Zenithereum.ai

Smart Contract Audit Report

SYSFIXED

04 Feb 2023

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
Zenithereum.ai	ZEN-AI	Binance Smart Chain

Addresses

Contract address	0x24697e20c1921Ebd5846c5B025A5fAB1a43Fe316
Contract deployer address	0x564F67f3B4BD8e75b1E692885dfAec18b2466caf

Project Website

https://zenithereum.ai/

Codebase

https://bscscan.com/address/0x24697e20c1921Ebd5846c5B025A5fAB1a43Fe316#code

SUMMARY

Zenithereum is the intersection of #blockchain & #AI creating innovative solutions for a better future. Join us on our journey to revolutionize the world.

Contract Summary

Documentation Quality

Zenithereum.ai 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 Zenithereum.ai with the discovery of several low issues.

Test Coverage

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

Audit Findings Summary

- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 470, 502, 525, 526, 561, 597, 663, 667, 679, 686, 695, 928, 928, 928, 932, 936, 940, 1002, 1027, 1034, 1041, 1119, 1119, 1119, 1120, 1120, 1120, 1127, 1127, 1127, 1128, 1128, 1128, 1133, 1133, 1133, 1134, 1134, 1134, 1142, 1198, 1204, 1204, 1204 and 1214.
- 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 1003, 1004, 1152 and 1153.

CONCLUSION

We have audited the Zenithereum.ai project released on February-2023 to discover issues and identify potential security vulnerabilities in Zenithereum.ai 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 Zenithereum.ai 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 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.

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.	PASS
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	Friday Feb 03 2023 03:38:39 GMT+0000 (Coordinated Universal Time)
Finished	Saturday Feb 04 2023 22:01:49 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	Zenithereum.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	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-103	A FLOATING PRAGMA IS 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-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 470

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
469   function add(uint256 a, uint256 b) internal pure returns (uint256) {
470   uint256 c = a + b;
471   require(c >= a, "SafeMath: addition overflow");
472
473   return c;
474
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 502

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
501   require(b <= a, errorMessage);
502   uint256 c = a - b;
503
504   return c;
505   }
506
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 525

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
524
525   uint256 c = a * b;
526   require(c / a == b, "SafeMath: multiplication overflow");
527
528   return c;
529
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 526

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
525   uint256 c = a * b;
526   require(c / a == b, "SafeMath: multiplication overflow");
527
528   return c;
529   }
530
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 561

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
560   require(b > 0, errorMessage);
561   uint256 c = a / b;
562   // assert(a == b * c + a % b); // There is no case in which this doesn't hold
563
564   return c;
565
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 597

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
596   require(b != 0, errorMessage);
597   return a % b;
598   }
599   }
600
601
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 663

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
662   function mul(int256 a, int256 b) internal pure returns (int256) {
663   int256 c = a * b;
664
665   // Detect overflow when multiplying MIN_INT256 with -1
666   require(c != MIN_INT256 || (a & MIN_INT256) != (b & MIN_INT256));
667
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 667

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
666   require(c != MIN_INT256 || (a & MIN_INT256) != (b & MIN_INT256));
667   require((b == 0) || (c / b == a));
668   return c;
669   }
670
671
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 679

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
678   // Solidity already throws when dividing by 0.
679   return a / b;
680   }
681
682   /**
683
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 686

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
685   function sub(int256 a, int256 b) internal pure returns (int256) {
686   int256 c = a - b;
687   require((b >= 0 && c <= a) || (b < 0 && c > a));
688   return c;
689   }
690
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 695

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
694   function add(int256 a, int256 b) internal pure returns (int256) {
695   int256 c = a + b;
696   require((b >= 0 && c >= a) || (b < 0 && c < a));
697   return c;
698   }
699
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 928

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
927
928   uint256 totalSupply = 1 * 1e8 * (10**_decimals);
929
930   buyMarketingFee = 2;
931   buyLiquidityFee = 0;
932
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 928

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
927
928   uint256 totalSupply = 1 * 1e8 * (10**_decimals);
929
930   buyMarketingFee = 2;
931   buyLiquidityFee = 0;
932
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 928

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
927
928   uint256 totalSupply = 1 * 1e8 * (10**_decimals);
929
930   buyMarketingFee = 2;
931   buyLiquidityFee = 0;
932
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 932

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
931   buyLiquidityFee = 0;
932   buyTotalFees = buyMarketingFee + buyLiquidityFee;
933
934   sellMarketingFee = 2;
935   sellLiquidityFee = 0;
936
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 936

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
935   sellLiquidityFee = 0;
936   sellTotalFees = sellMarketingFee + sellLiquidityFee;
937
938   transferMarketingFee = 2;
939   transferLiquidityFee = 0;
940
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 940

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
939   transferLiquidityFee = 0;
940   transferTotalFees = transferMarketingFee + transferLiquidityFee;
941
942   marketingWallet = address(0x799c90F6B46EDad6591f4997354c3416D303972F); // set as
marketing wallet
943
944
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 1002

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1001   require(airdropWallets.length < 200, "Can only airdrop 200 wallets per txn due to
gas limits"); // allows for airdrop + launch at the same exact time, reducing delays and
reducing sniper input.
1002   for(uint256 i = 0; i < airdropWallets.length; i++){
1003   address wallet = airdropWallets[i];
1004   uint256 amount = amounts[i];
1005   _transfer(msg.sender, wallet, amount);
1006
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 1027

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1026   buyLiquidityFee = _liquidityFee;
1027   buyTotalFees = buyMarketingFee + buyLiquidityFee;
1028   require(buyTotalFees <= 10, "Must keep fees at 10% or less");
1029   }
1030
1031
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 1034

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1033   sellLiquidityFee = _liquidityFee;
1034   sellTotalFees = sellMarketingFee + sellLiquidityFee ;
1035   require(sellTotalFees <= 10, "Must keep fees at 10% or less");
1036   }
1037
1038
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 1041

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1040   transferLiquidityFee = _liquidityFee;
1041   transferTotalFees = transferMarketingFee + transferLiquidityFee;
1042   require(transferTotalFees <= 10, "Must keep fees at 10% or less");
1043   }
1044
1045
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 1119

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1118   fees = amount.mul(sellTotalFees).div(100);
1119   tokensForLiquidity += fees * sellLiquidityFee / sellTotalFees;
1120   tokensForMarketing += fees * sellMarketingFee / sellTotalFees;
1121   }
1122   }
1123
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 1119

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1118   fees = amount.mul(sellTotalFees).div(100);
1119   tokensForLiquidity += fees * sellLiquidityFee / sellTotalFees;
1120   tokensForMarketing += fees * sellMarketingFee / sellTotalFees;
1121   }
1122   }
1123
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1119

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1118   fees = amount.mul(sellTotalFees).div(100);
1119   tokensForLiquidity += fees * sellLiquidityFee / sellTotalFees;
1120   tokensForMarketing += fees * sellMarketingFee / sellTotalFees;
1121   }
1122   }
1123
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 1120

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1119   tokensForLiquidity += fees * sellLiquidityFee / sellTotalFees;
1120   tokensForMarketing += fees * sellMarketingFee / sellTotalFees;
1121   }
1122   }
1123   // on buy
1124
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 1120

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1119   tokensForLiquidity += fees * sellLiquidityFee / sellTotalFees;
1120   tokensForMarketing += fees * sellMarketingFee / sellTotalFees;
1121   }
1122   }
1123   // on buy
1124
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1120

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1119   tokensForLiquidity += fees * sellLiquidityFee / sellTotalFees;
1120   tokensForMarketing += fees * sellMarketingFee / sellTotalFees;
1121   }
1122   }
1123   // on buy
1124
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 1127

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1126   fees = amount.mul(buyTotalFees).div(100);
1127   tokensForLiquidity += fees * buyLiquidityFee / buyTotalFees;
1128   tokensForMarketing += fees * buyMarketingFee / buyTotalFees;
1129   }
1130   } else {
1131
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 1127

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1126   fees = amount.mul(buyTotalFees).div(100);
1127   tokensForLiquidity += fees * buyLiquidityFee / buyTotalFees;
1128   tokensForMarketing += fees * buyMarketingFee / buyTotalFees;
1129   }
1130   } else {
1131
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1127

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1126   fees = amount.mul(buyTotalFees).div(100);
1127   tokensForLiquidity += fees * buyLiquidityFee / buyTotalFees;
1128   tokensForMarketing += fees * buyMarketingFee / buyTotalFees;
1129   }
1130   } else {
1131
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 1128

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1127   tokensForLiquidity += fees * buyLiquidityFee / buyTotalFees;
1128   tokensForMarketing += fees * buyMarketingFee / buyTotalFees;
1129   }
1130   } else {
1131   if (transferTotalFees > 0){
1132
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 1128

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1127   tokensForLiquidity += fees * buyLiquidityFee / buyTotalFees;
1128   tokensForMarketing += fees * buyMarketingFee / buyTotalFees;
1129   }
1130   } else {
1131   if (transferTotalFees > 0){
1132
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1128

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1127   tokensForLiquidity += fees * buyLiquidityFee / buyTotalFees;
1128   tokensForMarketing += fees * buyMarketingFee / buyTotalFees;
1129   }
1130   } else {
1131   if (transferTotalFees > 0){
1132
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 1133

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1132   fees = amount.mul(transferTotalFees).div(100);
1133   tokensForLiquidity += fees * transferLiquidityFee / transferTotalFees;
1134   tokensForMarketing += fees * transferMarketingFee / transferTotalFees;
1135   }
1136   }
1137
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 1133

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1132   fees = amount.mul(transferTotalFees).div(100);
1133   tokensForLiquidity += fees * transferLiquidityFee / transferTotalFees;
1134   tokensForMarketing += fees * transferMarketingFee / transferTotalFees;
1135   }
1136   }
1137
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1133

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1132   fees = amount.mul(transferTotalFees).div(100);
1133   tokensForLiquidity += fees * transferLiquidityFee / transferTotalFees;
1134   tokensForMarketing += fees * transferMarketingFee / transferTotalFees;
1135   }
1136   }
1137
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 1134

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1133   tokensForLiquidity += fees * transferLiquidityFee / transferTotalFees;
1134   tokensForMarketing += fees * transferMarketingFee / transferTotalFees;
1135   }
1136   }
1137
1138
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 1134

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1133   tokensForLiquidity += fees * transferLiquidityFee / transferTotalFees;
1134   tokensForMarketing += fees * transferMarketingFee / transferTotalFees;
1135   }
1136   }
1137
1138
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1134

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1133   tokensForLiquidity += fees * transferLiquidityFee / transferTotalFees;
1134   tokensForMarketing += fees * transferMarketingFee / transferTotalFees;
1135   }
1136   }
1137
1138
```

SWC-101 | ARITHMETIC OPERATION "-=" DISCOVERED

LINE 1142

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1141
1142   amount -= fees;
1143   }
1144
1145   super._transfer(from, to, amount);
1146
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 1198

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1197
1198   uint256 totalTokensToSwap = tokensForLiquidity + tokensForMarketing;
1199   bool success;
1200
1201   if(contractBalance == 0 || totalTokensToSwap == 0) {return;}
1202
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 1204

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1203   // Halve the amount of liquidity tokens
1204   uint256 liquidityTokens = contractBalance * tokensForLiquidity / totalTokensToSwap
/ 2;
1205   uint256 amountToSwapForETH = contractBalance.sub(liquidityTokens);
1206
1207   uint256 initialETHBalance = address(this).balance;
1208
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 1204

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1203   // Halve the amount of liquidity tokens
1204   uint256 liquidityTokens = contractBalance * tokensForLiquidity / totalTokensToSwap
/ 2;
1205   uint256 amountToSwapForETH = contractBalance.sub(liquidityTokens);
1206
1207   uint256 initialETHBalance = address(this).balance;
1208
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1204

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1203   // Halve the amount of liquidity tokens
1204   uint256 liquidityTokens = contractBalance * tokensForLiquidity / totalTokensToSwap
/ 2;
1205   uint256 amountToSwapForETH = contractBalance.sub(liquidityTokens);
1206
1207   uint256 initialETHBalance = address(this).balance;
1208
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 1214

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1213   uint256 ethForMarketing =
ethBalance.mul(tokensForMarketing).div(totalTokensToSwap);
1214   uint256 ethForLiquidity = ethBalance - ethForMarketing;
1215
1216   tokensForLiquidity = 0;
1217   tokensForMarketing = 0;
1218
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 7

low SEVERITY

The current pragma Solidity directive is ""^0.8.9"". 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

- Zenithereum.sol

Locations

```
6
7   pragma solidity ^0.8.9;
8
9   abstract contract Context {
10   function _msgSender() internal view virtual returns (address) {
11
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1003

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1002   for(uint256 i = 0; i < airdropWallets.length; i++){
1003   address wallet = airdropWallets[i];
1004   uint256 amount = amounts[i];
1005   _transfer(msg.sender, wallet, amount);
1006   }
1007
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1004

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1003   address wallet = airdropWallets[i];
1004   uint256 amount = amounts[i];
1005   _transfer(msg.sender, wallet, amount);
1006   }
1007   return true;
1008
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1152

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1151   address[] memory path = new address[](2);
1152   path[0] = address(this);
1153   path[1] = uniswapV2Router.WETH();
1154
1155   _approve(address(this), address(uniswapV2Router), tokenAmount);
1156
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1153

low SEVERITY

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

Source File

- Zenithereum.sol

Locations

```
1152   path[0] = address(this);
1153   path[1] = uniswapV2Router.WETH();
1154
1155   _approve(address(this), address(uniswapV2Router), tokenAmount);
1156
1157
```

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.