



SOLIDProof
Bring trust into your projects

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

MADE IN GERMANY

ImpulseX Staking Audit

**Security Assessment
09. March, 2023**

For



SolidProof_io



@solidproof_io

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	11
Risk Level	11
Capabilities	12
Inheritance Graph	13
CallGraph	14
Scope of Work/Verify Claims	15
Modifiers and public functions	24
Source Units in Scope	26
Critical issues	28
High issues	28
Medium issues	28
Low issues	28
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	23. February 2023	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary
1.1	9. March 2023	<ul style="list-style-type: none">• Reaudit

Network

Ethereum, BSC, Avalanche, and Polygon

Website

<http://www.inpulsex.io/>

Telegram

https://t.me/InpulseX_Official

Twitter

https://twitter.com/InpulseX_io

Discord

<https://discord.gg/kH6PaHsNHK>

Facebook

<https://www.facebook.com/InpulseX/>

Instagram

http://www.instagram.com/the_nftx/

TikTok

https://www.tiktok.com/@inpulsex_official

Medium

https://medium.com/@InpulseX_Official

Description

InpulseX is an ambitious project created to offer unwavering support to the biggest mission of humankind, which is to become a multiplanetary species.

The PulseX ecosystem will take the lead within the blockchain community, bringing awareness and raising financial resources to help write this exciting new chapter.

Together we will make history.

Project Engagement

During the Date of 23 February 2023, **InpulseX 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://github.com/KenshiTech/InpulseX/tree/master/staking>
- Commit: b82c25db733303f34aae4363d17f608717f275ec

v1.1

- <https://github.com/KenshiTech/InpulseX/tree/master/staking>
- Commit: 8c872789d3d06a74ede9d7d2081a42d469be6102

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 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:
v1.0

```
../Base.sol  
../interfaces/IERC20.sol
```

```
../interfaces/IERC1155.sol  
../interfaces/IERC1155Receiver.sol
```

```
../Base.sol  
../interfaces/IERC1155.sol  
../interfaces/IERC1155Receiver.sol
```

```
../interfaces/IERC1363.sol  
../interfaces/IERC1363Receiver.sol
```

```
../Base.sol  
../interfaces/IERC20.sol  
../rewards/ERC20.sol  
../rewards/ERC1155.sol
```

```
../Base.sol  
../interfaces/IERC20.sol  
../interfaces/IERC721.sol  
../interfaces/IERC721Receiver.sol  
../rewards/ERC20.sol  
../rewards/ERC1155.sol
```


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.

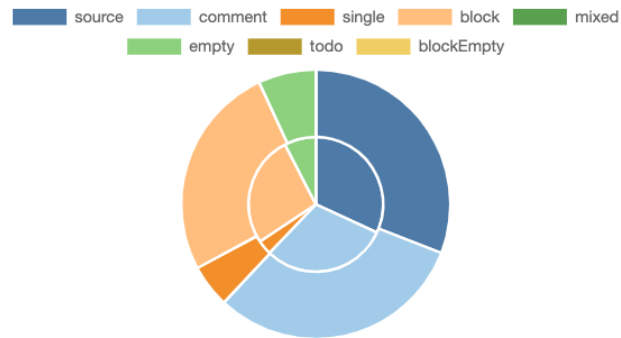
v1.0

File Name	SHA-1 Hash
contracts/interfaces/ IERC165.sol	bbb2af818780ce0aee1910aa988e4 c2d3738bcfb
contracts/interfaces/ IERC1363.sol	f4b26a591eefe329d454153d428a58 f4977191c2
contracts/interfaces/ IERC1363Receiver.sol	72b322bc3ebf8acc82847969d9628 e5c1373ea9f
contracts/interfaces/ IERC721.sol	2b4172e8f2424ad2ad30f888474c3d 31e07230a8
contracts/interfaces/ IERC1155.sol	a212fd8cab21a6d07adcb22cb3e04 61a40e17047
contracts/interfaces/ IERC1363Spender.sol	91959bd12baa5a3922d1c686f6e15 86aac04fe13
contracts/interfaces/ IERC721Receiver.sol	ed74e31fbacf270281fc36ff0e16e49 ea6637ee1
contracts/interfaces/ IERC1155Receiver.sol	d12019ad5816a2b6007c59278a5af 9947af04dd5
contracts/interfaces/IERC20.sol	e31040bd37a737946ff14ab726582b b99f22d35e
contracts/interfaces/ IERC721Enumerable.sol	841bc27064d5a0652115b3832c586 87fbab5e41c
contracts/Repo.sol	0b03cb7e65a135d12fa3d0661a965 93663bf9e01

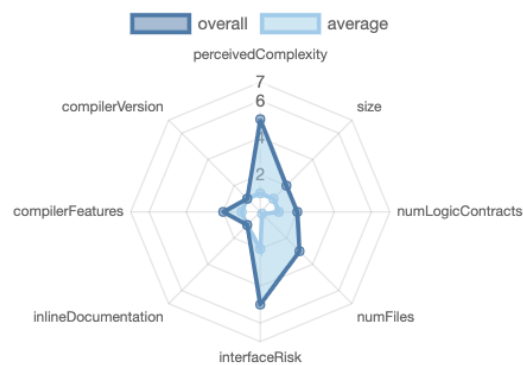
contracts/staking/ERC1363.sol	eea7fe107f9e57547beea73784276d aad35d4a3f
contracts/staking/ERC721.sol	8bb319394a59b060c226d81b11086 ff9158ba73c
contracts/staking/ERC20.sol	a5e83ce3e17b52ccf1b072a4c200cb faa630ef81
contracts/staking/ERC1155.sol	fc0245d3989b16aae6326a7fd47ebe 06fdf7c8fe
contracts/Base.sol	1ba4c2f74dc91d350b4cff4fa48e482 30f8ed479
contracts/utils/NFTSweep.sol	104961e6f54efdd1b6654f07008479 469f154385
contracts/libraries/Context.sol	7b80abcebc3aefb2e038554fe625f0 486a92cce2
contracts/libraries/Address.sol	042ebb5c266fa61fbab8035f02824c 050cc6e89d
contracts/libraries/Ownable.sol	ebde8ee4a2625d1784506ced979a9 1e5faad6308
contracts/rewards/ERC20.sol	7af0134aa55596282af5af73290387f 98c51a990
contracts/rewards/ERC1155.sol	24bea42990479bd33c56ec7b4776b 31704931937

Metrics

Source Lines v1.0



Risk Level v1.0



Capabilities Components

 Contracts	 Libraries	 Interfaces	 Abstract
11	1	10	8


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
93	4

External	Internal	Private	Pure	View
87	58	0	5	41

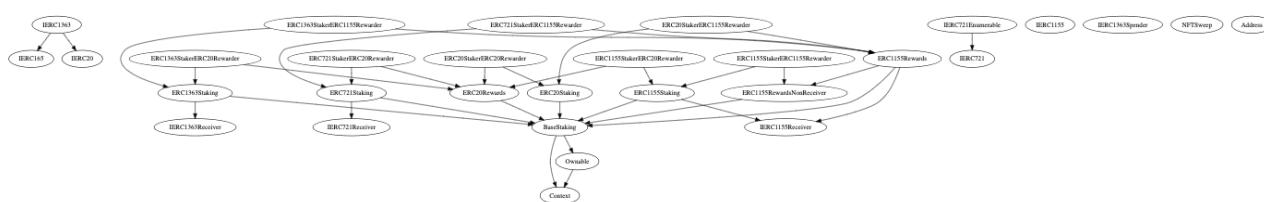
StateVariables

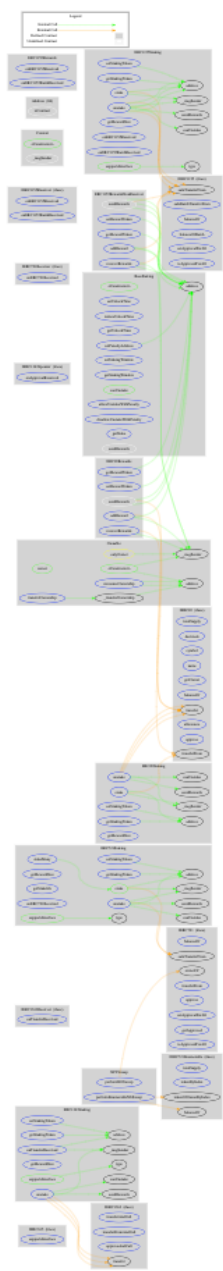
Total	 Public
18	0

Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts	
<input type="text" value="^0.8.17"/>		<input type="text" value="yes"/>	<input type="text"/>	<input type="text"/>	
 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRrecover	 New/Create/Create2
<input type="text" value="yes"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
 TryCatch	Σ Unchecked				
<input type="text" value="yes"/>	<input type="text"/>				

Inheritance Graph





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. Deployer cannot mint any new tokens
3. Deployer cannot burn or lock user funds
4. Deployer cannot pause the contract
5. Deployer cannot set fees
6. Deployer cannot blacklist/antisnipe addresses
7. Overall checkup (Smart Contract Security)



Is contract an upgradeable

Name	
Is contract an upgradeable?	No



Write functions of contract v1.1

- ◆ setUnlockTime
- ◆ setPenaltyAddress
- ◆ allowUnstakeWithPenalty
- ◆ disallowUnstakeWithPenalty

- ◆ setStakingToken
- ◆ stake
- ◆ stakeMany
- ◆ unstake

- ◆ setStakingToken
- ◆ unstake
- ◆ onTransferReceived

Deployer cannot mint any new tokens

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



Deployer cannot burn or lock user funds

Name	Exist	Tested	Status
Deployer cannot lock	✓	✓	✓
Deployer cannot burn	—	—	—

Comments:

v1.0

- Owner cannot lock user funds by changing the staking token address because it can only be set once

Deployer cannot pause the contract

Name	Exist	Tested	Status
Deployer can pause	—	—	—



Deployer cannot set fees

Name	Exist	Tested	Status
Deployer cannot set fees over 25%	✓	✓	✓
Deployer cannot set fees to nearly 100% or to 100%	✓	✓	✓

Comments:

v1.1

- The owner can set the penalty fees for any address to up to 25% only

Deployer can blacklist/antisnipe addresses

Name	Exist	Tested	Status
Deployer cannot 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

v1.1

rewards/ERC20.sol

- ◆ setRewardToken
- Ⓜ onlyOwner
- ◆ addReward
- ◆ recoverRewards
- Ⓜ onlyOwner

rewards/ERC1155.sol

- ◆ setRewardToken
- Ⓜ onlyOwner
- ◆ addReward
- ◆ recoverRewards
- Ⓜ onlyOwner

Base.sol

- ◆ setUnlockTime
- Ⓜ onlyOwner
- ◆ setPenaltyAddress
- Ⓜ onlyOwner
- ◆ allowUnstakeWithPenalty
- Ⓜ onlyOwner
- ◆ disallowUnstakeWithPenalty
- Ⓜ onlyOwner

Staking/ERC20.sol

- ◆ setStakingToken
- Ⓜ onlyOwner
- ◆ stake
- ◆ unstake

Staking/ERC721.sol

- ◆ setStakingToken
- Ⓜ onlyOwner
- ◆ stake
- ◆ stakeMany
- ◆ unstake


```
◆ setStakingToken
Ⓜ onlyOwner
◆ unstake
◆ onTransferReceived
```

Ownership Privileges:

- Base.sol:
 - Owner can set unlock time for the staked tokens to any arbitrary value but only once
 - Allow/Disallow users to unstake with a penalty. Therefore, owner can do this to any address at any time but the penalty fees cannot be more than 25%
 - Set penalty receiver address.
- staking/ERC20.sol:
 - Owner can update the staking token address only once, and it cannot be updated
 - **Note:** This same exist with the staking of ERC1155, ERC721, and ERC1363
- rewards/ERC20.sol:
 - Set/Update reward token, but only once
 - Recover the tokens from contract. Hence, withdraw reward token from the contract.
 - In the contract, any user can transfer the reward token but only owner can withdraw it.
 - **Note:** This same exist with rewards/ERC721.sol,

Source Units in Scope v1.0

File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score
contracts/interfaces/IERC165.sol	—————	1	25	24	3	20	3
contracts/interfaces/IERC1363.sol	—————	1	101	36	5	63	17
contracts/interfaces/IERC1363Receiver.sol	—————	1	35	29	3	24	3
contracts/interfaces/IERC721.sol	—————	1	129	43	18	74	31
contracts/interfaces/IERC1155.sol	—————	1	149	77	23	89	13
contracts/interfaces/IERC1363Spender.sol	—————	1	33	28	3	23	3
contracts/interfaces/IERC721Receiver.sol	—————	1	24	18	3	14	3
contracts/interfaces/IERC1155Receiver.sol	—————	1	49	21	3	30	5
contracts/interfaces/IERC20.sol	—————	1	106	26	21	66	21
contracts/interfaces/IERC721Enumerable.sol	—————	1	33	13	4	19	9
contracts/Repo.sol	—————	—————	7	7	5	1	—————
contracts/staking/ERC1363.sol	3	—————	128	123	65	41	56
contracts/staking/ERC721.sol	3	—————	154	145	69	53	68
contracts/staking/ERC20.sol	3	—————	108	108	60	34	51
contracts/staking/ERC1155.sol	3	—————	171	159	91	47	61
contracts/Base.sol	1	—————	128	124	58	50	42
contracts/utis/NFTSweep.sol	1	—————	57	48	29	16	43
contracts/libraries/Context.sol	1	—————	22	22	7	13	1
contracts/libraries/Address.sol	1	—————	43	43	6	35	1
contracts/libraries/Ownable.sol	1	—————	81	81	36	36	24
contracts/rewards/ERC20.sol	1	—————	70	67	38	22	33
contracts/rewards/ERC1155.sol	2	—————	118	103	65	29	45
Totals	20	10	1771	1345	615	799	533

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalised lines of the source unit (e.g. normalises functions spanning multiple lines)
nSLOC	normalised 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

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/latest/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.

09. March 2023:

- There is still an owner (Owner still has not renounced ownership)
- Read whole report and modifiers section for more information

SWC Attacks

ID	Title	Relationships	Status
SW C-1 36	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SW C-1 35	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SW C-1 34	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SW C-1 33	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SW C-1 32	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SW C-1 31	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SW C-1 30	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SW C-1 29	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SW C-1 28	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SW C-1 27	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SW C-1 25	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SW C-1 24	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SW C-1 23	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SW C-1 22	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SW C-1 21	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SW C-1 20	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SW C-11 9	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-11 8	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SW C-11 7	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SW C-11 6	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 5	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SW C-11 4	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SW C-11 3	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SW C-11 2	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 1	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SW C-11 0	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SW C-1 09	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SW C-1 08	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-1 07	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SW C-1 06	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SW C-1 05	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SW C-1 04	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SW C-1 03	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	PASSED
SW C-1 02	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SW C-1 01	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SW C-1 00	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED



*Solid
Proofed*

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


MADE IN GERMANY