</b>	

### 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 found -

### High issues

- no high issues found -

### Medium issues

- no medium issues found -

### Low issues

Issue	File	Type	Line	Description
#1	Main	Contract doesn't import npm packages from source (like OpenZeppelin etc.)	-	We recommend to import all packages from npm directly without flatten the contract. Functions could be modified or can be susceptible to vulnerabilities
#2	Main	A floating pragma is set	6	The current pragma Solidity directive is „>=0.6.0 <0.9.0 ""
#3	Main	State variable visibility is not set	314, 378, 385, 409	It is best practice to set the visibility of state variables explicitly

### Informational issues

Issue	File	Type	Line	Description
#1	Main	State variables that could be declared constant (constable-states)	221, 170, 243, 242,	Add the `constant` attributes to state variables that never change

#2	Main	Delete spaces for better readability	622	Delete space between staticVals. and maxSellTaxes  && sellFee <=staticVals. maxSellTaxes,
#3	Main	Write better descriptive error messages	623, 637	"Taxes exceed maximums" instead of "Cannot exceed maximums."  "Cannot set max wallet sell percentage below 10%" instead of "Cannot set below 10%"
#4	Main	Unused state variables	371, 372	Remove unused state variables
#5	Main	Never use static variables for addresses	391, 392	Implement functions to change state variables instead of using static variables
#6	Main	Naming convention not continuous	343	All structs has Struct at the end except Ratios Struct

## Audit Comments

### 24. November 2021:

- There is still an owner (Owner still has not renounced ownership)
  - [0x6547c77aa67b2e751d608a3c1ae5d7133fd4897f](#)
- \_hasLiqBeenAdded
  - Is False (24. Nov, 12:35 PM)

### 04. November 2021

- Look 24. November 2021 comments
- Require statement were removed

```

628     function setRatios(uint16 tokens↑, uint16 bnb↑, uint16 busd↑) external onlyOwner {
629         require (tokens↑ + bnb↑ + busd↑ >= 99, "Must add up to 100% or 99%.");
630         ratios.tokens = tokens↑;
631         ratios.bnb = bnb↑;
632         ratios.busd = busd↑;
633         ratios.total = tokens↑ + bnb↑ + busd↑;
634     }

```

## SWC Attacks

ID	Title	Relationships	Status
<a href="#">SW C-13 6</a>	Unencrypted Private Data On-Chain	<a href="#">CWE-767: Access to Critical Private Variable via Public Method</a>	PASSED
<a href="#">SW C-13 5</a>	Code With No Effects	<a href="#">CWE-1164: Irrelevant Code</a>	PASSED
<a href="#">SW C-13 4</a>	Message call with hardcoded gas amount	<a href="#">CWE-655: Improper Initialization</a>	PASSED
<a href="#">SW C-13 3</a>	Hash Collisions With Multiple Variable Length Arguments	<a href="#">CWE-294: Authentication Bypass by Capture-replay</a>	PASSED
<a href="#">SW C-13 2</a>	Unexpected Ether balance	<a href="#">CWE-667: Improper Locking</a>	PASSED
<a href="#">SW C-13 1</a>	Presence of unused variables	<a href="#">CWE-1164: Irrelevant Code</a>	PASSED
<a href="#">SW C-13 0</a>	Right-To-Left-Override control character (U+202E)	<a href="#">CWE-451: User Interface (UI) Misrepresentation of Critical Information</a>	PASSED
<a href="#">SW C-12 9</a>	Typographical Error	<a href="#">CWE-480: Use of Incorrect Operator</a>	PASSED
<a href="#">SW C-12 8</a>	DoS With Block Gas Limit	<a href="#">CWE-400: Uncontrolled Resource Consumption</a>	PASSED

<a href="#">SW C-12 7</a>	Arbitrary Jump with Function Type Variable	<a href="#">CWE-695: Use of Low-Level Functionality</a>	<b>PASSED</b>
<a href="#">SW C-12 5</a>	Incorrect Inheritance Order	<a href="#">CWE-696: Incorrect Behavior Order</a>	<b>PASSED</b>
<a href="#">SW C-12 4</a>	Write to Arbitrary Storage Location	<a href="#">CWE-123: Write-what-where Condition</a>	<b>PASSED</b>
<a href="#">SW C-12 3</a>	Requirement Violation	<a href="#">CWE-573: Improper Following of Specification by Caller</a>	<b>PASSED</b>
<a href="#">SW C-12 2</a>	Lack of Proper Signature Verification	<a href="#">CWE-345: Insufficient Verification of Data Authenticity</a>	<b>PASSED</b>
<a href="#">SW C-12 1</a>	Missing Protection against Signature Replay Attacks	<a href="#">CWE-347: Improper Verification of Cryptographic Signature</a>	<b>PASSED</b>
<a href="#">SW C-12 0</a>	Weak Sources of Randomness from Chain Attributes	<a href="#">CWE-330: Use of Insufficiently Random Values</a>	<b>PASSED</b>
<a href="#">SW C-11 9</a>	Shadowing State Variables	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	<b>PASSED</b>
<a href="#">SW C-11 8</a>	Incorrect Constructor Name	<a href="#">CWE-665: Improper Initialization</a>	<b>PASSED</b>
<a href="#">SW C-11 7</a>	Signature Malleability	<a href="#">CWE-347: Improper Verification of Cryptographic Signature</a>	<b>PASSED</b>

<a href="#">SW C-11 6</a>	Timestamp Dependence	<a href="#">CWE-829: Inclusion of Functionality from Untrusted Control Sphere</a>	PASSED
<a href="#">SW C-11 5</a>	Authorization through tx.origin	<a href="#">CWE-477: Use of Obsolete Function</a>	PASSED
<a href="#">SW C-11 4</a>	Transaction Order Dependence	<a href="#">CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')</a>	PASSED
<a href="#">SW C-11 3</a>	DoS with Failed Call	<a href="#">CWE-703: Improper Check or Handling of Exceptional Conditions</a>	PASSED
<a href="#">SW C-11 2</a>	Delegatecall to Untrusted Callee	<a href="#">CWE-829: Inclusion of Functionality from Untrusted Control Sphere</a>	PASSED
<a href="#">SW C-111</a>	Use of Deprecated Solidity Functions	<a href="#">CWE-477: Use of Obsolete Function</a>	PASSED
<a href="#">SW C-11 0</a>	Assert Violation	<a href="#">CWE-670: Always-Incorrect Control Flow Implementation</a>	PASSED
<a href="#">SW C-10 9</a>	Uninitialized Storage Pointer	<a href="#">CWE-824: Access of Uninitialized Pointer</a>	PASSED
<a href="#">SW C-10 8</a>	State Variable Default Visibility	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	NOT PASSED
<a href="#">SW C-10 7</a>	Reentrancy	<a href="#">CWE-841: Improper Enforcement of Behavioral Workflow</a>	PASSED
<a href="#">SW C-10 6</a>	Unprotected SELFDESTRUCT Instruction	<a href="#">CWE-284: Improper Access Control</a>	PASSED

<a href="#">SW C-10 5</a>	Unprotected Ether Withdrawal	<a href="#">CWE-284: Improper Access Control</a>	<b>PASSED</b>
<a href="#">SW C-10 4</a>	Unchecked Call Return Value	<a href="#">CWE-252: Unchecked Return Value</a>	<b>PASSED</b>
<a href="#">SW C-10 3</a>	Floating Pragma	<a href="#">CWE-664: Improper Control of a Resource Through its Lifetime</a>	<b>NOT PASSED</b>
<a href="#">SW C-10 2</a>	Outdated Compiler Version	<a href="#">CWE-937: Using Components with Known Vulnerabilities</a>	<b>PASSED</b>
<a href="#">SW C-10 1</a>	Integer Overflow and Underflow	<a href="#">CWE-682: Incorrect Calculation</a>	<b>PASSED</b>
<a href="#">SW C-10 0</a>	Function Default Visibility	<a href="#">CWE-710: Improper Adherence to Coding Standards</a>	<b>PASSED</b>

The logo features the words "SolidProof" in a white, handwritten-style script. The "P" is large and stylized, with a long horizontal stroke that extends to the left. The background is a solid blue color with a faint, large shield emblem. The shield has a grid-like pattern on its right side and a solid blue area on its left side.

SolidProof

**Blockchain Security | Smart Contract Audits | KYC**

A small horizontal bar representing the German flag, with black, red, and gold stripes.

MADE IN GERMANY