



EndlessWebWorlds  
**Smart Contract  
Audit Report**

# TABLE OF CONTENTS

## [Audited Details](#)

- Audited Project
- Blockchain
- Addresses
- Project Website
- Codebase

## [Summary](#)

- Contract Summary
- Audit Findings Summary
- Vulnerabilities Summary

## [Conclusion](#)

## [Audit Results](#)

## [Smart Contract Analysis](#)

- Detected Vulnerabilities

## [Disclaimer](#)

## [About Us](#)

# AUDITED DETAILS

## Audited Project

Project name	Token ticker	Blockchain
EndlessWebWorlds	EWV	Ethereum

## Addresses

Contract address	0x3d38F87BeF0123f5764635C7E11048027E0721a8
Contract deployer address	0xD69EBCcD52F86B2Aa2134D888d821688858a1400

## Project Website

<https://endless-web-worlds.com/>

## Codebase

<https://etherscan.io/address/0x3d38F87BeF0123f5764635C7E11048027E0721a8#code>

# SUMMARY

Enter a new way to collaborate and explore. EWW is built on an universe of tiny 2.5D online worlds that anyone can create individually and for free. We are creating a platform where people can easily and amusingly learn about projects or other people. Where teams/clans/holders can meet and have fun with various tool sets that we offer.

## Contract Summary

### Documentation Quality

EndlessWebWorlds 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 EndlessWebWorlds 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 44, 215, 216, 331, 332, 337, 373, 378, 379 and 380.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 41, 66, 81, 130, 176, 209, 327, 363 and 581.

## CONCLUSION

We have audited the EndlessWebWorlds project released on November 2022 to discover issues and identify potential security vulnerabilities in EndlessWebWorlds 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 EndlessWebWorlds 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. 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 also it is best practice to set the visibility of state variables explicitly. The default visibility for "\_owner" is internal. Other possible visibility settings are public and private.

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Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.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

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 <code>abi.encodePacked()</code> with multiple variable length arguments can, in certain situations, lead to a hash collision.	PASS
Hardcoded gas amount	SWC-134	The <code>transfer()</code> and <code>send()</code> 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





<b>SWC-108</b>	STATE VARIABLE VISIBILITY IS NOT SET.	<b>low</b>	acknowledged
<b>SWC-108</b>	STATE VARIABLE VISIBILITY IS NOT SET.	<b>low</b>	acknowledged
<b>SWC-108</b>	STATE VARIABLE VISIBILITY IS NOT SET.	<b>low</b>	acknowledged
<b>SWC-108</b>	STATE VARIABLE VISIBILITY IS NOT SET.	<b>low</b>	acknowledged
<b>SWC-108</b>	STATE VARIABLE VISIBILITY IS NOT SET.	<b>low</b>	acknowledged

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 41

### low SEVERITY

The current pragma Solidity directive is ""^0.8.7"". 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

- EndlessWebWorlds.sol

### Locations

```
40
41  pragma solidity ^0.8.7;
42
43  abstract contract Ownable {
44  address _owner;
45
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 66

### low SEVERITY

The current pragma Solidity directive is ""^0.8.7"". 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

- EndlessWebWorlds.sol

### Locations

```
65
66  pragma solidity ^0.8.7;
67
68  interface IUniswapV2Factory {
69  function createPair(address tokenA, address tokenB)
70
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 81

### low SEVERITY

The current pragma Solidity directive is ""^0.8.7"". 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

- EndlessWebWorlds.sol

### Locations

```
80
81  pragma solidity ^0.8.7;
82
83  interface IUniswapV2Router02 {
84  function swapExactTokensForETH(
85
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 130

### low SEVERITY

The current pragma Solidity directive is `""^0.8.7"`. 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

- EndlessWebWorlds.sol

### Locations

```
129
130  pragma solidity ^0.8.7;
131
132
133  contract DoubleSwapped {
134
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 176

### low SEVERITY

The current pragma Solidity directive is `^0.8.7`. 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

- EndlessWebWorlds.sol

### Locations

```
175
176  pragma solidity ^0.8.7;
177
178  interface IERC20 {
179  function totalSupply() external view returns (uint256);
180
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 209

### low SEVERITY

The current pragma Solidity directive is `""^0.8.7"`. 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

- EndlessWebWorlds.sol

### Locations

```
208
209  pragma solidity ^0.8.7;
210
211
212  abstract contract ERC20 is IERC20 {
213
```



## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 327

### low SEVERITY

The current pragma Solidity directive is ""^0.8.7"". 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

- EndlessWebWorlds.sol

### Locations

```
326
327  pragma solidity ^0.8.7;
328
329
330  abstract contract MaxWalletDynamic {
331
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 363

### low SEVERITY

The current pragma Solidity directive is ""^0.8.7"". 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

- EndlessWebWorlds.sol

### Locations

```
362
363  pragma solidity ^0.8.7;
364
365  abstract contract TradableErc20 is ERC20, DoubleSwapped, Ownable, Withdrawable {
366    IUniswapV2Router02 internal constant _uniswapV2Router =
367
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 581

### low SEVERITY

The current pragma Solidity directive is `""^0.8.7"`. 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

- EndlessWebWorlds.sol

### Locations

```
580
581  pragma solidity ^0.8.7;
582
583
584  struct AirdropData {
585
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 44

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
43  abstract contract Ownable {
44  address _owner;
45
46  modifier onlyOwner() {
47  require(msg.sender == _owner);
48
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 215

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
214 uint8 constant _decimals = 9;
215 string _name;
216 string _symbol;
217 mapping(address => uint256) internal _balances;
218 mapping(address => mapping(address => uint256)) internal _allowances;
219
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 216

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
215 string _name;  
216 string _symbol;  
217 mapping(address => uint256) internal _balances;  
218 mapping(address => mapping(address => uint256)) internal _allowances;  
219 uint256 internal constant INFINITY_ALLOWANCE = 2**256 - 1;  
220
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 331

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
330 abstract contract MaxWalletDynamic {
331     uint256 startMaxWallet;
332     uint256 startTime; // last increment time
333     uint256 constant startMaxBuyPercentil = 5; // maximum buy on start 1000=100%
334     uint256 constant maxBuyIncrementMinutesTimer = 2; // increment maxbuy minutes
335 }
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 332

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
331 uint256 startMaxWallet;  
332 uint256 startTime; // last increment time  
333 uint256 constant startMaxBuyPercentil = 5; // maximum buy on start 1000=100%  
334 uint256 constant maxBuyIncrementMinutesTimer = 2; // increment maxbuy minutes  
335 uint256 constant maxBuyIncrementPercentil = 3; // increment maxbyu percentil  
1000=100%  
336
```



## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 337

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
336 uint256 constant maxIncrements = 1000; // maximum time incrementations
337 uint256 maxBuyIncrementValue; // value for increment maxBuy
338
339 function startMaxWalletDynamic(uint256 totalSupply) internal {
340     startTime = block.timestamp;
341 }
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 373

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
372 address public extraAddress;
373 mapping(address => bool) _isExcludedFromFee;
374 uint256 public buyFeePpm = 2; // fee in 1/1000
375 uint256 public sellFeePpm = 2; // fee in 1/1000
376 uint256 public thisShare = 410; // in 1/1000
377
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 378

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
377 uint256 public extraShare = 0; // in 1/1000
378 uint256 maxWalletStart = 5e16;
379 uint256 addMaxWalletPerMinute = 5e16;
380 uint256 tradingStartTime;
381
382
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 379

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
378 uint256 maxWalletStart = 5e16;
379 uint256 addMaxWalletPerMinute = 5e16;
380 uint256 tradingStartTime;
381
382 constructor(string memory name_, string memory symbol_)
383
```

## SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 380

### low SEVERITY

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

### Source File

- EndlessWebWorlds.sol

### Locations

```
379     uint256 addMaxWalletPerMinute = 5e16;
380     uint256 tradingStartTime;
381
382     constructor(string memory name_, string memory symbol_)
383         ERC20(name_, symbol_)
384
```

# 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.