

# KISHIELD

Security Audit

**Salah ad-Din Token**

May 28, 2022



Audit Passed



# Table of Contents

## **1 Audit Summary**

## **2 Project Overview**

### 2.1 Token Summary

### 2.2 Main Contract Assessed

## **3 Smart Contract Vulnerability Checks**

## **4 Contract Ownership**

### 4.1 Privileged Functions

## **5 Important Notes To The Users**

## **6 Findings Summary**

### 6.1 Classification of Issues

### 6.1 Findings Table

#### 01 Public function that could be declared external

#### 02 Missing events arithmetic

## **7 Statistics**

### 7.1 Liquidity

### 7.2 Token Holders

### 7.3 Liquidity Holders

## **8 Liquidity Ownership**

## **9 Disclaimer**



# Audit Summary

This report has been prepared for Salah ad-Din Token on the Polygon network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

# Project Overview

## Token Summary

Parameter	Result
Address	0x589316714A657603397c1FceAD5E5C2Ef8824B82
Name	Salah ad-Din
Token Tracker	Salah ad-Din (SALAH)
Decimals	18
Supply	1,000,000,000,000
Platform	Polygon
compiler	v0.8.4+commit.c7e474f2
Optimization	Yes with 1 runs
LicenseType	MIT
Language	Solidity
Codebase	<a href="https://polygonscan.com/address/0x589316714A657603397c1FceAD5E5C2Ef8824B82#code">https://polygonscan.com/address/0x589316714A657603397c1FceAD5E5C2Ef8824B82#code</a>
Url	<a href="https://Salah.finance">https://Salah.finance</a>

## Main Contract Assessed

Name	Contract	Live
Salah ad-Din	0x589316714A657603397c1FceAD5E5C2Ef8824B82	Yes

# Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	✓ Low / No Risk
Code With No Effects	Complete	Complete	✓ Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	✓ Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	✓ Low / No Risk
Unexpected Ether balance	Complete	Complete	✓ Low / No Risk
Presence of unused variables	Complete	Complete	✓ Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	✓ Low / No Risk
Typographical Error	Complete	Complete	✓ Low / No Risk
DoS With Block Gas Limit	Complete	Complete	✓ Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	✓ Low / No Risk
Insufficient Gas Griefing	Complete	Complete	✓ Low / No Risk
Incorrect Inheritance Order	Complete	Complete	✓ Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	✓ Low / No Risk
Requirement Violation	Complete	Complete	✓ Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	✓ Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	✓ Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	✓ Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	✓ Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	✓ Low / No Risk
Assert Violation	Complete	Complete	✓ Low / No Risk
Reentrancy	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Value	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow and Underflow	Complete	Complete	✓ Low / No Risk
Function Default Visibility	Complete	Complete	✓ Low / No Risk

## Contract Ownership

The contract ownership of Salah ad-Din is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x30de33f6f557acd66e7919b9379044e2de4294b6 which can be viewed from: [HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

## Important Notes To The Users:

- The contract is well made and is secure. At no point the owner can stop users from selling or take control over users funds.
- The owner cannot stop trading.
- The owner cannot mint new tokens after deployment.
- The owner cannot blacklist wallets, only contracts.
- The owner cannot set buy/sell fees over 24%
- Once the owner renounces ownership of the contract, none of the following are applicable.
- Owner can change the buy and sell fees up to 12% respectively.
- Owner can add/remove contracts addresses from the blacklist.
- Owner can enable/disable the tax mechanism.
- Owner can trigger the tax mechanism, to send the accumulated fees to the respective wallets.
- Owner can add/remove wallets from fee exemption.
- No high-risk Exploits/Vulnerabilities Were Found in token Source Code.

## Audit Passed



# Technical Findings Summary

## Classification of Issues

Severity	Description
● High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency
● Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
● Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
● Info	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

## Findings

Severity	Found
● High	0
● Medium	0
● Low	0
● Info	2
Total	2



# Findings

## Public function that could be declared external

ID	Severity	Contract	Function
01	● Informational	Salah ad-Din	Functions: transferOwnership, renounceOwnership

### Description

Gas Optimization. Public function that could be declared external

### Recommendation

Public functions that are never called by the contract should be declared external to save gas.

## Missing events arithmetic

ID	Severity	Contract	Function
02	● Informational	Salah ad-Din	Missing events for setBuyTax, setSellTax

### Description

Functions that change critical arithmetic parameters should emit an event.

### Recommendation

Emit corresponding events for critical parameter changes.

## Privileged Functions (onlyOwner & Others)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
triggerTax	none	public
burn	uint256 amount	public
enableBlacklist	address account	public
disableBlacklist	address account	public
exclude	address account	public
removeExclude	address account	public
setBuyTax	uint256 dev, uint256 marketing, uint256 liquidity, uint256 charity	public
setSellTax	uint256 dev, uint256 marketing, uint256 liquidity, uint256 charity	public
setTaxWallets	address dev, address marketing, address charity	public
enableTax	none	public
disableTax	none	public

# Statistics

## Liquidity Info

Parameter	Result
Pair Address	0xeb2fee0b6968e441a9fc6d0b42090fc8b9dc81ba
SALAH Reserves	0.00 SALAH
MATIC Reserves	0.00 MATIC
Liquidity Value	\$0 USD

## Token (SALAH) Holders Info

Parameter	Result
SALAH Percentage Burnt	0.00%
SALAH Amount Burnt	0 SALAH
Top 10 Percentage Own	100.00%
Top 10 Amount Owned	1,000,000,000,000 SALAH
Top 10 Aprox Value	\$NaN USD

## LP (SALAH/MATIC) Holders Info

Parameter	Result
SALAH/MATIC % Burnt	0.00%
SALAH/MATIC Amount Burnt	0 SALAH/MATIC
Top 10 Percentage Owned	0.00%
Top 10 Amount Owned	0 SALAH/MATIC
Locked Tokens Percentage	0.00%
Locked Tokens Amount	0 SALAH/MATIC

\* All the data displayed above was taken on-chain at block 28888501

\* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

## Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 28888501

# KISHIELD



## Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that 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 completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD 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 and/or actions with regards to the information provided in this audit report.

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