



SOLIDProof
Bring trust into your projects

Blockchain Security | Smart Contract Audits | KYC

MADE IN GERMANY

Audit

Security Assessment

30. September 2021

For



EXOTIC MONSTER

Disclaimer	3
Description	5
Project Engagement	5
Logo	5
Contract Link	5
Methodology	7
Used Code from other Frameworks/Smart Contracts (direct imports)	8
Tested Contract Files	9
Source Lines	10
Risk Level	10
Capabilities	11
Scope of Work	12
Inheritance Graph	12
Verify Claims	13
CallGraph	18
Source Units in Scope	19
Critical issues	20
High issues	20
Medium issues	20
Low issues	20
Informational issues	20
Audit Comments	21
SWC Attacks	22

Disclaimer

SolidProof.io reports are not, nor should be considered, a "endorsement" or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of an "product" or "asset" created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Uniswap, PancakeSwap etc...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing 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. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	30. September 2021	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary

Network

Binance Smart Chain (BEP20)

Website

<https://exoticmonster.com/>

Telegram

<https://t.me/emscnft>

<https://t.me/exoticmonsterNFT>

Twitter

<https://twitter.com/ExoticMonsteNFT/>

Youtube

<https://www.youtube.com/channel/UChdLxyKRgmvy5gu8fMF8usA>

Description

ExoticMonster is a platform that integrates NFT games and decentralized yield farm applications. Joining ExoticMonster not only entertains you but also generates a lot of profit. Our mission is to build a comprehensive platform of digital monsters that will enable millions of individuals to participate in the NFT and blockchain-based gaming world in a simple, creative, and enjoyable way.

ExoticMonster will be the first ecosystem to combine the greatest aspects of gaming and digital collectibles, transforming it into the digital creatures universe. With ExoticMonster, Players can use their pets to fight, collect, grow, and earn money.

Project Engagement

During the 8th of August 2021, **ExoticMonster** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. **ExoticMonster** provided Solidproof.io with access to their code repository and whitepaper.

Logo



EXOTIC MONSTER

Contract Link

v1.0

ExoticMonster TokenGuard:

<https://bscscan.com/address/0xbad403ee1fcd49aef16e782c1c072f9358685236#code>

ExoticMonster:

<https://testnet.bscscan.com/address/0xa4a5d2f2551d623971f308c8c5e4db080ce1392d#writeContract>

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 – 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 – 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 – 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 – 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
 - ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
 2. Testing and automated analysis that includes the following:
 - i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
 - ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
 3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
 4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.
-

Used Code from other Frameworks/Smart Contracts (direct imports)

ExoticMonster

Imported packages:

v1.0

- OpenZeppelin
 - Address
 - Ownable
 - SafeMath
 - TokenGuard
- Pancakeswap
 - PancakeFactory
 - PancakePair
 - PancakeRouter



Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

File Name	SHA-1 Hash
contracts/ExoticMonsterToken.sol	0x5031566c0894a2683ca975d0fbafe675ba74c8dc
contracts/ExoticMonsterController.sol	0xa4a5d2f2551d623971f308c8c5e4db080ce1392d

Metrics

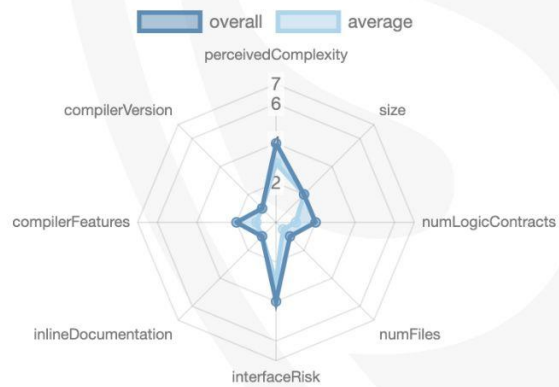
Source Lines

v1.0



Risk Level

v1.0



Capabilities

Components

Version	Contracts	Libraries	Interfaces	Abstract
1.0	2	2	6	4

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

Version	Public	Payable
1.0	46	0

Version	External	Internal	Private	Pure	View
1.0	17	66	3	28	24

State Variables

Version	Total	Public
1.0	16	7

Capabilities

Version	Solidity Versions observed	Experimental Features	Can Receive Funds	Uses Assembly	Has Destroyable Contracts
1.0	0.8.0			**** (0 asm blocks)	

Version	Transfers ETH	Low-Level Calls	DelegateCall	Uses Hash Functions	ECRecover	New/Create/Create2
1.0	yes					

Scope of Work

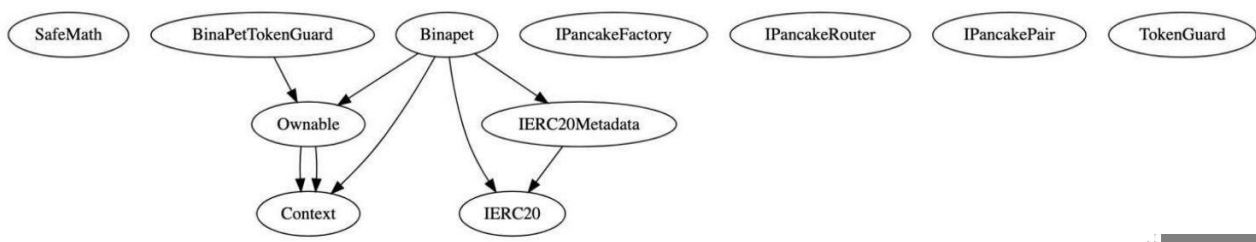
The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Correct implementation of Token standard
2. Deployer cannot mint any new tokens
3. Deployer cannot burn or lock user funds
4. Deployer cannot pause the contract
5. Overall checkup (Smart Contract Security)

Inheritance Graph

Exotic Mnster v1.0



Verify Claims

Correct implementation of Token standard

Tested	Verified
✓	✓

Function	Description	Exist	Tested	Verified
TotalSupply	provides information about the total token supply	✓	✓	✓
BalanceOf	provides account balance of the owner's account	✓	✓	✓
Transfer	executes transfers of a specified number of tokens to a specified address	✓	✓	✓
TransferFrom	executes transfers of a specified number of tokens from a specified address	✓	✓	✓
Approve	allow a spender to withdraw a set number of tokens from a specified account	✓	✓	✓
Allowance	returns a set number of tokens from a spender to the owner	✓	✓	✓

Optional implementations

Function	Description	Exist	Tested	Verified
renounceOwnership	Owner renounce ownership for more trust	✓	✓	✗

Deployer cannot mint any new tokens

Tested	Deployer cannot mint	File	Comment
✓	✓	Main	Line: -

Max / Total Supply:

```
constructor() {
    _mint(msg.sender, _initSupply);

    taxAddress = payable(msg.sender);

    IPancakeRouter _router = IPancakeRouter(0xECC5428A66808FC40A464e5B3F4D265Df985E3E8); //for test
    //IPancakeRouter _router = IPancakeRouter(0x10ED43C718714eb63d5aA57B78B54704E256024E);

    pairAddress = IPancakeFactory(_router.factory())
        .createPair(address(this), _router.WETH());

    // set the rest of the contract variables
    routerAddress = address(_router);

    _isExcludedFromFee[owner()] = true;
}
```

```
function _mint(address account, uint256 amount) internal virtual {
    require(account != address(0), "ERC20: mint to the zero address");

    _beforeTokenTransfer(address(0), account, amount);

    _totalSupply = _totalSupply.add(amount);
    _balances[account] = _balances[account].add(amount);
    emit Transfer(address(0), account, amount);
}
```

Deployer cannot burn or lock user funds

Name	Tested	Exist	Verified
Deployer cannot lock	✓	✓	✗
Deployer cannot burn	✓	✓	✓

Comments:

v1.0

- Deployer can lock over the ExoticMonster TokenGuard

ExoticMonster TokenGuard

1. addBlackList	→
2. removeBlackList	→
3. renounceOwnership	→
4. setLimit	→
5. transferOwnership	→

ExoticMonster

1. approve	→
2. decreaseAllowance	→
3. excludeFromFee	→
4. includeInFee	→
5. increaseAllowance	→
6. renounceOwnership	→
7. setTax	→
8. setTaxAddress	→
9. transfer	→
10. transferFrom	→
11. transferOwnership	→

[Browse source code](#)

Deployer cannot pause the contract

Tested	Verified	Deployer cannot pause
✓	✓	✓

1. approve	→
2. decreaseAllowance	→
3. excludeFromFee	→
4. includeInFee	→
5. increaseAllowance	→
6. renounceOwnership	→
7. setTax	→
8. setTaxAddress	→
9. transfer	→
10. transferFrom	→
11. transferOwnership	→

[Browse source code](#)

Overall checkup (Smart Contract Security)







Tested	Verified
✓	✓

Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	⚠
Unverified / Not checked	✗

Source Units in Scope

v1.0

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/ExoticMonsterTokenGuard.sol	4	—	348	336	123	177	54	
	contracts/ExoticMonster.sol	4	6	825	697	292	384	237	
	Totals	8	6	1173	1033	415	561	291	

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
nSLOC	normalized source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments
Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, .)

Audit Results

AUDIT PASSED

Critical issues

- no critical issues found -

High issues

- no high issues found -

Medium issues

- no medium issues found -

Low issues

Issue	File	Type	Line	Description
#1	Exotic Monster	Missing Zero Address Validation (missing-zero-check)	524, 512	Check that the address is not zero

Informational issues

- no informational issues found -

Audit Comments

30.September 2021:

- Deployer can lock user assets with TokenGuard.protect function
- Deployer can set transactions limit



SWC Attacks

ID	Title	Relationships	Status
SW C-13 6	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SW C-13 5	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SW C-13 4	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SW C-13 3	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SW C-13 2	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SW C-13 1	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SW C-13 0	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SW C-12 9	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SW C-12 8	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

<u>SW C-12 7</u>	Arbitrary Jump with Function Type Variable	<u>CWE-695: Use of Low-Level Functionality</u>	PASSED
<u>SW C-12 5</u>	Incorrect Inheritance Order	<u>CWE-696: Incorrect Behavior Order</u>	PASSED
<u>SW C-12 4</u>	Write to Arbitrary Storage Location	<u>CWE-123: Write-what-where Condition</u>	PASSED
<u>SW C-12 3</u>	Requirement Violation	<u>CWE-573: Improper Following of Specification by Caller</u>	PASSED
<u>SW C-12 2</u>	Lack of Proper Signature Verification	<u>CWE-345: Insufficient Verification of Data Authenticity</u>	PASSED
<u>SW C-12 1</u>	Missing Protection against Signature Replay Attacks	<u>CWE-347: Improper Verification of Cryptographic Signature</u>	PASSED
<u>SW C-12 0</u>	Weak Sources of Randomness from Chain Attributes	<u>CWE-330: Use of Insufficiently Random Values</u>	PASSED
<u>SW C-11 9</u>	Shadowing State Variables	<u>CWE-710: Improper Adherence to Coding Standards</u>	PASSED
<u>SW C-11 8</u>	Incorrect Constructor Name	<u>CWE-665: Improper Initialization</u>	PASSED
<u>SW C-11 7</u>	Signature Malleability	<u>CWE-347: Improper Verification of Cryptographic Signature</u>	PASSED

<u>SW C-11 6</u>	Timestamp Dependence	<u>CWE-829: Inclusion of Functionality from Untrusted Control Sphere</u>	PASSED
<u>SW C-11 5</u>	Authorization through tx.origin	<u>CWE-477: Use of Obsolete Function</u>	PASSED
<u>SW C-11 4</u>	Transaction Order Dependence	<u>CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')</u>	PASSED
<u>SW C-11 3</u>	DoS with Failed Call	<u>CWE-703: Improper Check or Handling of Exceptional Conditions</u>	PASSED
<u>SW C-11 2</u>	Delegatecall to Untrusted Callee	<u>CWE-829: Inclusion of Functionality from Untrusted Control Sphere</u>	PASSED
<u>SW C-111</u>	Use of Deprecated Solidity Functions	<u>CWE-477: Use of Obsolete Function</u>	PASSED
<u>SW C-11 0</u>	Assert Violation	<u>CWE-670: Always-Incorrect Control Flow Implementation</u>	PASSED
<u>SW C-10 9</u>	Uninitialized Storage Pointer	<u>CWE-824: Access of Uninitialized Pointer</u>	PASSED
<u>SW C-10 8</u>	State Variable Default Visibility	<u>CWE-710: Improper Adherence to Coding Standards</u>	PASSED
<u>SW C-10 7</u>	Reentrancy	<u>CWE-841: Improper Enforcement of Behavioral Workflow</u>	PASSED
<u>SW C-10 6</u>	Unprotected SELFDESTRUC T Instruction	<u>CWE-284: Improper Access Control</u>	PASSED

<u>SW</u> <u>C-10</u> <u>5</u>	Unprotected Ether Withdrawal	<u>CWE-284: Improper Access Control</u>	PASSED
<u>SW</u> <u>C-10</u> <u>4</u>	Unchecked Call Return Value	<u>CWE-252: Unchecked Return Value</u>	PASSED
<u>SW</u> <u>C-10</u> <u>3</u>	Floating Pragma	<u>CWE-664: Improper Control of a Resource Through its Lifetime</u>	PASSED
<u>SW</u> <u>C-10</u> <u>2</u>	Outdated Compiler Version	<u>CWE-937: Using Components with Known Vulnerabilities</u>	PASSED
<u>SW</u> <u>C-10</u> <u>1</u>	Integer Overflow and Underflow	<u>CWE-682: Incorrect Calculation</u>	PASSED
<u>SW</u> <u>C-10</u> <u>0</u>	Function Default Visibility	<u>CWE-710: Improper Adherence to Coding Standards</u>	PASSED



Solid
Proofed

Blockchain Security | Smart Contract Audits | KYC


MADE IN GERMANY