



DefiHorse

# 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
DefiHorse	DFH	Ethereum

## Addresses

Contract address	0x79Ab5a5629714A1139d53a23089A3c498D4dF60F
Contract deployer address	0x700CcA3Be4E8fe882A9F623f4947d0f48485ea9b

## Project Website

<a href="https://defihorse.com/">https://defihorse.com/</a>
---

## Codebase

<a href="https://etherscan.io/address/0x79Ab5a5629714A1139d53a23089A3c498D4dF60F#code">https://etherscan.io/address/0x79Ab5a5629714A1139d53a23089A3c498D4dF60F#code</a>
---

# SUMMARY

DeFiHorse - The Best P2E Horse-Racing Game with a total of 7M followers is now starting the parade to the ERC chain with an exclusive, ongoing \$DFH Presale!

## Contract Summary

### Documentation Quality

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

- The technical description is provided clearly and structured and also don't have any high risk issue.

### Code Quality

The Overall quality of the basecode is standard.

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

### Test Coverage

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

## Audit Findings Summary

- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 11, 91, 120, 138 and 340.

# CONCLUSION

We have audited the DefiHorse project released on November 2022 to discover issues and identify potential security vulnerabilities in DefiHorse 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 DefiHorse 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 floating pragma is 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.

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

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	Thursday Nov 03 2022 23:39:13 GMT+0000 (Coordinated Universal Time)
Finished	Friday Nov 04 2022 20:43:54 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	CoinToken.sol

## Detected Issues

ID	Title	Severity	Status
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged

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

LINE 11

### low SEVERITY

The current pragma Solidity directive is `""^0.8.0""`. 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

- CoinToken.sol

### Locations

```
10
11  pragma solidity ^0.8.0;
12
13  /**
14   * @dev Interface of the ERC20 standard as defined in the EIP.
15
```

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

LINE 91

### low SEVERITY

The current pragma Solidity directive is `""^0.8.0""`. 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

- CoinToken.sol

### Locations

```
90
91  pragma solidity ^0.8.0;
92
93
94  /**
95
```

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

LINE 120

### low SEVERITY

The current pragma Solidity directive is ""^0.8.0"". 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

- CoinToken.sol

### Locations

```
119
120  pragma solidity ^0.8.0;
121
122
123  abstract contract Context {
124
```

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

LINE 138

### low SEVERITY

The current pragma Solidity directive is `""^0.8.0""`. 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

- CoinToken.sol

### Locations

```
137
138  pragma solidity ^0.8.0;
139
140
141
142
```

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

LINE 340

### low SEVERITY

The current pragma Solidity directive is `""^0.8.0""`. 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

- CoinToken.sol

### Locations

```
339
340  pragma solidity ^0.8.0;
341
342
343
344
```

# 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.