



# SOLIDProof

*Bring trust into your projects*

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

MADE IN GERMANY

# Oscar Swap

# Audit

**Security Assessment**  
**01. May, 2023**

**For**



**SolidProof\_io**



**@solidproof\_io**

|  |    |
|--|----|
| Disclaimer   | 3  |
| Description  | 5  |
| Project Engagement   | 5  |
| Logo   | 5  |
| Contract Links   | 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                                   | 16 |
| Source Units in Scope  | 19 |
| Critical issues  | 20 |
| High issues  | 20 |
| Medium issues  | 20 |
| Low issues   | 20 |
| Informational issues   | 21 |
| Audit Comments   | 21 |
| SWC Attacks  | 22 |

# 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     | 29. April 2023 - 1. May 2023 | <ul style="list-style-type: none"><li>• Layout project</li><li>• Automated- /Manual-Security Testing</li><li>• Summary</li></ul> |

## **Network**

Arbitrum

## **Website**

<https://oscarswap.com/>

## **Medium**

<https://medium.com/@oscarswap>

## **Twitter**

[https://twitter.com/Oscar\\_Swap](https://twitter.com/Oscar_Swap)

## **Discord**

<https://discord.gg/G8Qfn7cmjy>

## **Instagram**

[https://www.instagram.com/oscar\\_swap/](https://www.instagram.com/oscar_swap/)

## **Reddit**

[https://www.reddit.com/r/Oscar\\_swap/](https://www.reddit.com/r/Oscar_swap/)

## Description

Oscarswap is a decentralized exchange (DEX) that operates on the Arbitrum network, utilizing automated market-maker (AMM) technology. Its cutting-edge technology is designed to offer the lowest fees for swapping cryptocurrencies, coupled with highly profitable yield farming rewards, making it an ideal choice for passive income seekers. Oscarswap is a decentralized exchange (DEX) that operates on the Arbitrum network, utilizing automated market-maker (AMM) technology. Its cutting-edge technology is designed to offer the lowest fees for swapping cryptocurrencies, coupled with highly profitable yield farming rewards, making it an ideal choice for passive income seekers.

## Project Engagement

During the 28 of April 2023, **OscarSwap 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 Links

### v1.0

Arbitrum Network

**Oscarswap:** 0x7976ff355313747852aab6d0a06c378214b74c34

**Factory:** 0x20fc9D10d7391bC9C7F338fd94F7185B0Fed9A4C

**Timelock:** 0x2bee4903ffeebecBBd2Dac20Ef823fa566F3EBfd

**Masterchef:** 0x1A635bb3fC03e6e7109eBdFb61a4DA971B37A329

**Multisig:** 0xe8ffe751dea181025a9acf3d6bde8cda5380f53f

**Router:** 0x4d381C158d74c88dA251BabfE33d320239324213

**Zap:** 0x1627c27eB95ee0856Cc1a76484D3F5d9cBEE167c

**OscarPool:** 0x826fb9072Dd8C5187B0ac1D1429F7bFc9e3F93ee

**OscarFlexPool:** 0xC680aD5a7C42BF8a6a669D08C40317fa1a16b7bC

# 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:

MasterChef

- SafeMath
- IERC20
- Address
- SafeERC20
- Context
- Ownable
- ERC20
- OscarToken

OscarFactory

- IOscarFactory
- IOscarPair
- IOscarERC20
- SafeMath
- OscarERC20
- Math
- UQ112x112
- IERC20
- IOscarCallee
- OscarPair

TimelockController

- IAccessControl
- Context
- IERC165
- ERC165
- Strings
- AccessControl

OscarRouter

- IOscarFactory
- TransferHelper
- IOscarRouter01
- IOscarRouter02
- IOscarPair
- SafeMath
- OscarLibrary
- IERC20
- IWETH

OscarToken

- SafeMath
- IBEP20
- Address
- SafeBEP20
- Context
- Ownable
- BEP20

OscarDexZapV1

- IERC20
- IOscarDexPair
- IOscarDexRouter01
- IOscarDexRouter02
- IWETH
- Address
- Context
- Ownable
- SafeERC20
- ReentrancyGuard
- Babylonian

OscarPool

- Context
- Ownable
- IERC20
- Address
- SafeERC20
- Pausable
- IMasterChefV2

OscarFlexiblePool

- Context
- Ownable
- IERC20
- Address
- SafeERC20
- Pausable
- IoscarPool



## Tested Contract Files

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

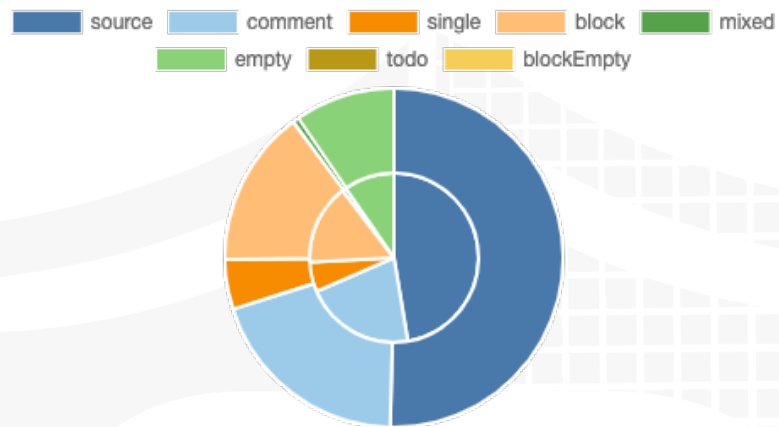
*A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.*

### v1.0

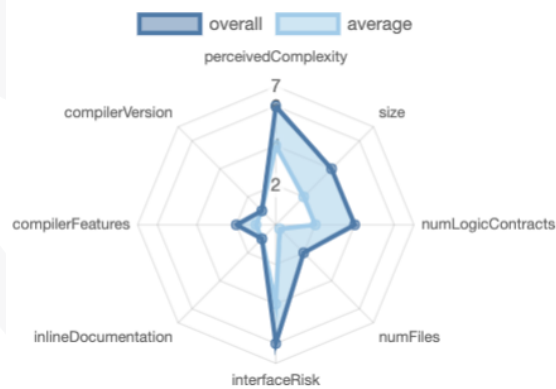
| File Name                            | SHA-1 Hash                                   |
|--------------------------------------|--|
| contracts/<br>TimelockController.sol | fcd24eb9c654d6fb580e0783dced1de9a43<br>8d23d |
| contracts/MasterChef.sol             | 01326904c0f9fa52ca22ef5f4fa024769c8e<br>08aa |
| contracts/OscarToken.sol             | a38d2b11254bce89b5ec750929c000f6da<br>7444dd |
| contracts/OscarPool.sol              | b82c4539861f58b65eb30c2ecbc58bf7d9<br>74fc0  |
| contracts/<br>OscarFlexiblePool.sol  | 171459e180bbb0e422750d409334984a2<br>c0669a1 |
| contracts/OscarRouter.sol            | 38d1cdb4e71cfbe9ae81065f31be3c7b0b6<br>6333f |
| contracts/<br>OscarDexZapV1.sol      | 154cd23ad85525ffd365c178eec84adf8be<br>9fe78 |
| contracts/OscarFactory.sol           | f18f754e39a72d24717c8d527d53be9902<br>e56d0d |

# Metrics

## Source Lines v1.0



## Risk Level v1.0



# Capabilities

## Components

|  Contracts |  Libraries |  Interfaces |  Abstract |
|---|---|--|--|
| 17  | 20  | 24   | 12   |

### 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 |
|--|---|
| 441  | 21  |







| External | Internal | Private | Pure | View |
|----------|----------|---------|------|------|
| 329      | 548      | 19      | 82   | 189  |


### StateVariables

| Total |  Public |
|-------|--|
| 149   | 112  |

### Capabilities

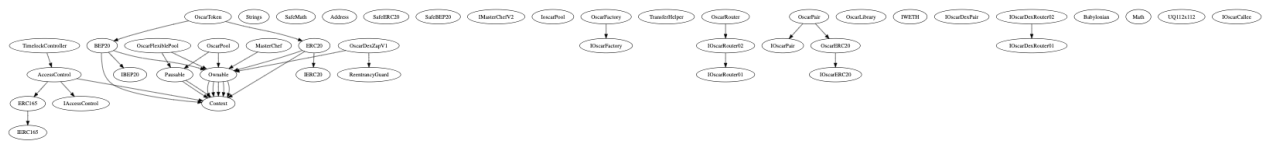
| Solidity Versions observed  |  Experimental Features |  Can Receive Funds |  Uses Assembly |  Has Destroyable Contracts |
|---|---|---|---|---|
| <div><div>^0.8.0</div><div>0.8.16</div><div>0.6.12</div><div>=0.6.6</div><div>&gt;=0.5.0</div><div>&gt;=0.6.2</div><div>^0.8.1</div><div>^0.8.4</div><div>^0.5.16</div></div> |   | <div>yes</div>  | <div>yes</div> <div>(12 asm blocks)</div>   |   |

|  Transfers ETH |  Low-Level Calls |  DelegateCall |  Uses Hash Functions |  ECRRecover |  New/Create/Create2 |
|---|---|--|---|--|--|
| <div>yes</div>  |   | <div>yes</div>   | <div>yes</div>  | <div>yes</div>   | <div>yes</div> <div>→ AssemblyCall:Name:create2</div>  |

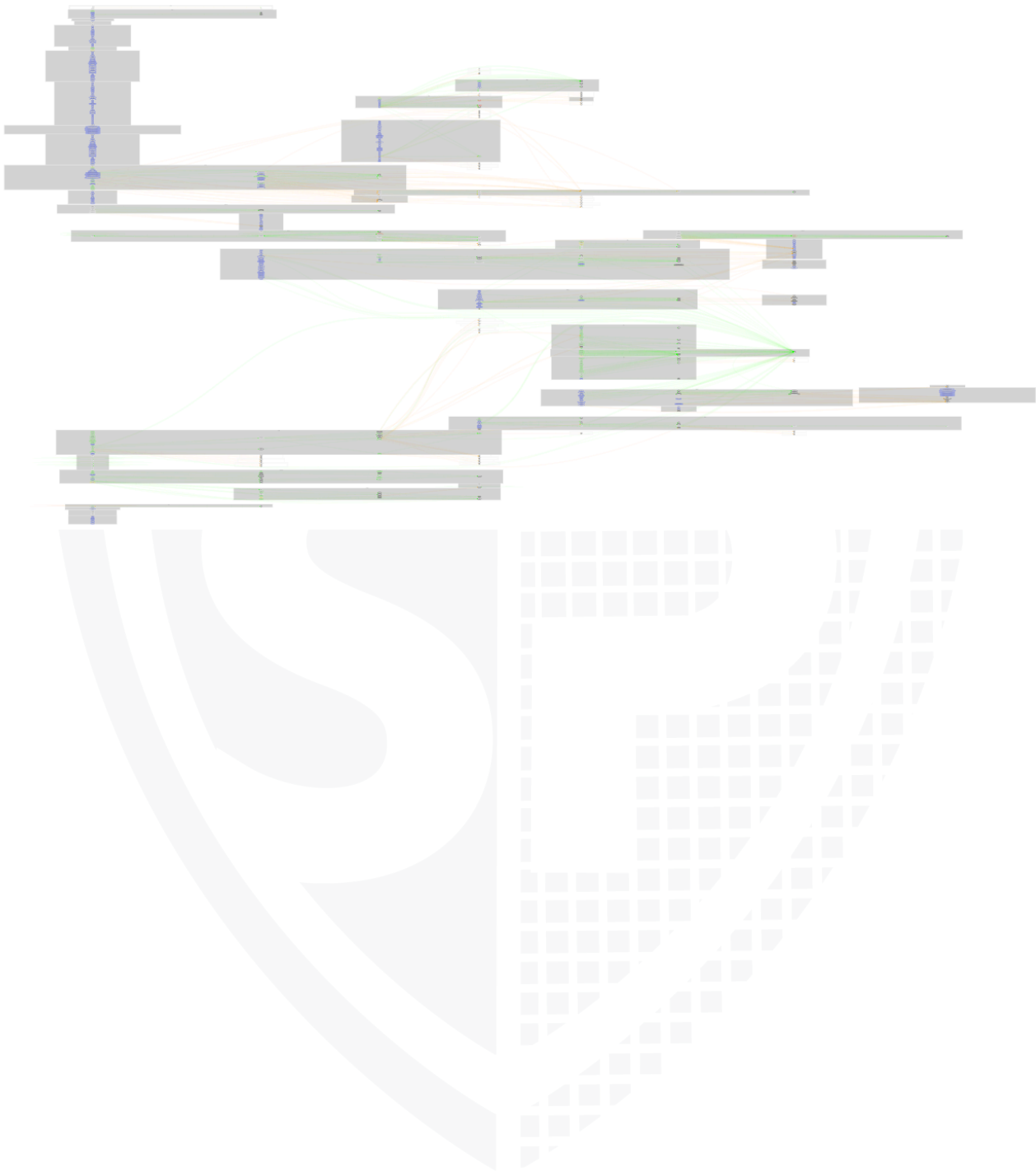
|  TryCatch | $\Sigma$ Unchecked |
|--|--------------------|
|  | <div>yes</div>     |

# Inheritance Graph

## v1.0



CallGraph  
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. Overall checkup (Smart Contract Security)



## 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

## MasterChef

- 🔹 setTreasury
- Ⓜ onlyOwner
- 🔹 updateOscarPerSec
- Ⓜ onlyOwner
- 🔹 updateWETHPerSec
- Ⓜ onlyOwner
- 🔹 updateStableCoin
- Ⓜ onlyOwner
- 🔹 updateStableCoinPerSec
- Ⓜ onlyOwner
- 🔹 updateMultiplier
- Ⓜ onlyOwner
- 🔹 add
- Ⓜ onlyOwner
- 🔹 set
- Ⓜ onlyOwner
- 🔹 massUpdatePools
- 🔹 updatePool
- 🔹 deposit
- 🔹 withdraw
- 🔹 emergencyWithdraw
- 🔹 setStartTime
- Ⓜ onlyOwner

## OscarFlexiblePool

- 🔹 deposit
- Ⓜ whenNotPaused
- 🔹 withdraw
- 🔹 withdrawAll
- 🔹 setTreasury
- Ⓜ onlyOwner
- 🔹 setPerformanceFee
- Ⓜ onlyOwner
- 🔹 setWithdrawFee
- Ⓜ onlyOwner
- 🔹 setWithdrawFeePeriod
- Ⓜ onlyOwner
- 🔹 setWithdrawAmountBooster
- Ⓜ onlyOwner
- 🔹 emergencyWithdraw
- Ⓜ onlyOwner
- 🔹 inCaseTokensGetStuck
- Ⓜ onlyOwner
- 🔹 pause
- Ⓜ onlyOwner
- Ⓜ whenNotPaused
- 🔹 unpause
- Ⓜ onlyOwner
- Ⓜ whenPaused

## OscarPool

- 🔹 init
- 🔹 unlock
- Ⓜ onlyOwner
- Ⓜ whenNotPaused
- 🔹 deposit
- Ⓜ whenNotPaused
- 🔹 withdrawByAmount
- Ⓜ whenNotPaused
- 🔹 withdraw
- Ⓜ whenNotPaused
- 🔹 withdrawAll
- 🔹 setTreasury
- Ⓜ onlyOwner
- 🔹 setFreePerformanceFeeUser
- Ⓜ onlyOwner
- 🔹 setOverdueFeeUser
- Ⓜ onlyOwner
- 🔹 setWithdrawFeeUser
- Ⓜ onlyOwner
- 🔹 setPerformanceFee
- Ⓜ onlyOwner
- 🔹 setPerformanceFeeContract
- Ⓜ onlyOwner
- 🔹 setWithdrawFee
- Ⓜ onlyOwner
- 🔹 setOverdueFee
- Ⓜ onlyOwner
- 🔹 setWithdrawFeeContract
- Ⓜ onlyOwner
- 🔹 setWithdrawFeePeriod
- Ⓜ onlyOwner
- 🔹 setMaxLockDuration
- Ⓜ onlyOwner
- 🔹 setDurationFactor
- Ⓜ onlyOwner
- 🔹 setDurationFactorOverdue
- Ⓜ onlyOwner
- 🔹 setUnlockFreeDuration
- Ⓜ onlyOwner
- 🔹 inCaseTokensGetStuck
- Ⓜ onlyOwner
- 🔹 pause
- Ⓜ onlyOwner
- Ⓜ whenNotPaused
- 🔹 unpause

## OscarDexZapV1

- 🔹 updateMaxZapInverseRatio
- Ⓜ onlyOwner
- 🔹 recoverWrongTokens
- Ⓜ onlyOwner

## TimelockController

- 🔹 schedule
- Ⓜ onlyRole
- 🔹 scheduleBatch
- Ⓜ onlyRole
- 🔹 cancel
- Ⓜ onlyRole
- 🔹 execute 💰
- Ⓜ onlyRoleOrOpenRole
- 🔹 executeBatch 💰
- Ⓜ onlyRoleOrOpenRole
- 🔹 updateDelay



## Note:

### ❖ General fork from PancakeSwap

- Contracts inside are the same as the pancake-smart-contracts directory
  - <https://github.com/pancakeswap/pancake-smart-contracts/tree/master/projects>
  - Differences between OscarSwap and PancakeSwap contracts are the following:
    - MasterChefv2 contract does not have the staking functionality as it does in the Pancake swap. And an added stable coin reward mechanism along with the native token
    - Boost Weight functionality of CakePool has been removed from OscarPool
    - Factory contract has no changes that are critical to the logic
    - OscarRouter has no modified functionalities

## Ownership Privileges

### ❖ MasterChef.sol -

- Set Treasury and StableCoin address
- Update OscarPerSec, WETHPerSec, StableCoinPerSec, and Multiplier to any arbitrary value.
- Add new Lp to the pool
- Set allocation point for a given ARX
- Set Start Time

### ❖ OscarPool.sol -

- Unlock user Oscar funds only when the contract is not paused
- Pause/Unpause Deposits and Withdraws
- Set treasury address, fee address, overdue fee address, and withdraw fee address
- Set performance fee but cannot be set more than 20%
- Set withdraw fee but cannot be set more than 5%
- The overdue fees can be set up to 100%. This fee will only be levied based on users overdue duration. Beware of it
- Set withdraw fee contract and period
- Set max lock duration but not more than 1000 days, but keep in mind that it could be set to zero.
- Set duration factor, duration factor overdue, and unlock free duration
- Withdraw unexpected tokens from the contract, but not the staked one

❖ [OscarFlexiblePool.sol](#)

- Pause/Unpause Deposits
- Set treasury address
- Set performance, and withdraw fee
- Set withdraw fee period and amount booster
- Owner can withdraw their shares while the staking is true, and once it is done then no more staking could be done in the contract.
- Withdraw unexpected tokens from the contract but not the deposit tokens

❖ [OscarToken.sol](#)

- Owner can Mint tokens but not more than max supply which is 50 Million

❖ [TimelockController.sol](#)

- The Proposer Role contract/wallet can schedule, cancel, and execute an operation

**Please check if an `OnlyOwner` or similar restrictive modifier has been forgotten.**

## Source Units in Scope

### v1.0

| File                             | Logic Contracts | Interfaces | Lines       | nLines      | nSLOC       | Comment Lines | Complex. Score |
|----------------------------------|-----------------|------------|-------------|-------------|-------------|---------------|----------------|
| contracts/TimelockController.sol | 5               | 2          | 907         | 782         | 380         | 395           | 258            |
| contracts/MasterChef.sol         | 8               | 1          | 1578        | 1394        | 720         | 628           | 531            |
| contracts/OscarToken.sol         | 7               | 1          | 1198        | 1014        | 434         | 565           | 300            |
| contracts/OscarPool.sol          | 6               | 2          | 1309        | 1170        | 657         | 525           | 410            |
| contracts/OscarFlexiblePool.sol  | 6               | 2          | 943         | 795         | 421         | 404           | 288            |
| contracts/OscarRouter.sol        | 4               | 6          | 1229        | 628         | 555         | 29            | 577            |
| contracts/OscarDexZapV1.sol      | 7               | 5          | 1762        | 1239        | 644         | 505           | 543            |
| contracts/OscarFactory.sol       | 6               | 5          | 726         | 493         | 413         | 47            | 432            |
| <b>Totals</b>                    | <b>49</b>       | <b>24</b>  | <b>9652</b> | <b>7515</b> | <b>4224</b> | <b>3098</b>   | <b>3339</b>    |

### 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

| Issue | File                 | Type   | Line                      | Description  |
|-------|----------------------|--|---------------------------|--|
| #1    | All                  | Multiple pragma is set                               | —                         | Some of the contracts contain different pragma versions which is not recommended for deployment. We recommend to have the same pragma in all contracts and also to update the old pragma versions to the new ones. |
| #2    | MasterC<br>hefv2.sol | Missing Zero Address Validation (missing-zero-check) | 1307                      | Check that the address is not zero   |
| #3    | MasterC<br>hef.sol   | Missing Events Arithmetic                            | 13017-1328,<br>1338, 1361 | Emit an event for critical parameter changes   |
| #4    | OscarR<br>outer.sol  | Old Compiler Version                                 | 2                         | The contract uses a very old compiler version which is not recommended for deployment as it is susceptible to known vulnerabilities  |

|    |                  |                      |   |   |
|----|------------------|----------------------|---|---|
| #5 | OscarFactory.sol | Old Compiler Version | 2 | The contract uses a very old compiler version which is not recommended for deployment as it is susceptible to known vulnerabilities |
| #6 | OscarToken.sol   | Old Compiler Version | 3 | The contract uses a very old compiler version which is not recommended for deployment as it is susceptible to known vulnerabilities |

## Informational issues

| Issue | File | Type  | Line | Description   |
|-------|------|---|------|---|
| #1    | All  | Contract doesn't import npm packages from source (like OpenZeppelin etc.) | —    | We recommend importing all packages from npm directly without flattening the contract. Functions could be modified or can be susceptible to vulnerabilities |

## 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.

### 01. May 2023:

- This project consists of the following forks
  - Pancake Swap
  - Uniswap
- Unit tests with 100% code coverage was not provided to SolidProof so we cannot ensure complete functional correctness of the code's logic.
- We recommend OscarSwap team to conduct unit and fuzz tests thoroughly to rule out possibilities of an unwanted logical and calculation errors.
- Read whole report and modifiers section for more information
- The low issues that exist in the PancakeSwap codebase still exist in the forked code.
- We recommend using a multisig wallet for the owner address to prevent any risk of the loss of private key
- Do your own research here

## SWC Attacks

| ID                        | Title   | Relationships  | Status |
|---------------------------|---|--|--------|
| <a href="#">SW C-1 36</a> | Unencrypted Private Data On-Chain                       | <a href="#">CWE-767: Access to Critical Private Variable via Public Method</a>         | PASSED |
| <a href="#">SW C-1 35</a> | Code With No Effects                                    | <a href="#">CWE-1164: Irrelevant Code</a>  | PASSED |
| <a href="#">SW C-1 34</a> | Message call with hardcoded gas amount                  | <a href="#">CWE-655: Improper Initialization</a>                                       | PASSED |
| <a href="#">SW C-1 33</a> | Hash Collisions With Multiple Variable Length Arguments | <a href="#">CWE-294: Authentication Bypass by Capture-replay</a>                       | PASSED |
| <a href="#">SW C-1 32</a> | Unexpected Ether balance                                | <a href="#">CWE-667: Improper Locking</a>  | PASSED |
| <a href="#">SW C-1 31</a> | Presence of unused variables                            | <a href="#">CWE-1164: Irrelevant Code</a>  | PASSED |
| <a href="#">SW C-1 30</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-1 29</a> | Typographical Error                                     | <a href="#">CWE-480: Use of Incorrect Operator</a>                                     | PASSED |
| <a href="#">SW C-1 28</a> | DoS With Block Gas Limit                                | <a href="#">CWE-400: Uncontrolled Resource Consumption</a>                             | PASSED |

|                           |   |   |               |
|---------------------------|---|---|---------------|
| <a href="#">SW C-1 27</a> | Arbitrary Jump with Function Type Variable          | <a href="#">CWE-695: Use of Low-Level Functionality</a>                   | <b>PASSED</b> |
| <a href="#">SW C-1 25</a> | Incorrect Inheritance Order                         | <a href="#">CWE-696: Incorrect Behavior Order</a>                         | <b>PASSED</b> |
| <a href="#">SW C-1 24</a> | Write to Arbitrary Storage Location                 | <a href="#">CWE-123: Write-what-where Condition</a>                       | <b>PASSED</b> |
| <a href="#">SW C-1 23</a> | Requirement Violation                               | <a href="#">CWE-573: Improper Following of Specification by Caller</a>    | <b>PASSED</b> |
| <a href="#">SW C-1 22</a> | Lack of Proper Signature Verification               | <a href="#">CWE-345: Insufficient Verification of Data Authenticity</a>   | <b>PASSED</b> |
| <a href="#">SW C-1 21</a> | Missing Protection against Signature Replay Attacks | <a href="#">CWE-347: Improper Verification of Cryptographic Signature</a> | <b>PASSED</b> |
| <a href="#">SW C-1 20</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>                                    | <b>PASSED</b> |
| <a href="#">SW C-11 5</a> | Authorization through tx.origin      | <a href="#">CWE-477: Use of Obsolete Function</a>  | <b>PASSED</b> |
| <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> | <b>PASSED</b> |
| <a href="#">SW C-11 3</a> | DoS with Failed Call                 | <a href="#">CWE-703: Improper Check or Handling of Exceptional Conditions</a>  | <b>PASSED</b> |
| <a href="#">SW C-11 2</a> | Delegatecall to Untrusted Callee     | <a href="#">CWE-829: Inclusion of Functionality from Untrusted Control Sphere</a>                                    | <b>PASSED</b> |
| <a href="#">SW C-11 1</a> | Use of Deprecated Solidity Functions | <a href="#">CWE-477: Use of Obsolete Function</a>  | <b>PASSED</b> |
| <a href="#">SW C-11 0</a> | Assert Violation                     | <a href="#">CWE-670: Always-Incorrect Control Flow Implementation</a>  | <b>PASSED</b> |
| <a href="#">SW C-1 09</a> | Uninitialized Storage Pointer        | <a href="#">CWE-824: Access of Uninitialized Pointer</a>   | <b>PASSED</b> |
| <a href="#">SW C-1 08</a> | State Variable Default Visibility    | <a href="#">CWE-710: Improper Adherence to Coding Standards</a>  | <b>PASSED</b> |
| <a href="#">SW C-1 07</a> | Reentrancy                           | <a href="#">CWE-841: Improper Enforcement of Behavioral Workflow</a>   | <b>PASSED</b> |
| <a href="#">SW C-1 06</a> | Unprotected SELFDESTRUCT Instruction | <a href="#">CWE-284: Improper Access Control</a>   | <b>PASSED</b> |



|   |                                      |  |                       |
|---|--------------------------------------|--|-----------------------|
| <a href="#">SW</a><br><a href="#">C-1</a><br><a href="#">05</a> | Unprotected<br>Ether<br>Withdrawal   | <a href="#">CWE-284: Improper Access<br/>Control</a>                                 | <b>PASSED</b>         |
| <a href="#">SW</a><br><a href="#">C-1</a><br><a href="#">04</a> | Unchecked<br>Call Return<br>Value    | <a href="#">CWE-252: Unchecked Return<br/>Value</a>                                  | <b>PASSED</b>         |
| <a href="#">SW</a><br><a href="#">C-1</a><br><a href="#">03</a> | Floating<br>Pragma                   | <a href="#">CWE-664: Improper Control of<br/>a Resource Through its<br/>Lifetime</a> | <b>NOT<br/>PASSED</b> |
| <a href="#">SW</a><br><a href="#">C-1</a><br><a href="#">02</a> | Outdated<br>Compiler<br>Version      | <a href="#">CWE-937: Using Components<br/>with Known Vulnerabilities</a>             | <b>NOT<br/>PASSED</b> |
| <a href="#">SW</a><br><a href="#">C-1</a><br><a href="#">01</a> | Integer<br>Overflow and<br>Underflow | <a href="#">CWE-682: Incorrect<br/>Calculation</a>                                   | <b>PASSED</b>         |
| <a href="#">SW</a><br><a href="#">C-1</a><br><a href="#">00</a> | Function<br>Default<br>Visibility    | <a href="#">CWE-710: Improper Adherence<br/>to Coding Standards</a>                  | <b>PASSED</b>         |



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

 **MADE IN GERMANY**