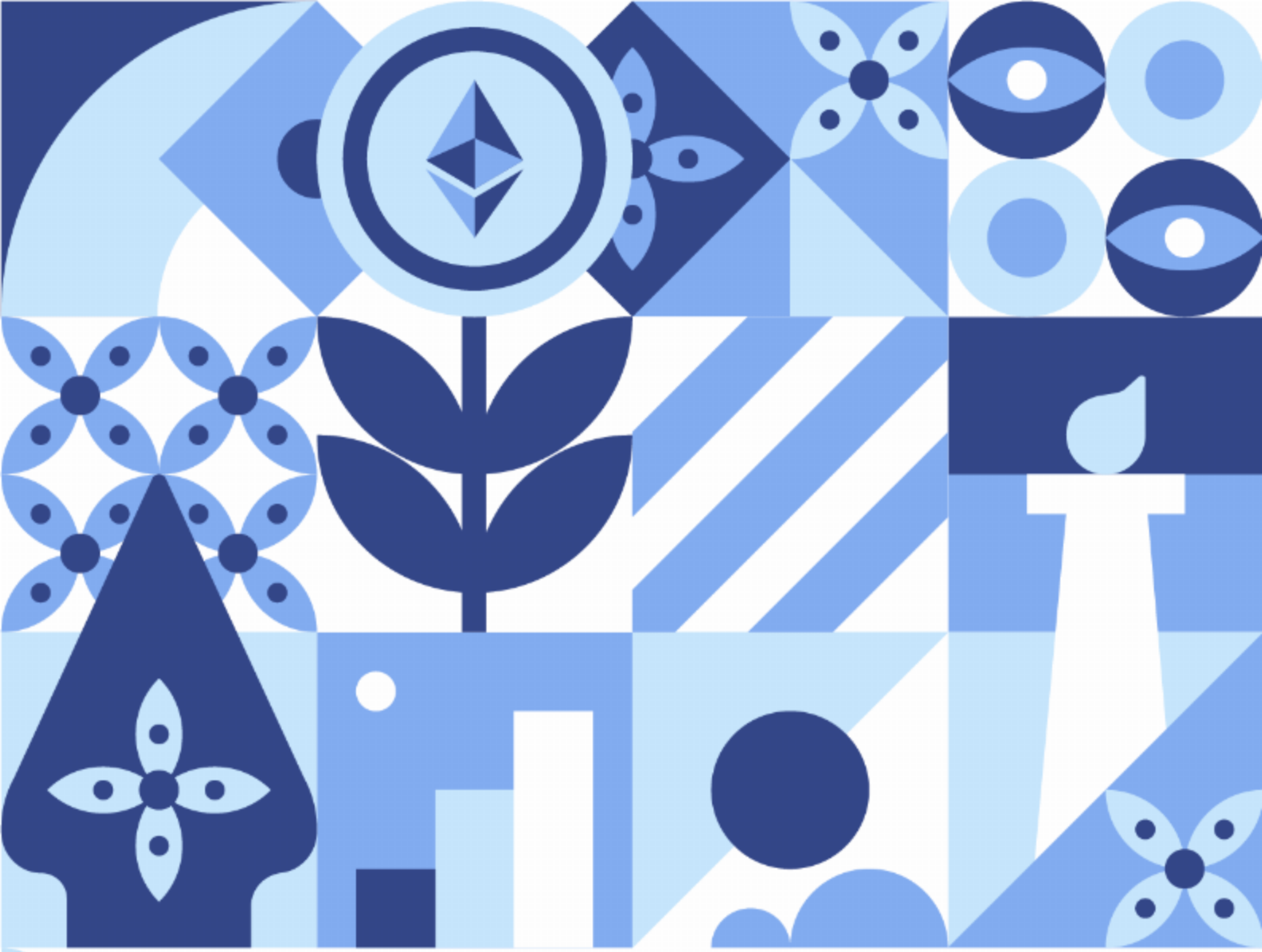

BRB Cash

Smart Contract Audit Report

SYSFIXED

10 Nov 2022

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
BRB Cash	BRBC	Ethereum

Addresses

Contract address	0x02130d419dc3c0e73fb9d028741ccabbd2d31062
Contract deployer address	0x9653fAb1EDB1704FbA4838E1Be129C8cB9d3cd52

Project Website

https://brbinc.us/

Codebase

https://etherscan.io/address/0x02130d419dc3c0e73fb9d028741ccabbd2d31062#code

SUMMARY

BRBC is an ERC-20 utility token used in a cross-chain ecosystem with utilities to support a WEB3 marketplace. By incorporating WEB3 utilities and explicitly using the Ethereum blockchain, we are also reducing the overall energy consumed.

Contract Summary

Documentation Quality

BRB Cash provides a very good documentation with standard of solidity base code.

- The technical description is provided clearly and structured and also dont have any high risk issue.

Code Quality

The Overall quality of the basecode is standard.

- Standard solidity basecode and rules are already followed by BRB Cash with the discovery of several low issues.

Test Coverage

Test coverage of the project is 100% (Through Codebase)

Audit Findings Summary

- SWC-100 SWC-108 | Explicitly define visibility for all state variables on lines 395.
- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 23, 31, 37, 38, 45, 51, 55, 58, 61, 64, 67, 72, 78, 84, 380, 380, 381, 381, 397, 397, 398, 398, 500, 502, 538, 577, 601, 606, 611 and 502.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 7.
- SWC-110 SWC-123 | It is recommended to use of revert(), assert(), and require() in Solidity, and the new REVERT opcode in the EVM on lines 501, 502, 502, 578, 578, 579, 580, 679 and 680.

CONCLUSION

We have audited the BRB Cash project released on November 2022 to discover issues and identify potential security vulnerabilities in BRB Cash Project. This process is used to find technical issues and security loopholes which might be found in the smart contract.

The security audit report provides a satisfactory result with some low-risk issues.

The issues found in the BRB Cash smart contract code do not pose a considerable risk. The writing of the contract is close to the standard of writing contracts in general. The low-risk issues found are some arithmetic operation issues, a floating pragma is set, a state variable visibility is not set, and out of bounds array access which the index access expression can cause an exception in case of the use of an invalid array index value. It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

AUDIT RESULT

Article	Category	Description	Result
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	ISSUE FOUND
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	ISSUE FOUND
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	PASS
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	ISSUE FOUND
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	PASS
Unprotected Ether Withdrawal	SWC-105	Due to missing or insufficient access controls, malicious parties can withdraw from the contract.	PASS
SELFDESTRUCT Instruction	SWC-106	The contract should not be self-destructible while it has funds belonging to users.	PASS
Reentrancy	SWC-107	Check effect interaction pattern should be followed if the code performs recursive call.	PASS
Uninitialized Storage Pointer	SWC-109	Uninitialized local storage variables can point to unexpected storage locations in the contract.	PASS
Assert Violation	SWC-110 SWC-123	Properly functioning code should never reach a failing assert statement.	ISSUE FOUND
Deprecated Solidity Functions	SWC-111	Deprecated built-in functions should never be used.	PASS
Delegate call to Untrusted Callee	SWC-112	Delegatecalls should only be allowed to trusted addresses.	PASS

DoS (Denial of Service)	SWC-113 SWC-128	Execution of the code should never be blocked by a specific contract state unless required.	PASS
Race Conditions	SWC-114	Race Conditions and Transactions Order Dependency should not be possible.	PASS
Authorization through tx.origin	SWC-115	tx.origin should not be used for authorization.	PASS
Block values as a proxy for time	SWC-116	Block numbers should not be used for time calculations.	PASS
Signature Unique ID	SWC-117 SWC-121 SWC-122	Signed messages should always have a unique id. A transaction hash should not be used as a unique id.	PASS
Incorrect Constructor Name	SWC-118	Constructors are special functions that are called only once during the contract creation.	PASS
Shadowing State Variable	SWC-119	State variables should not be shadowed.	PASS
Weak Sources of Randomness	SWC-120	Random values should never be generated from Chain Attributes or be predictable.	PASS
Write to Arbitrary Storage Location	SWC-124	The contract is responsible for ensuring that only authorized user or contract accounts may write to sensitive storage locations.	PASS
Incorrect Inheritance Order	SWC-125	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order. The rule of thumb is to inherit contracts from more /general/ to more /specific/.	PASS
Insufficient Gas Griefing	SWC-126	Insufficient gas griefing attacks can be performed on contracts which accept data and use it in a sub-call on another contract.	PASS
Arbitrary Jump Function	SWC-127	As Solidity doesnt support pointer arithmetics, it is impossible to change such variable to an arbitrary value.	PASS

Typographical Error	SWC-129	A typographical error can occur for example when the intent of a defined operation is to sum a number to a variable.	PASS
Override control character	SWC-130	Malicious actors can use the Right-To-Left-Override unicode character to force RTL text rendering and confuse users as to the real intent of a contract.	PASS
Unused variables	SWC-131 SWC-135	Unused variables are allowed in Solidity and they do not pose a direct security issue.	PASS
Unexpected Ether balance	SWC-132	Contracts can behave erroneously when they strictly assume a specific Ether balance.	PASS
Hash Collisions Variable	SWC-133	Using abi.encodePacked() with multiple variable length arguments can, in certain situations, lead to a hash collision.	PASS
Hardcoded gas amount	SWC-134	The transfer() and send() functions forward a fixed amount of 2300 gas.	PASS
Unencrypted Private Data	SWC-136	It is a common misconception that private type variables cannot be read.	PASS

SMART CONTRACT ANALYSIS

Started	Wednesday Nov 09 2022 10:05:41 GMT+0000 (Coordinated Universal Time)
Finished	Thursday Nov 10 2022 10:38:48 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	BRBToken.sol

Detected Issues

ID	Title	Severity	Status
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged

SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged

SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 23

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
22   unchecked {
23   uint256 c = a + b;
24   if (c < a) return (false, 0);
25   return (true, c);
26   }
27
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 31

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
30   if (b > a) return (false, 0);
31   return (true, a - b);
32   }
33   }
34   function tryMul(uint256 a, uint256 b) internal pure returns (bool, uint256) {
35
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 37

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
36   if (a == 0) return (true, 0);
37   uint256 c = a * b;
38   if (c / a != b) return (false, 0);
39   return (true, c);
40   }
41
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 38

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
37   uint256 c = a * b;
38   if (c / a != b) return (false, 0);
39   return (true, c);
40   }
41   }
42
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 45

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
44   if (b == 0) return (false, 0);
45   return (true, a / b);
46   }
47   }
48   function tryMod(uint256 a, uint256 b) internal pure returns (bool, uint256) {
49
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 51

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
50   if (b == 0) return (false, 0);
51   return (true, a % b);
52   }
53   }
54   function add(uint256 a, uint256 b) internal pure returns (uint256) {
55
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 55

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
54   function add(uint256 a, uint256 b) internal pure returns (uint256) {
55   return a + b;
56   }
57   function sub(uint256 a, uint256 b) internal pure returns (uint256) {
58   return a - b;
59
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 58

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
57   function sub(uint256 a, uint256 b) internal pure returns (uint256) {
58   return a - b;
59   }
60   function mul(uint256 a, uint256 b) internal pure returns (uint256) {
61   return a * b;
62
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 61

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
60   function mul(uint256 a, uint256 b) internal pure returns (uint256) {
61   return a * b;
62   }
63   function div(uint256 a, uint256 b) internal pure returns (uint256) {
64   return a / b;
65
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 64

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
63   function div(uint256 a, uint256 b) internal pure returns (uint256) {
64   return a / b;
65   }
66   function mod(uint256 a, uint256 b) internal pure returns (uint256) {
67   return a % b;
68
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 67

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
66   function mod(uint256 a, uint256 b) internal pure returns (uint256) {
67   return a % b;
68   }
69   function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
70   unchecked {
71
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 72

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
71   require(b <= a, errorMessage);
72   return a - b;
73   }
74   }
75   function div(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
76
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 78

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
77   require(b > 0, errorMessage);
78   return a / b;
79   }
80   }
81   function mod(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
82
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 84

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
83   require(b > 0, errorMessage);
84   return a % b;
85   }
86   }
87   }
88
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 380

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
379   uint256 private constant MAX = ~uint256(0);
380   uint256 private _tTotal = 1000000000 * 10**18;
381   uint256 private _rTotal = (MAX - (MAX % _tTotal));
382   uint256 private _tFeeTotal;
383   string private _name = "BRB Cash";
384
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 380

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
379   uint256 private constant MAX = ~uint256(0);
380   uint256 private _tTotal = 1000000000 * 10**18;
381   uint256 private _rTotal = (MAX - (MAX % _tTotal));
382   uint256 private _tFeeTotal;
383   string private _name = "BRB Cash";
384
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 381

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
380   uint256 private _tTotal = 1000000000 * 10**18;
381   uint256 private _rTotal = (MAX - (MAX % _tTotal));
382   uint256 private _tFeeTotal;
383   string private _name = "BRB Cash";
384   string private _symbol = "BRBC";
385
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 381

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
380   uint256 private _tTotal = 1000000000 * 10**18;
381   uint256 private _rTotal = (MAX - (MAX % _tTotal));
382   uint256 private _tFeeTotal;
383   string private _name = "BRB Cash";
384   string private _symbol = "BRBC";
385
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 397

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
396   bool public swapAndLiquifyEnabled = true;
397   uint256 public _maxTxAmount = 1000000000 * 10**18;
398   uint256 private numTokensSellToAddToLiquidity = 500000000 * 10**18;
399   event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
400   event SwapAndLiquifyEnabledUpdated(bool enabled);
401
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 397

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
396   bool public swapAndLiquifyEnabled = true;
397   uint256 public _maxTxAmount = 1000000000 * 10**18;
398   uint256 private numTokensSellToAddToLiquidity = 500000000 * 10**18;
399   event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
400   event SwapAndLiquifyEnabledUpdated(bool enabled);
401
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 398

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
397   uint256 public _maxTxAmount = 1000000000 * 10**18;
398   uint256 private numTokensSellToAddToLiquidity = 500000000 * 10**18;
399   event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
400   event SwapAndLiquifyEnabledUpdated(bool enabled);
401   event SwapAndLiquify(
402
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 398

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
397   uint256 public _maxTxAmount = 1000000000 * 10**18;
398   uint256 private numTokensSellToAddToLiquidity = 500000000 * 10**18;
399   event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
400   event SwapAndLiquifyEnabledUpdated(bool enabled);
401   event SwapAndLiquify(
402
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 500

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
499   require(_isExcluded[account], "Account is already included");
500   for (uint256 i = 0; i < _excluded.length; i++) {
501   if (_excluded[i] == account) {
502   _excluded[i] = _excluded[_excluded.length - 1];
503   _tOwned[account] = 0;
504
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 502

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
501   if (_excluded[i] == account) {
502   _excluded[i] = _excluded[_excluded.length - 1];
503   _tOwned[account] = 0;
504   _isExcluded[account] = false;
505   _excluded.pop();
506
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 538

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
537   _maxTxAmount = _tTotal.mul(maxTxPercent).div(
538   10**3
539   );
540   }
541   function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
542
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 577

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
576   uint256 tSupply = _tTotal;
577   for (uint256 i = 0; i < _excluded.length; i++) {
578   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
579   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
580   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
581
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 601

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
600   return _amount.mul(_taxFee).div(
601   10**3
602   );
603   }
604   function calculateDevelopmentFee(uint256 _amount) private view returns (uint256) {
605
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 606

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
605   return _amount.mul(_developmentFee).div(
606   10**3
607   );
608   }
609   function calculateLiquidityFee(uint256 _amount) private view returns (uint256) {
610
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 611

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
610   return _amount.mul(_liquidityFee).div(
611   10**3
612   );
613   }
614   function removeAllFee() private {
615
```

SWC-101 | COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED

LINE 502

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- BRBToken.sol

Locations

```
501   if (_excluded[i] == account) {
502   _excluded[i] = _excluded[_excluded.length - 1];
503   _tOwned[account] = 0;
504   _isExcluded[account] = false;
505   _excluded.pop();
506
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 7

low SEVERITY

The current pragma Solidity directive is ""^0.8.17"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source File

- BRBToken.sol

Locations

```
6
7   pragma solidity ^0.8.17;
8
9   interface IERC20 {
10   function totalSupply() external view returns (uint256);
11
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 395

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "inSwapAndLiquify" is internal. Other possible visibility settings are public and private.

Source File

- BRBToken.sol

Locations

```
394   address public immutable uniswapV2Pair;
395   bool inSwapAndLiquify;
396   bool public swapAndLiquifyEnabled = true;
397   uint256 public _maxTxAmount = 1000000000 * 10**18;
398   uint256 private numTokensSellToAddToLiquidity = 500000000 * 10**18;
399
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 501

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
500   for (uint256 i = 0; i < _excluded.length; i++) {
501   if (_excluded[i] == account) {
502   _excluded[i] = _excluded[_excluded.length - 1];
503   _tOwned[account] = 0;
504   _isExcluded[account] = false;
505
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 502

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
501   if (_excluded[i] == account) {
502   _excluded[i] = _excluded[_excluded.length - 1];
503   _tOwned[account] = 0;
504   _isExcluded[account] = false;
505   _excluded.pop();
506
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 502

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
501   if (_excluded[i] == account) {
502   _excluded[i] = _excluded[_excluded.length - 1];
503   _tOwned[account] = 0;
504   _isExcluded[account] = false;
505   _excluded.pop();
506
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 578

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
577   for (uint256 i = 0; i < _excluded.length; i++) {
578   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
579   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
580   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
581   }
582
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 578

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
577   for (uint256 i = 0; i < _excluded.length; i++) {
578   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
579   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
580   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
581   }
582
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 579

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
578   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
579   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
580   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
581   }
582   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
583
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 580

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
579   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
580   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
581   }
582   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
583   return (rSupply, tSupply);
584
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 679

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
678   address[] memory path = new address[](2);
679   path[0] = address(this);
680   path[1] = uniswapV2Router.WETH();
681   _approve(address(this), address(uniswapV2Router), tokenAmount);
682   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
683
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 680

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- BRBToken.sol

Locations

```
679   path[0] = address(this);
680   path[1] = uniswapV2Router.WETH();
681   _approve(address(this), address(uniswapV2Router), tokenAmount);
682   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
683   tokenAmount,
684
```

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to, or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without Sysfixed's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Sysfixed to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model, or legal compliance.

This is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the 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 below disclaimer below – please make sure to read it in full.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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.

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 Sysfixed and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (Sysfixed) owe no duty of care.

ABOUT US

Sysfixed is a blockchain security certification organization established in 2021 with the objective to provide smart contract security services and verify their correctness in blockchain-based protocols. Sysfixed automatically scans for security vulnerabilities in Ethereum and other EVM-based blockchain smart contracts. Sysfixed a comprehensive range of analysis techniques—including static analysis, dynamic analysis, and symbolic execution—can accurately detect security vulnerabilities to provide an in-depth analysis report. With a vibrant ecosystem of world-class integration partners that amplify developer productivity, Sysfixed can be utilized in all phases of your project's lifecycle. Our team of security experts is dedicated to the research and improvement of our tools and techniques used to fortify your code.