



Royalproof

Security Audit Report



Completed on

30,01,2023

royalproof.net



OVERVIEW

This audit has been prepared for **MetaRuffy** 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

OVERVIEW	2
TABLE OF CONTENTS	3
PROJECT DESCRIPTION	4
CONTRACT INFO	5
OUR CONTRACT REVIEW PROCESS	6
CURRENT STATS	7
TOKEN TRANSFERS STATS	8
SMART CONTRACT STATS	8
FEATURED WALLETS	9
VULNERABILITY CHECK	10
THREAT LEVELS	11
TOKENOMICS:	14
THE TEAM	15
WEBSITE	16
SOCIAL MEDIA& ONLINE PRESENCE	17
DISCLAIMER	19



PROJECT DESCRIPTION

MetaRuffy is an open world in the Metaverse based on the latest technology which merges together, web3.0, blockchain, VR and AR. With Meta Ruffy you enter a world, where the creation of entertainment is the essence within its metaverse. The creation and full development of Ruffy World is the main goal and the ultimate milestone for the project. A fully developed and fully functional Ruffy World environment with all its assets in place is the big picture.

Release Date: Presale starts on Oct. 03, 2022

Category: Metaverse



CONTRACT INFO

Token Name	METARUFFY
Symbol	MR
Contract Address	0xa4Cb3ef5f41a4D89D6FCed22ea8a1C57957629Aa
Network	Ethereum
Language	Solidity
Deployment Date	17.Sep.2022
Verified?	Yes
Total Supply	300,000,000,000
Status	Not launched

TAXES

Buy Tax	4 %
Sell Tax	4 %



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: 17.33 % of total supply

MaxTxAmount: No limit

DES: Uniswap

LP Address(es): Liquidity not added yet



TOKEN TRANSFERS STATS

Transfer Count	11
Uniq Senders	2
Uniq Receivers	4
Total Amount	599999999999.9999 MR
Median Transfer Amount	24999999999.999996 MR
Average Transfer Amount	54545454545.45454 MR
First transfer date	2022-09-17
Last transfer date	2022-09-25
Days token transferred	2

SMART CONTRACT STATS

Calls Count	35
External calls	7
Internal calls	28
Transactions count	16
Uniq Callers	3
Days contract called	3
Last transaction time	2022-09-25 23:05:23 UTC
Created	2022-09-23 22:08:11 UTC
Create TX	0x29ce5beb4bfcc7ea40109468b6453ad347db0a474b59f96064238361e27a93f4
Creator	0x49273b37ad4bbb7b85c292a540f39e4cac9e6277



FEATURED WALLETS

Owner address	0x49273b37ad4bbb7b85c292a540f39e4cac9e6277
*Marketing fee receiver	0x0a5e73df3836677eb7e22cb782e1cbfdc56da22a
Dev fee receiver	0x26f3f79e5777c72de8432e438adcfb1c799064c9
LP address	Liquidity not added yet

*Address can be changed in future



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.



- **Medium Risk**

If marketing divider variable is set above 100 and contract's token balances are above the swap Threshold, selling will fail.

```
event UpdateMarketingDivider(uint256 _newPercent);
function updateMarketingDivider(uint256 _newPercent) external onlyOwner {
    require(_newPercent >= 25, "Marketing divider is low.");
    marketingDivider = _newPercent;
    emit UpdateMarketingDivider(_newPercent);
}

function sendETHToWallets() internal {
    uint256 balance = address(this).balance;
    if(balance > 0) {
        uint256 _marketingFee = balance.mul(marketingDivider).div(10**2);
        uint256 _devFee = balance.sub(_marketingFee);
        if(_marketingFee > 0) {
            payable(marketingFeeReceiver).transfer(_marketingFee);
        }
        if(_devFee > 0) {
            payable(devFeeReceiver).transfer(_devFee);
        }
    }
}
```

- **Recommendation:**
 - Restrict the marketingDivider variable values in scope from 0 to 100.



- **Informational**

Owner can buy and sell fees up to 10%. Combined buy+sell = 20%.

```
event UpdateBuyFees(uint256 _marketingFee, uint256 _devFee, uint256 _burnFee);
function updateBuyFees(uint256 _marketingFee, uint256 _devFee, uint256 _burnFee) external onlyOwner {
    require(_marketingFee.add(_devFee).add(_burnFee) <= 10, "METARUFFY: Max fee limit exceeds");
    buyMarketingFee = _marketingFee;
    buyDevFee = _devFee;
    buyBurnFee = _burnFee;
    emit UpdateBuyFees(_marketingFee, _devFee, _burnFee);
}

event UpdateSellFees(uint256 _marketingFee, uint256 _devFee, uint256 _burnFee);
function updateSellFees(uint256 _marketingFee, uint256 _devFee, uint256 _burnFee) external onlyOwner {
    require(_marketingFee.add(_devFee).add(_burnFee) <= 10, "METARUFFY: Max fee limit exceeds");
    sellMarketingFee = _marketingFee;
    sellDevFee = _devFee;
    sellBurnFee = _burnFee;
    emit UpdateSellFees(_marketingFee, _devFee, _burnFee);
}
```

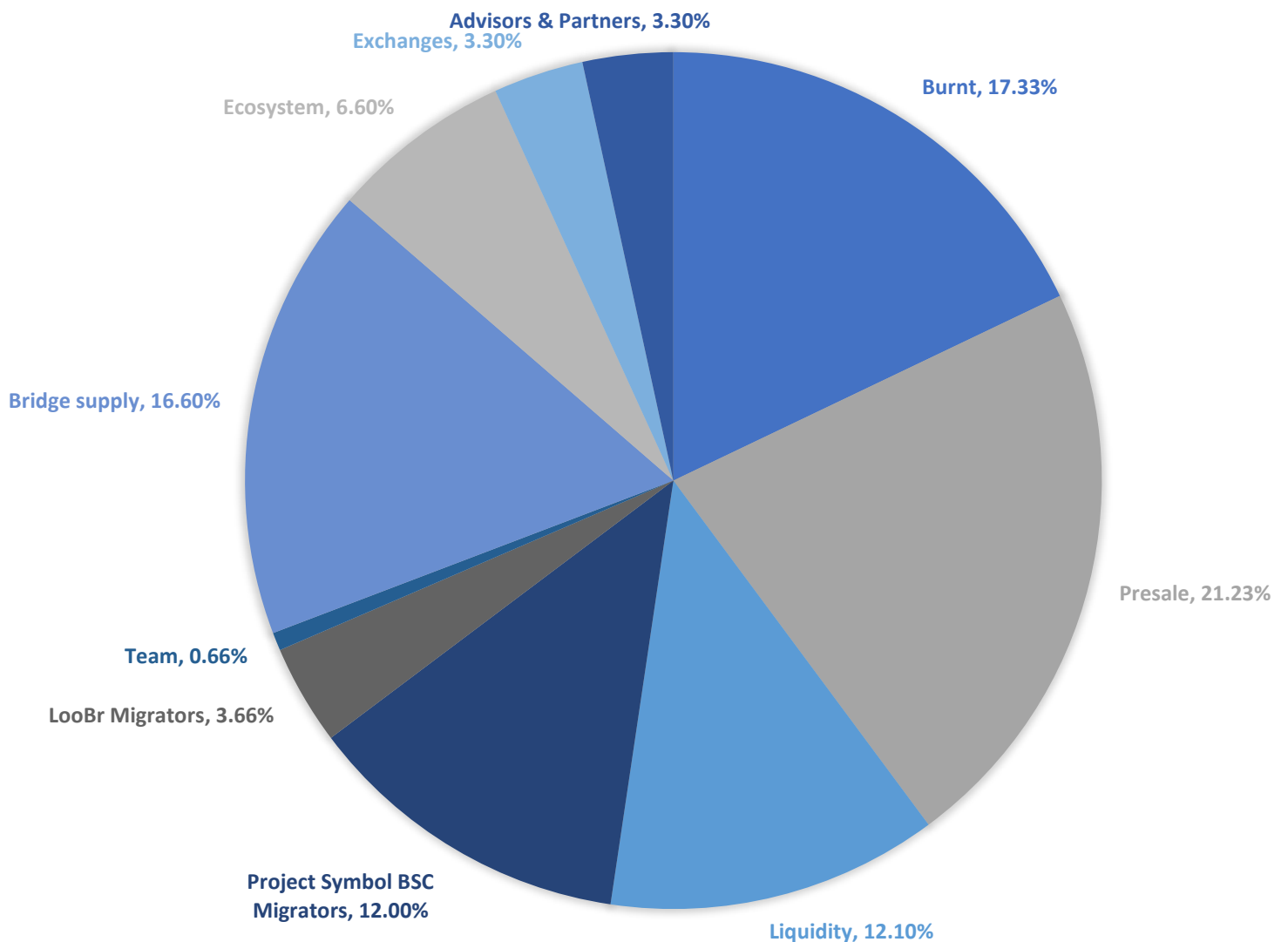
- **Owner can exclude address from fees.**

```
function exemptFromFee(address account, bool _exempt) external onlyOwner {
    isFeeExempt[account] = _exempt;
    emit ExemptFromFee(account, _exempt);
}
```



Tokenomics:


Burnt	17,33%
Presale	21,23%
Liquidity	12,10%
Project Symbol BSC Migrators	12,00%
LooBr Migrators	3,66%
Team	0,66%
Bridge supply	16,60%
Ecosystem	6,60%
Exchanges	3,30%
Advisors & Partners	3,30%






THE TEAM

The team at **MetaRuffy** is publicly doxxed on their website and socials with a KYC from Pinksale.




CIHAN
CEO, FOUNDER




FOX
COO, OPERATING



SAFI
CTO, IT



RAMEEN
CFO




ANNA MARIA
CCO, CREATIVE




KENPACHI
LEAD Business Dev & Innovation



VOLODYMYR
BLOCKCHAIN DEVLEOPER



DANIEL
LEAD STRATEGIC ADVISOR



ANDRE
HEAD OF SOCIAL MEDIA





Website

Website URL	https://metaruffy.io/
Domain Registry	https://www.key-systems.net/
Domain Expiration	Expires on 2023-01-02
Technical SEO Test	Passed
Security Test	Passed. SSL certificate present

Design

- Very nice color scheme and overall layout.

Whitepaper

- Well written, explanatory.
- The information helps new investors understand what the product does right away. No grammar mistakes found..

Content

Roadmap Mobile- friendly?.

- Yes, goals set without time frames..
- Yes

[Metaruffy.io](https://metaruffy.io/)



SOCIAL MEDIA& ONLINE PRESENCE

ANALYSIS

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



Twitter : @meta_ruffy

- 13 300 Followers
- Very active
- Posts few times a day



Discord : @metaruffy

- 1538 members
- Active community and mods



Telegram : @metaruffy_international

- 11 528 members
- Active members
- Active mods



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.