Royalproof

Security Audit Report

Completed on

Feb,06,2023

OVERWIEW

This audit has been prepared for **HedgePay** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

"The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal "

- RoyalProof Team -

TABLE OF CONTENTS

PROJECT DESCRIPTION

According to their website:

Hedgepay is staking platform which will pay rewards in form of $BUSD and $HPAY to its users. The required staking amount to receive rewards is 1,000,000 $HPAY tokens. The future plans of Hedgepay are Dapp wallet UI, HedgePay fiat brige, cross-chain integration, collateral and lending, AI guided investment customization, HedgePay card and payment processing services.

Team:

KYCed with PinkSale.

CONTRACT INFO

contract Name	HedgeToken
Ticker	HPAY
Contract Address	0xC75aa1Fa199EaC5adaBC832eA4522Cff6dFd521A
Network	Binance Smart Chain
Language	Solidity
Initial supply	250,000,000
Initial Burn	200,575,875
Circulating supply	49,424,124
Max supply	1,000,000,000 -Mint Function available
MaxTxAmount	No limit
Status	Not launched yet

TAXES

Buy Tax	18 %
Sell Tax	20 %

Our Contract Review Process

The contract review process pays special attention to the following:

Testing the smart contracts against both common and uncommon vulnerabilities

- ❖ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ❖ Ensuring contract logic meets the specifications and intentions of the client.
- ❖ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ❖ Thorough line-by-line manual review of the entire codebase by industry experts.

- ❖ Blockchain security tools used:
- ✓ Open Zeppelin
- ✓ Mythril
- ✓ Solidity Compiler
- ✓ Hardhat

CURRENT STATS

(As of Sep 26, 2022)

Status: Not Launched

Liquidity: Not added yet

Burn: No burnt tokens

MaxTxAmount: 20,000,000,000,000

DEX: PancakeSwap

LP Address(es): Liquidity not added yet.

TOKEN TRANSFERS STATS

Transfer Count	54
Uniq Senders	6
Uniq Receivers	25
Total Amount	1487817393 HPAY
Median Transfer Amount	104339 HPAY
Average Transfer Amount	27552173 HPAY
First transfer date	2021-12-12
Last transfer date	2022-01-31
Days token transferred	53 days

SMART CONTRACT STATS

Calls Count	---------
External calls	--------
Internal calls	--------
Transactions count	--------
Uniq Callers	-------
Days contract called	--------
Last transaction time	--------
Created	---------
Create TX	----------
Creator	----------

FEATURED WALLETS

FeeManager	0xb1588ca2529ff4f1a8e21d6fe24ba6d0b6e000b0
LP token address	Liquidity not provided yet
Deploy/Owner	0x346abB57CfB43aD3Bb8210E3DD1dB12353160A0b
Reward Manager	0x020f50300c85ee89cfcd73e1a46d55e9e9a93844

*Address can be changed in future

TOP 3 UNLOCKED WALLETS

Wallet 1 (1.57%)	0x6c7f7aef7ca6412020409704 78e3a6235c9673a1
Wallet 2 (1.26%)	0x2a2873c29a93d90e164b72da332eca3a181d9983
Wallet 3 (1.06%)	0xf4efed3f70d86bb875ba70dd5701d8f9a006d046

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer Overflow and Underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk-free factor.

THREAT LEVELS

- **Owner can mint new tokens.**

```
function mint(address to, uint256 amount) public virtual {
    require(hasRole(MINTER_ROLE, _msgSender()),
    "ERC20PresetMinterPauser: must have minter role to mint");
    _mint(to, amount);
}
```

- **Owner can pause trading.**

```
function pause() public virtual {
    require(hasRole(PAUSER_ROLE, _msgSender()),
    "ERC20PresetMinterPauser: must have pauser role to pause");
    _pause();
}
```

- **Owner can buy/sell Fees up to 100%.**

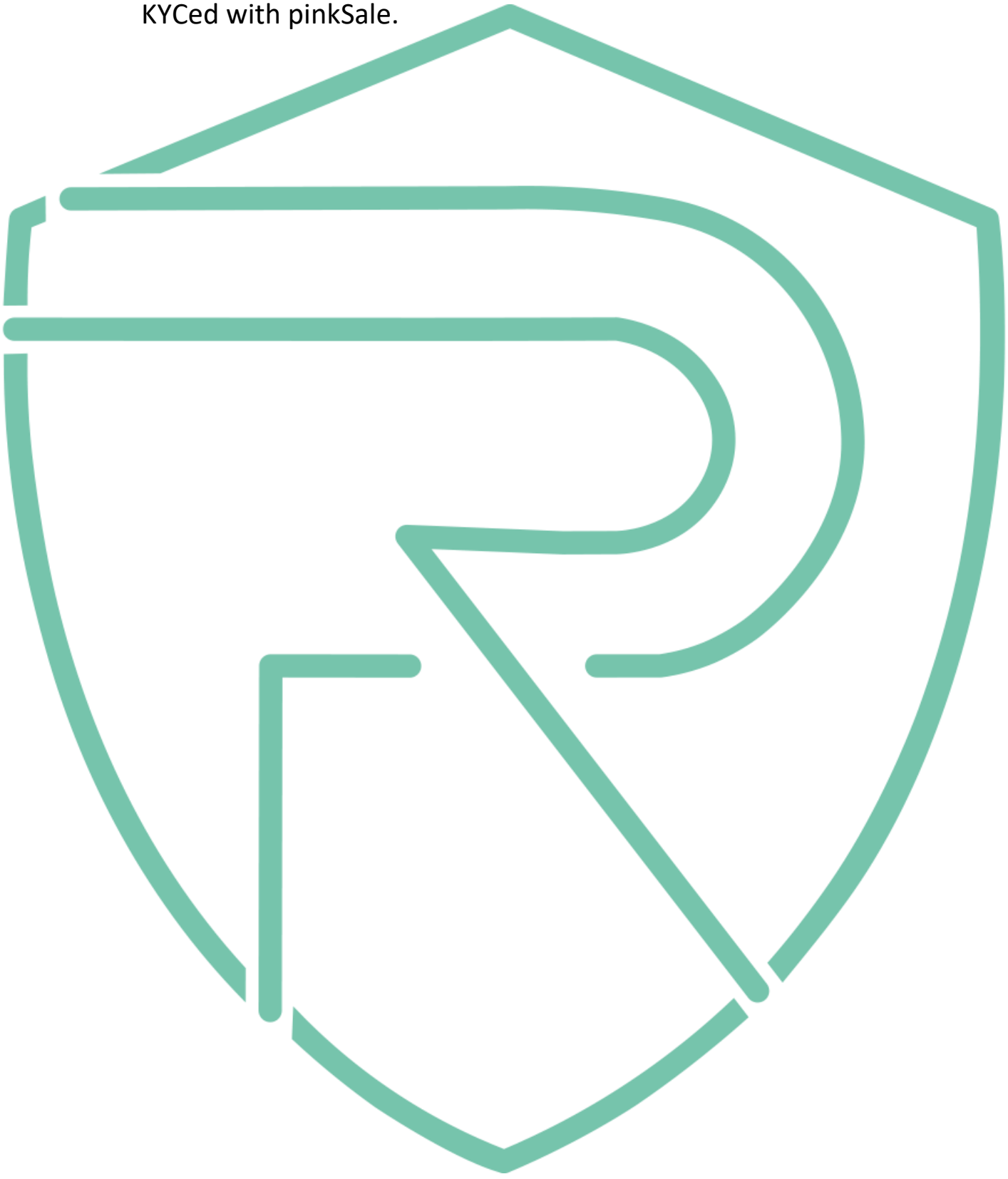
```
function setBuyFee(uint8 newFee) external onlyRole(DEFAULT_ADMIN_ROLE) {
    require(newFee <= 100, "Fee cannot be greater than 100%");
    buyFee = newFee;
}

function setSellFee(uint8 newFee) external onlyRole(DEFAULT_ADMIN_ROLE) {
    require(newFee <= 100, "Fee cannot be greater than 100%");
    sellFee = newFee;
}
```

Tokenomics:

There is no information about initial tokens distribution on the project's whitepaper and/or website.

THE TEAM

KYCed with pinkSale.



Website

Website URL	hedgepay.org
Domain Registry	whois.namecheap.com
Domain Expiration	Expires on 2024-10-28
Technical SEO Test	Passed
Security Test	Passed. SSL certificate present

Design	• Nice color gradient and overall layout
Whitepaper	• well written and explanatory.
Content	• The information helps new investors understand what the product does right away. No grammar errors found.
Roadmap	• Well defined goals.
Mobile-friendly?.	• Yes

HedgePay.org

SOCIAL MEDIA& ONLINE PRESENCE

ANALYSIS

Project's social media pages are very active with activity from organic users

Twitter : @HedgePay_

- 9 054 Followers
- active
- Low engament from audience

Telegram : @hedgepay

- 8 785 members
- Few Active members
- Active mods & devs

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

RoyalProof

CRYPTO SECURITY

Audits | KYCs | dApps

Contract Development

FIND US ONLINE

https://royalproof.net/

@RoyalproofAudit

@RoyalProofOfficial

https://github.com/Royal-Proof

@RoyalProofAudit

@Royalproof_Admin

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and Royal Proof and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Royal Proof) owe no duty of care towards you or any other person, nor does Royal Proof make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Royal Proof hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Royal Proof hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Royal Proof, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.