Assure DeFi®

THE VERIFICATION GOLD STANDARD

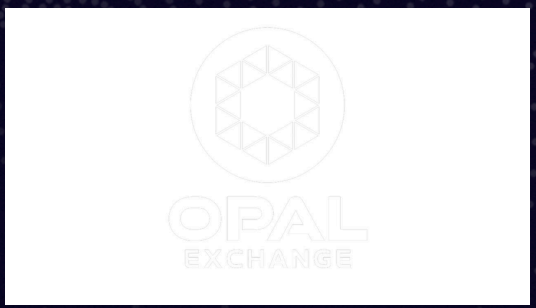
Security Assessment

OPAL

Date: 24/09/2025

Audit Status: PASS

Audit Edition: Advanced



ASSURE DEFI®

THE VERIFICATION GOLD STANDARD

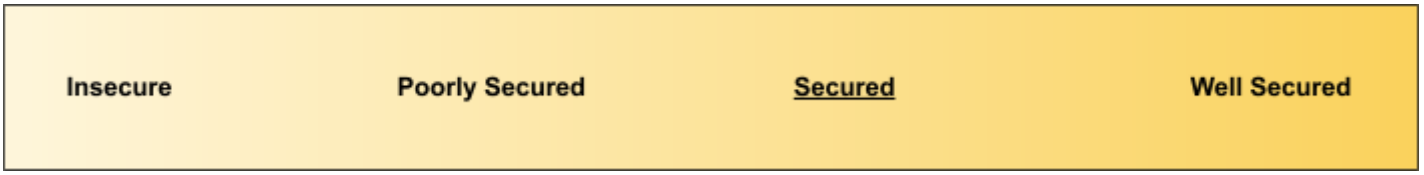
Risk Analysis

Vulnerability summary

Classification	Description
High	High-level vulnerabilities can result in the loss of assets or manipulation of data.
Medium	Medium-level vulnerabilities can be challenging to exploit, but they still have a considerable impact on smart contract execution, such as allowing public access to critical functions.
Low	Low-level vulnerabilities are primarily associated with outdated or unused code snippets that generally do not significantly impact execution, sometimes they can be ignored.
Informational	Informational vulnerabilities, code style violations, and informational statements do not affect smart contract execution and can typically be disregarded.

Executive Summary

According to the Assure assessment, the Customer's smart contract is **Secured.**



Scope

Target Code And Revision

For this audit, we performed research, investigation, and review of the OPAL contracts followed by issue reporting, along with mitigation and remediation instructions outlined in this report.

Target Code And Revision

Project	Assure
Language	Solidity
Codebase	Opal code final.txt [SHA256] - 56abd2e56b53e097cc9dfdf36cadc773c9ec7140c2d6a1f69da28be9628252b0 code allowing usdc (2) [SHA256] - fedd5e0843b042cc2ac9e9bfb906d3b9cacbe66ceab24116917c304d54f7db64 codeusdctest.txt [SHA256] - 0b5fff3721d1dde5f0a5e35eaada84aa02a5fbc7c2e62d1aeb787505dc4a80e5
Audit Methodology	Static, Manual

Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Category	Item
Code review & Functional Review	• Compiler warnings. • Race conditions and Reentrancy. • Cross-function race conditions. • Possible delays in data delivery. • Oracle calls. • Front running. • Timestamp dependence. • Integer Overflow and Underflow. • DoS with Revert. • DoS with block gas limit. • Methods execution permissions. • Economy model. • Private user data leaks. • Malicious Event log. • Scoping and Declarations. • Uninitialized storage pointers. • Arithmetic accuracy. • Design Logic. • Cross-function race conditions. • Safe Zeppelin module. • Fallback function security. • Overpowered functions / Owner privileges

AUDIT OVERVIEW

HIGH

No high severity issues were found.

MEDIUM

1. Tax and tokenomics bypass via unofficial AMM pairs [Fixed ✅]

Function: _transfer, createPair, enableTrading (context)

Issue: Tax is applied only when from == uniswapV2Pair (buy) or to == uniswapV2Pair (sell). Anyone can deploy an alternative Uniswap V2 pair for the token, trades through such pairs won't match these conditions, resulting in permanent tax-free trading that undermines tokenomics.

Recommendation: Track and tax all AMM pairs: maintain mapping(address => bool) isAMMPair, set it on official pair creation and add an owner-only setAMMPair(pair, bool) to register additional pairs. Use isAMMPair[from]/isAMMPair[to] checks in _transfer. Optionally auto-detect known pair factories.

Fix: now track pairs with mapping(address => bool) isAMMPair, set the official pair in createPair(), and expose setAMMPair(address,bool) for owner updates.

_transfer() applies AMM-specific logic using isAMMPair[from] / isAMMPair[to]. This closes the "trade on a rogue pair tax-free" hole.

LOW

---

1. tradingOpen flag is not enforced (trading effectively always open) [Fixed ✅]

Function: _transfer, enableTrading

Issue: Although enableTrading() sets tradingOpen = true, _transfer never checks it. Transfers (including AMM trades) are allowed before “official” launch, contrary to expectation.

Recommendation: Gate transfers if intended:

```
require(tradingOpen || from == owner() || to == owner(), "Trading not open");
```

Optionally restrict only AMM interactions until open.

Fix: _transfer() now gates AMM activity

2. Auto-swap threshold uses stale pre-credit balance snapshot [Fixed ✅]

Function: _transfer

Issue: contractTokenBalance is read before adding the current taxAmount to the contract. This can delay the swap by one transaction because the latest tax isn’t considered in the threshold check.

Recommendation: Read contractTokenBalance after crediting tax (or add taxAmount to the snapshot) before evaluating the swap condition.

Fix: The contract now credit the tax to address(this) before reading contractTokenBalance = balanceOf(address(this)). The check now includes the current tx’s tax.

3. Unused and unenforced transaction/wallet limits [Fixed ✅]

Function: _maxTxAmount, _maxWalletSize; event MaxTxAmountUpdated

Issue: Declared limits are never enforced or updated by any function. This is a misleading configuration without effect.

Recommendation: Either implement enforcement checks in _transfer with admin setters and events, or remove these variables and related events to reduce confusion.

Fix: Fixed by removal.

4. Centralization and sweep authority (non-bug, trust risk) [Acknowledge ✅]

Function: changeTaxWallet, updateTaxSwapThreshold, manualSwap, manualSend, manualSendToken, renounceOwnership

Issue: Admin can change fee wallet and sweep tokens/ETH from the contract, tax wallet can manually drain contract balances. While intended, this centralization requires trust and operational security.

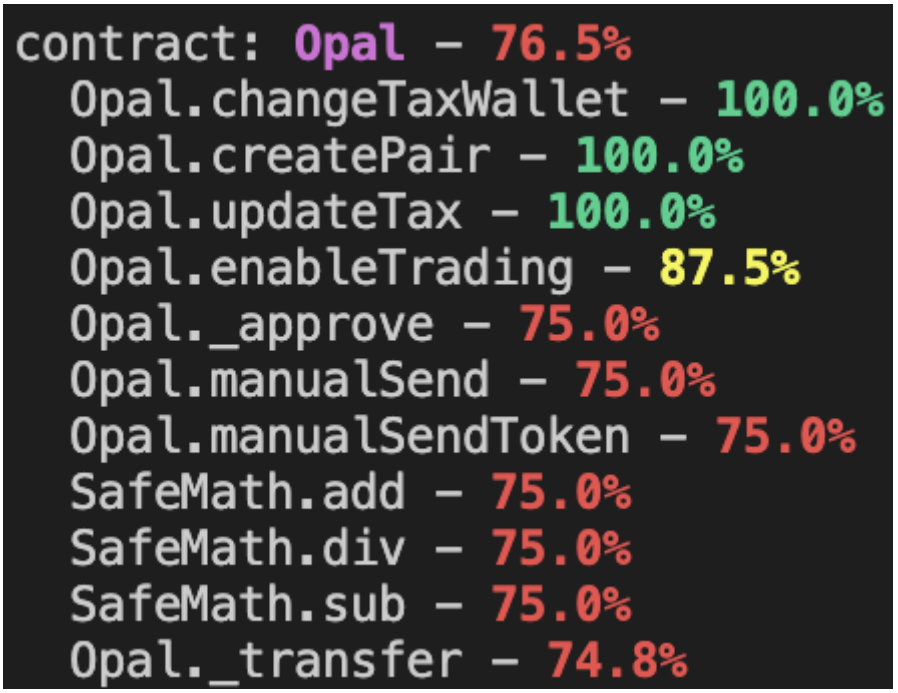
Recommendation: Document powers, consider multisig/timelock for admin actions, emit specific events for manual sweeps, consider renouncing ownership only after configuration is finalized.

INFORMATIONAL

1. Replace the hardcoded USDC address with the real one [if you’are targeting Ethereum Mainnet]

Testing coverage

During the testing phase, custom use cases were written to cover all the logic of contracts. *Check “Annexes” to see the testing code.*



Annexes

Testing code:

```
tests/test_opal.py::test_update_tax RUNNING
Transaction sent: 0x5e498dafd576ea23ae0ac8190f0c88ec53e4422eddce4cc8c0cc4aaffe88f272
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0
  Opal.constructor confirmed   Block: 1   Gas used: 1770687 (14.76%)
  Opal deployed at: 0x3194cBDC3dbcd3E11a07892e7bA5c3394048Cc87

Transaction sent: 0xd0b67c0d7c6c609219bc7cc1053c69cb96935f4be79570290b784d55db4791ac
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0
  Opal.updateTax confirmed (Ownable: caller is not the owner)   Block: 2   Gas used: 22711 (0.19%)

Transaction sent: 0x7c7b2508667421fa13f8702cec02b8fe35f35f6f3ae3e92b0fbfc6ab57c6fd75
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1
  Opal.updateTax confirmed (Can only decrease buy tax)   Block: 3   Gas used: 23519 (0.20%)

Transaction sent: 0xd03076dd4ec437fc43fd5223d9410f0f1aa3a99e7989158d74bbc2137a047c52
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2
  Opal.updateTax confirmed (Can only decrease sell tax)   Block: 4   Gas used: 24345 (0.20%)

Transaction sent: 0xf1cc2df7665f3f872960306b03b8b0e5dc833860d26a06ecd08e4f2099a08342
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3
  Opal.updateTax confirmed   Block: 5   Gas used: 35594 (0.30%)

tests/test_opal.py::test_update_tax PASSED
tests/test_opal.py::test_update_swap_treshold RUNNING
Transaction sent: 0xb1dbe6a280e2802ff029379fb10311d084f072d7fcf0c3a2146d5e63c5f0ae9d
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4
  Opal.constructor confirmed   Block: 6   Gas used: 1770687 (14.76%)
  Opal deployed at: 0xe0aA552A10d7EC8760Fc6c246D391E698a82dDf9

Transaction sent: 0x0a96c6e54b6982a2158e3b04f37cb58b0aeee40be5a012efe0db40c235a1cee6
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1
  Opal.updateTaxSwapThreshold confirmed (Ownable: caller is not the owner)   Block: 7   Gas used: 22462 (0.19%)

Transaction sent: 0xb9f0ee55deb324bc883f75c851f5e1cbb81925993d796519e20c6d0bba5ebfc8
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5
  Opal.updateTaxSwapThreshold confirmed   Block: 8   Gas used: 28405 (0.24%)

tests/test_opal.py::test_update_swap_treshold PASSED
tests/test_opal.py::test_change_tax_wallet RUNNING
Transaction sent: 0x2f5dcf7597d46d4a23ecab96e61e92f8dcb2cbe79afef0c24e54229fb548b1eb
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6
  Opal.constructor confirmed   Block: 9   Gas used: 1770687 (14.76%)
  Opal deployed at: 0x9E4c14403d7d9A8A782044E86a93CAE09D7B2ac9

Transaction sent: 0xb0a882646c57ffa99a89d265c067b3fb4c13361ff923b4ecfcd56b8fffe0ed06
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 2
  Opal.changeTaxWallet confirmed (Ownable: caller is not the owner)   Block: 10   Gas used: 22747 (0.19%)

Transaction sent: 0xf10feadf7a6a52143aba73c90dc267836399ac2d299979a9156538001f86cf1b
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7
  Opal.changeTaxWallet confirmed (Tax wallet cannot be zero address)   Block: 11   Gas used: 22560 (0.19%)

Transaction sent: 0xf315eeb38f2383c28666380d7dd63cc3d923200282bf37f8f087f1dbfd532cb0
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8
  Opal.changeTaxWallet confirmed   Block: 12   Gas used: 30063 (0.25%)

tests/test_opal.py::test_change_tax_wallet PASSED
```

```
tests/test_opal.py::test_transfer RUNNING
Transaction sent: 0x075d8e5602d809184df1419c32506d903f264706abbe9ffceaa7696ad9175a70
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 9
  UniswapV2Factory.constructor confirmed   Block: 13   Gas used: 2412742 (20.11%)
  UniswapV2Factory deployed at: 0xa3B53dDCd2E3fC28e8E130288F2aBD8d5EE37472

Transaction sent: 0xe12acafa81b246daf37dac57320532b6ff1f73cf8f2c24453c81342a764be0b0
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 10
  WETH9.constructor confirmed   Block: 14   Gas used: 476546 (3.97%)
  WETH9 deployed at: 0xb6286fAFd0451320ad6A8143089b216C2152c025

Transaction sent: 0x0d693be4590e141c8c3ab00f57b1325d9d48d17d495e25eae24edaa1041acc01
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 11
  UniswapV2Router02.constructor confirmed   Block: 15   Gas used: 3895430 (32.46%)
  UniswapV2Router02 deployed at: 0x7a3d735ee6873f17Dbdcab1d51B604928dc10d92

Transaction sent: 0xc99ba6c03bb054827850da9e8430493f7772ffa6c343e671d1f557b9aaadaa04
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 12
  Opal.constructor confirmed   Block: 16   Gas used: 1770687 (14.76%)
  Opal deployed at: 0x2c15A315610Bfa5248E4CbCbd693320e9D8E03Cc

Transaction sent: 0xeb409db2b18eb5a3587f23fa3c27b479aa3ebdbe110ad8be7825a2c6ed8aee46
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0
  Opal.transfer confirmed (ERC20: transfer from the zero address)   Block: 17   Gas used: 22172 (0.18%)

Transaction sent: 0xb075abdfb9fe059465eed3766fe768326baf0d214b579775b691443c0a87f31c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 3
  Opal.transfer confirmed (ERC20: transfer to the zero address)   Block: 18   Gas used: 21967 (0.18%)

Transaction sent: 0x2f928bd418c28036d0a17c7d0a3b6cebbac2b12faee44a08d10163194be7a0a7
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 4
  Opal.transfer confirmed (Transfer amount must be greater than zero)   Block: 19   Gas used: 22182 (0.18%)

Transaction sent: 0x440e8c656a28f39b5047b7844f7f41dad2cfcceb2e22d401852254d4da4ff3ce
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 5
  Opal.enableTrading confirmed (Ownable: caller is not the owner)   Block: 20   Gas used: 22218 (0.19%)

Transaction sent: 0x975d2e746e53d043b0cae0eded0dab5233c3dc7882f631ea77d99b76d765334c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 13
  Opal.enableTrading confirmed (Pair not created yet)   Block: 21   Gas used: 23884 (0.20%)

Transaction sent: 0x0f3f9d7205a44c92be466f7b2fcb2fa00bf532eea9a68dc5c3388fce37741905
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 6
  Opal.createPair confirmed (Ownable: caller is not the owner)   Block: 22   Gas used: 22826 (0.19%)

Transaction sent: 0x1d546c05c0c6ac4861328c49386c6828adbfc53f5f1ff2005f0f313dc9980d2c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 14
  Opal.createPair confirmed   Block: 23   Gas used: 2091377 (17.43%)

Transaction sent: 0xe00f145db8377701f5ce312bf64c759db27035b9d42379dded48a3d3f423ff1c
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 15
  Opal.createPair confirmed (Pair already created)   Block: 24   Gas used: 23652 (0.20%)

Transaction sent: 0xa30b3f49abab9e4a9f55b303915ca27da1b0610bbd35fce5cc363e2110ba8bcc
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 16
  Opal.enableTrading confirmed   Block: 25   Gas used: 53872 (0.45%)

Transaction sent: 0x536467fcd8f87342a12e85eff1cc86bdeb196abb3f8df2b1190cba27259b2eaa
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 17
  Opal.enableTrading confirmed (Trading is already open)   Block: 26   Gas used: 23043 (0.19%)

Transaction sent: 0x45a9874aa632194d88451fe211cc19f45f0a7c1651a43653751c57ccd955cf55
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 18
  Opal.transfer confirmed   Block: 27   Gas used: 54544 (0.45%)

Transaction sent: 0x76cb351dfad55722147009bfd32a9ce5d371edcede7e5b7be1fedefe93c208f3
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 19
  Opal.transfer confirmed   Block: 28   Gas used: 54532 (0.45%)

Transaction sent: 0x3e5dd71409dcf3ab479a328cb934f80095c6f58a78d2f4a2195099315c6bf217
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 7
  Opal.transfer confirmed   Block: 29   Gas used: 47191 (0.39%)

Transaction sent: 0x6aa80e55ddc86412945caa5e4283c67955c9cafa6c41194aebc766bc6e1173aa
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 20
  Opal.updateTax confirmed   Block: 30   Gas used: 31394 (0.26%)
```

```
Transaction sent: 0xe273d4445482398eb79f19ca121e1644c26469ea100ebdf40ba123be98dcfb85
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 8
  Opal.transfer confirmed   Block: 31   Gas used: 87312 (0.73%)

Transaction sent: 0xa78ceeb700d96823a0bf56b1809517e59dd4ca13b177c13e6641ab873d1eba94
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1
  Opal.transfer confirmed   Block: 32   Gas used: 75673 (0.63%)

Transaction sent: 0x742eb63320aa7033c77e1d5744bca7079dbd38276134139f4bc9e132a6881825
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 0
  Opal.manualSendToken confirmed   Block: 33   Gas used: 49649 (0.41%)

Transaction sent: 0x6e3302f006ed168a5241a1060c41423b7aac2ced037b96be74bb1f0971f82392
  Gas price: 0.0 gwei   Gas limit: 12000000   Nonce: 1
  Opal.manualSend confirmed   Block: 34   Gas used: 23823 (0.20%)

tests/test_opal.py::test_transfer PASSED
```

Technical Findings Summary

Findings

Vulnerability Level		Total	Pending	Not Apply	Acknowledged	Partially Fixed	Fixed
	HIGH	0					
	MEDIUM	1					1
	LOW	4			1		3
	INFORMATIONAL	1					

Assessment Results

Score Results

Review	Score
Global Score	**90/100**
Assure KYC	Not completed
Audit Score	90/100

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

Audit PASS

Following our comprehensive security audit of the token contract for the OPAL project, the project did meet the necessary criteria required to pass the security audit.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocating for the Project, and users relying on this report should not consider this as having any merit for financial adOPAL in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment adOPAL, nor should it be used to signal that any person reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided ‘as is, and Assure Defi is under no covenant to audit completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment serOPALs provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any serOPALs, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The serOPALs may access, and depend upon, multiple layers of third parties.