



TrustFacture

SECURITY AUDIT REPORT



POLEMOS ARENA

COMPLETED ON:
20.11.2022

OVERVIEW

The purpose of this report is to audit the smart contract source code of POLEMOS ARENA (POLE), their website and social media. TrustFacture scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Smart Contract Vulnerabilities:

- Re-entrancy
- Unhandled Exceptions
- Transaction Order Dependency
- Integer Overflow
- Unrestricted Action
- Incorrect Inheritance Order
- Typographical Errors
- Requirement Violation

Source Code Review:

- Ownership Takeover
- Gas Limit and Loops
- Deployment Consistency
- Repository Consistency
- Data Consistency
- Token Supply Manipulation

Functional Assessment:

- Access Control and Authorization
- Operations Trail and Event Generation
- Assets Manipulation
- Liquidity Access

ABOUT PROJECT

Polemos Arena it is a Play-to-Earn game based in the BSC Ecosystem, an Auto Battler genre game with a game concept similar to chess by prioritizing combinations and strategies for the heroes it owns. Partners with Yahoo, Benzinga, Bloomberg, Marketwatch, AP News, BSCDaily, Morningstar, CoinSpeaker.

Contract Token Name	POLEMOS ARENA	
Symbol	POLE	
Contract Adress	0xbFf84B87d8E27C79d1aB8Da4113802d7244C9070	
Network	Binance Smart Chain	
Total Supply	400,000,000 POLE	
Deployment date	Jun-03-2022	
Language	Solidity	
Status	Not Launched	
Taxes	NO TAXES	0
Fairsale Launch	On Pinksale	
Realese date	23.11.2022	

TOKEN STATS

Liquidity	Not added yet
Burn	No burnt tokens
LP Address	Liquidity not added yet
First transfer date	Nov-18-2022
Creator Wallet	0x59c6caa81c712f4347fb6d9dbcf5de0ad2e480fd
Liquidity Percent	51% of supply
Liquidity Lockup Time	365 days after pool ends
Transfer Count	4

TOKEN HOLDERS

Rank	Address	Quantity	%
1.	0x59c6caa81c712f4347fb6d9dbcf5de0ad2e480fd	217,624,000	54.4060
2.	0x9c604f418cf4b18484ac38955ef9da8ab11e9007	182,376,000	45.5940



TrustFacture

VULNERABILITY CHECK

CONTRACT FUNCTIONS:

1. function approve(address spender, uint256 value) public returns (bool)
2. function burn(uint256 amount) public
3. function burnFrom(address account, uint256 amount) public onlyOwner
4. function decreaseAllowance(address spender, uint256 subtractedValue) public returns (bool)
5. function increaseAllowance(address spender, uint256 addedValue) public returns (bool)
6. function transfer(address to, uint256 value) public returns (bool)
7. function transferFrom(address from, address to, uint256 value) public returns (bool)
8. function transferOwnership(address newOwner) public onlyOwner

CHECKLIST:

No	Description	Results
1.	Compiler errors.	Passed
2.	Possible delays in data delivery.	Passed
3.	Timestamp dependence.	Passed
4.	Integer Overflow and Underflow.	Passed
5.	Race Conditions and Reentrancy.	Passed
6.	DoS with Revert.	Passed
7.	DoS with block gas limit.	Passed
8.	Methods execution permissions.	Passed
9.	Economy model of the contract.	Passed
10.	Private user data leaks.	Passed
11.	Malicious Events Log.	Passed
12.	Scoping and Declarations.	Passed
13.	Uninitialized storage pointers.	Passed
14.	Arithmetic accuracy.	Passed
15.	Design Logic.	Passed
16.	Impact of the exchange rate	Passed
17.	Oracle Calls.	Passed
18.	Cross-function race conditions.	Passed
19.	Fallback function security.	Passed
20.	Safe Open Zeppelin contracts and implementation usage.	Passed



TrustFacture

STATUS:

Main Category	Subcategory	Results
Contract Programming	Solidity version not specified.	Passed
	Solidity version too old.	Passed
	Integer overflow/underflow.	Passed
	Function input parameters lack of check.	Passed
	Function input parameters check bypass.	Passed
	Function access control lacks management.	Passed
	Critical operation lacks event log.	Passed
	Human/contract checks bypass.	Passed
	Random number generation/use vulnerability.	Passed
	Fallback function misuse.	Passed
	Race condition.	Passed
	Logical vulnerability.	Passed
	Other programming issues.	Passed
Code Specification	Visibility not explicitly declared.	Passed
	Var. storage location not explicitly declared.	Passed
	Use keywords/functions to be deprecated.	Passed
	Other code specification issues.	Passed
Gas Optimization	Assert () misuse.	Passed
	High consumption 'for/while' loop.	Passed
	High consumption 'storage' storage.	Passed
	"Out of Gas" Attack.	Passed
Business Risk	The maximum limit for mintage not set.	Passed
	"Short Address" Attack.	Passed
	"Double Spend" Attack.	Passed

CONCLUSION:

The Smart Contract code passed the audit. We have used all possible tests based on given objects as files. Since possible test cases can be unlimited for such extensive smart contract protocol, hence we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything. Smart Contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in Status section of the report. Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract is "**Well Secured**".

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high-level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

RISK SEVERITY

Risk Severity	Definition
! Critical	No Critical severity issues found
! High	No High severity issues found
! Medium	No Medium severity issues found
! Low	No Low severity issues found
Verified	28 Functions and instances checked
Safety Score	90 out of 100

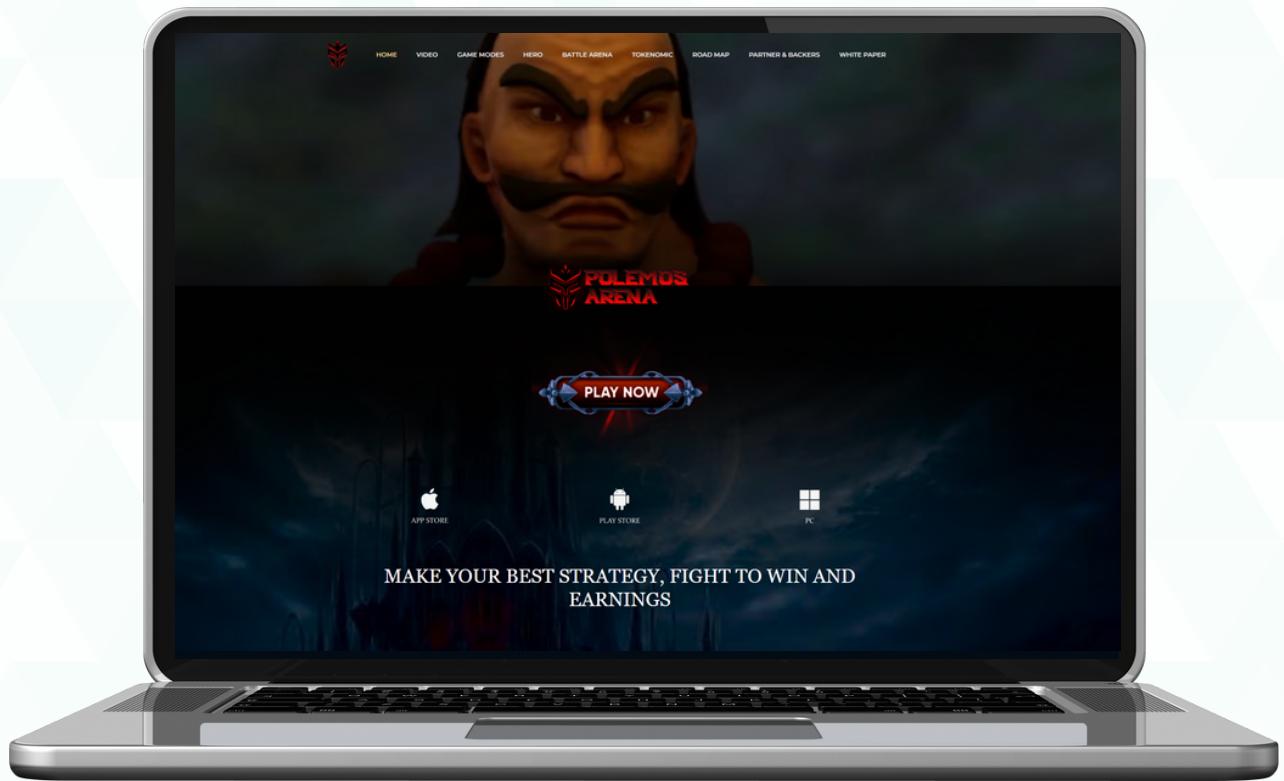
POLEMOS ARENA (POLE) has not shown any critical vulnerabilities or errors, the project has a transparent contract with no hidden features. However there's still unlocked owner wallet (54,4%) of total supply which may be suspicious. In the next part of the audit, we will check the website and social media of POLEMOS ARENA project.



TrustFacture



WEBSITE



www.polemosarena.com

Google Speed Insight Score:

Not passed

Domain Registration Date:

2022-05-29

Security Test:

Passed

Domain Expire Date:

2027-05-29

Whitepaper:

Realeased

Roadmap:

Detailed, presented in 9 phases

Interesting design, multipage website with all the necessary informations but there are too many images/videos which cause a significant reduction in page performance and speed

The site is secure and has an SSL certificate. The domain is registered for 5 years which means that the creators of the project plan to develop it for a long time. Not optimized for mobile and PC devices. CLS and optimization of images/videos need improvement for better results.

SOCIAL MEDIA



The site has active social media such as:

Twitter:

twitter.com/PolemosArena

Created in June 2022
33,6K Followers
Logo + Banner

Telegram:

t.me/PolemosArena

71K Group members
Active community
Logo and description

Discord:

No Discord

DISCLAIMER

By reading this report or any part of it, you agree to the terms of this Disclaimer. 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

TrustFacture.com owns no duty of care towards you or any other person, nor does

TrustFacture.com make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided as is, without any conditions, warranties or other terms of any kind except as set out in this disclaimer, TrustFacture.com hereby excludes all representations, warranties, conditions and other terms, TrustFacture.com hereby excludes all

liability and responsibility and neither you nor any other person shall have any claim against TrustFacture.com for any amount or kind of loss or damage that may result to you or any other person[including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and water in delict, tort (including without limitations negligence),

contract, breach of statutory duty, misinterpretation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction] in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. 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 intended 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.

Snipe. Finance's positions that each company and individual are responsible for their own due diligence and continuous security. TrustFacture.com goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The analysis of the security is purely based on the smart contract, website and social media. No applications were reviewed for security.



TrustFacture

ABOUT US



TrustFacture

WE ARE A FAST GROWING AGENCY OFFERING SMART CONTRACT AUDITS, KYC AND EFFECTIVE MARKETING.

WHAT WE OFFER?

FULL SMART CONTRACT AUDIT - WE WILL THOROUGHLY REVIEW YOUR SMART CONTRACT. MANUALLY LINE BY LINE AS WELL AS WITH AUTOMATED TOOLS.

FAST - WE DELIVER OUR AUDITS FROM 6 TO 48H AFTER WE RECEIVE YOUR MONEY.

AFFORDABLE - WE PROVIDE AUDITS AT AN AFFORDABLE PRICE FOR EVERYONE.

PREMIUM AND CLEAN LOOK - OUR AUDITS HAVE A CLEAR DESIGN AND MOST IMPORTANTLY, THEY ARE EASY TO READ FOR NEW INVESTORS.

OUR SERVICES:

PREMIUM SMART CONTRACT SECURITY AUDIT
KYC - ONLINE IDENTITY VERIFICATION PROCESS OFFERS MAXIMUM SECURITY AND TRUST FOR YOUR INVESTORS

SOCIAL MEDIA MARKETING
SEO AND **REVIEW** OF YOUR PROJECT BY OUR TEAM.

CONNECT WITH US:

WEBSITE: WWW.TRUSTFACTURE.COM

TELEGRAM: T.ME/TRUSTWOJTEK

TWITTER: WWW.TWITTER.COM/TRUSTFACTURE