Audits

BY

ICSA

www.icsa.website

Disclaimer

ICSA audits and reports should not be considered as a form of project's
"advertisement" and does not cover any interaction and assessment from "project's contract"
to
"external contracts" such as Pancakeswap or similar.

ICSA does not provide any warranty on its released reports.
We should not be used as a decision to invest into an audited project please do
your own research. ICSA provides transparent reports to all its "clients" and to its
"clients participants" and will not claim any guarantee of bug-free code within its Smart
Contract.

Each company or project shall be liable for its own security flaws and functionalities.
ICSA presence is to analyze, audit and assess the client's smart contract's code.

Scope of Work

The main focus of this report/audit, is to document an accurate assessment of the condition of
the smart contract and whether it has any security flaws in the implementation of the contract.
GamersXP team agreed and provided us with the files that needed to be tested (Through Github, PolygonScan, files, etc.). ICSA will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, white paper and repository where available, which has been provided by the project. Code is reviewed manually and with the use of software using industry best practices.

Project

GamersXP mission is to introduce a platform that extends beyond and channels consistent value back into the gaming industry. Unique GamersXP avatars and collectibles are minted as valuable NFTs through gamers' interactions within the platform. As the first PoA gamers platform, GamersXP empowers players to earn rewards for their achievements from eSports titles, favorite games and exclusive titles.

Overview

ICSA was commissioned by GamersXP to perform an audit of their smart contract:

0x6ca6F60bd339Da93124ba29E4fd957aEe766B1b3 *

Blockchain —> Polygon Chain

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token Name - GamersXP

Token Description - Rewards Token

Compiler Version - v0.8.2

Current Holders - 363 Addresses

Current Transaction Count - 3441

Max Supply - 800,000,000 GMXP

Token Ticker - GMXP

Decimals - 10

LP Lock - N/A (No liquidity)

KYCd by - ICSA*

Buy Fee - 4%

Sell Fee - 4%

Socials

GMXP Telegram

GMXP Website

GMXP Twitter

GMXP Discord

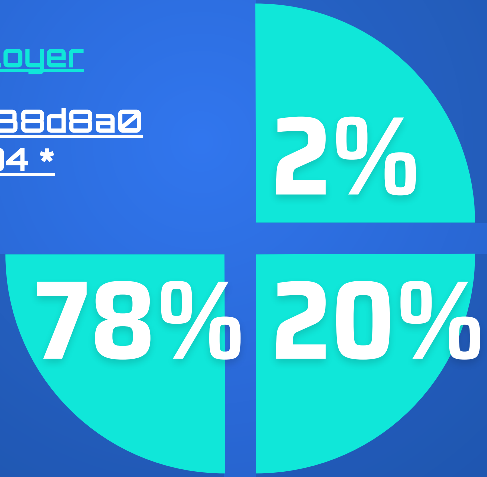
Tokenomics

Contract Address

**0x6ca6F60bd339Da93124ba2
9E4fd957aEe766B1b3 ***

Contract Owner/Deployer

**0x8e2eEfae04b191137438d8a0
7b72c9CD3512F9D4 ***



Burn Fee

2% of the tokens 4% fees go towards a Token Burn generating supply decrease

Project Development

78% of the tokens 4% fees go to the further development of the project

Rewards

20% of the tokens 4% fees get distributed back to Holders as a reward

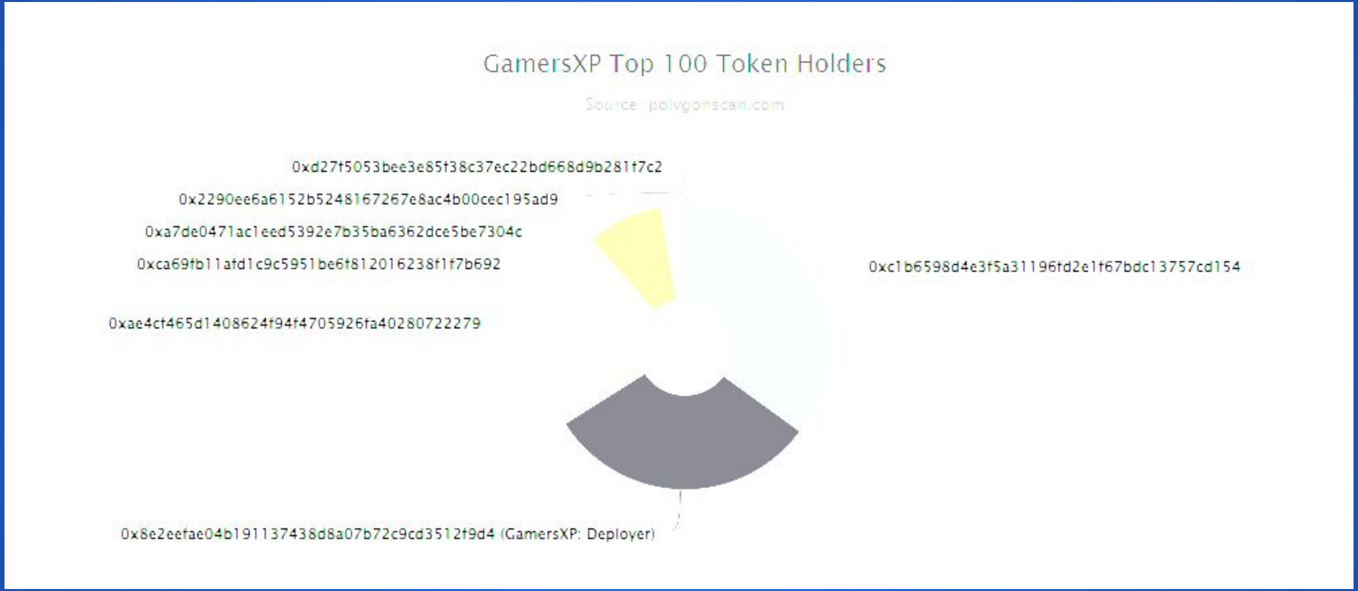
Owner Privileges

Notes

The owner has some privileges/authority to make SOME changes.

- Ownership HAS NOT been renounced
- The contract uses the UUPS (Universal Upgradeable Proxy Standard) pattern.
- Owner can pause transfers and can exclude wallets from reward.

Top 100 Holders



GamersXP Top 100 Token Holders

Source: polygonscan.com

The total supply of 800 Million tokens are held by the top 100 holders.

#1 *The Top Wallet* holds 34.9% (279,656,000)

Adjustable Functions

WRITE FUNCTIONS AS PROXY

1. Add Scheme
2. Approve
3. Burn
4. Buy Scheme
5. Decrease Allowance
6. Exclude From Reward
7. Grant Role
8. Include In Reward
9. Increase Allowance
10. Initialize
11. Renounce Role
12. Revoke Role
13. Reward
14. Set Excluded From Fee
15. Transfer
16. Transfer From
17. Update Scheme
18. Upgrade to
19. Upgrade To And Call

Vulnerabilities

Passed = No Issues detected. Code is in good working order

Low Issue = Low-level weakness/vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution.

High Issue = High-level weakness/vulnerabilities

SCAN RESULTS

SWC-100 –> Function Default Visibility = PASSED

SWC-101 –> Integer Overflow and Underflow = PASSED

SWC=102 –> Outdated Compiler Version = PASSED

SWC-103 –> Floating Pragma = PASSED

SWC-104 –> Unlocked Call Return Value = PASSED

Vulnerabilities

SCAN RESULTS

SWC-105 —> Unprotected Ether Withdrawal = PASSED

SWC=106 —> Unprotected SELF DESTRUCT Instruction = PASSED

SWC-107 —> Reentrancy = PASSED

SWC-108 —> State Variable Default Visibility = PASSED

SWC-109 —> Uninitialized Storage Pointer = PASSED

SWC-110 —> Assert Violation = PASSED

SWC-111 —> Use of Deprecated Solidity Functions = PASSED

SWC-112 —> Delegatecall to Untrusted Callee = PASSED

Vulnerabilities

SCAN RESULTS

SWC-113 –> DoS with Failed Call = PASSED

SWC-114 –> Transaction Order Dependence = PASSED

SWC-115 –> Authorization Through Tx. Origin = PASSED

SWC-116 –> Block Values as a Value for Time = PASSED

SWC-117 –> Signature Malleability = PASSED

SWC-118 –> Incorrect Constructor Name = PASSED

SWC-119 –> Shadowing State Variables = PASSED

SWC-120 –> Weak Source of Randomness From Chain Attributes = PASSED

Vulnerabilities

SCAN RESULTS

SWC-121 –> Missing Protection Against Signature Replay Attacks = PASSED

SWC-122 –> Lack of Proper Signature Verification = PASSED

SWC-123 –> Requirement Violation = PASSED

SWC-124 –> Write to Arbitrary Storage Location = PASSED

SWC-125 –> Incorrect Inheritance Order = PASSED

SWC-126 –> Insufficient Gas Griefing = PASSED

SWC-127 –> Arbitrary Jump with Function Type Variable = PASSED

SWC=128 –> DoS with Block Gas Limit = PASSED

Vulnerabilities

SCAN RESULTS

SWC-129 —> Typographical Error = PASSED

SWC-130 —> Right-to-Left Override Control Character = PASSED

SWC-131 —> Presence of Unused Variables = PASSED

SWC-132 —> Unexpected Ether Balance = PASSED

SWC-133 —> Hash Collisions with Multiple Variable Length Arguments = PASSED

SWC-134 —> Message Call with Hardcoded Gas Amount = PASSED

SWC-135 —> Code with no effects = PASSED

SWC-136 —> Unencrypted Private Data On-Chain = PASSED

No Issues Found

Please Note:

No issues found within the code! There are no functions that can affect the security of the contract.

Manual Review Notes

The contract is feature-rich but complex, we have thorough tested and audited to ensure security and efficiency.

Functions are generally safe due to role restrictions, but misuse of admin roles could be dangerous, team has been KYC through ourselves.

Overall Assessment

Satisfactory!

GamersXP has successfully passed the ICSA Audit!

June 13th, 2024

Closing Notes

Enhance the security of your crypto smart contracts with ICSA - the company you can trust with your digital assets. Contact us today to schedule an audit and benefit from our cutting-edge expertise in securing your blockchain projects. ICSA: Your gateway to safer, more secure smart contracts.

Whilst there are limitless ownable callable functions that have the potential to be dangerous,. Trust in the team would mitigate many of these risks. Please make sure you do your own research. If in doubt please contact the project team.

Always make sure to inspect all values and variables.
This includes, but is not limited to: · Ownership · Proper Ownership Renouncement (if any) · Taxes · Transaction/Wallet Limits · Token Distributions · Timelocks · Liquidity Locks · Any other owner-adjustable settings or variables.

Thank you for choosing ICSA