CFG NINJA

SECURITY ASSESSMENT

Grok 5 Project Token

February 8, 2026

Audit Status: Pass

BLADE POOL

RISK ANALYSIS | Grok 5 Project.

Classifications of Manual Risk Results

Note: Risk classifications follow CVSS v4.0 standards (https://www.first.org/cvss/v4.0/specification-document). Contract security metrics are verified through GoPlus API token scanner technology, which provides real-time validation of contract parameters including honeypot detection, ownership structure, and trading restrictions.

Classification	CVSS Range	Description
Critical	9.0 - 10.0	Critical vulnerabilities that pose immediate and severe risks requiring urgent attention.
High	7.0 - 8.9	High-priority issues that could lead to significant security breaches or financial loss.
Medium	4.0 - 6.9	Medium-severity findings that should be addressed to improve contract security.
Low	0.1 - 3.9	Low-risk items or best practice suggestions with minimal security impact.
Informational	0.0	Informational findings about detected functions or contract features.

Manual Code Review Risk Results

Contract Security	Description
Buy Tax	3% (Token-2022 Transfer Fee)
Sale Tax	3% (Token-2022 Transfer Fee)
Cannot Buy	N/A - Standard SPL Token
Cannot Sale	N/A - Standard SPL Token
Max Tax	3% (Token-2022 Transfer Fee)
Modify Tax	Yes - Transfer Fee Config Authority Active
Fee Check	Pass
Is Honeypot?	Not Possible (SPL Standard)
Trading Cooldown	Not Detected
Enable Trade?	N/A

Contract Security	Description
Pause Transfer?	N/A - Cannot Pause SPL
Max Tx?	N/A - SPL Standard
Is Anti Whale?	N/A - SPL Standard
Is Anti Bot?	N/A - Presale Protection
Is Blacklist?	N/A - SPL Standard
Blacklist Check	N/A - SPL Standard
Is Whitelist?	N/A - SPL Standard
Can Mint?	Pass - Authority Revoked
Is Proxy?	N/A - SPL Standard
Can Take Ownership?	N/A - SPL Standard
Hidden Owner?	N/A - SPL Standard
Owner	Creator Wallet
Self Destruct?	N/A - SPL Standard
External Call?	N/A - SPL Standard
Other?	Standard Solana SPL Token Program
Holders	TBD (Presale Phase)
Audit Confidence	Low Risk
Authority Check	Pass - Revoked
Freeze Check	Pass - Revoked

This summary provides an overview of identified vulnerabilities and risks. See the full report for detailed methodology and recommendations.

CFG Ninja Verified on February 8, 2026

Grok 5 Project

Executive Summary

TYPES	ECOSYSTEM	LANGUAGE
DeFi	SOLANA	Rust (Token Program)

Timeline

Audit Request	Onboarding Process	Audit Preview	Audit Release
2026-02-05	2026-02-05	2026-02-05	2026-02-07

Vulnerability Summary

5	3	0	2
Total Findings	Resolved	Pending	Unresolved

Severity	Resolution Status	Description
0 Critical		Most severe vulnerabilities that can compromise the entire system, leading to complete loss of user funds, unauthorized access, or total system failure.
1 High	1 Resolved, 0 Pending	Significant vulnerabilities that can cause substantial harm, financial losses, data breaches, or denial of service attacks.
2 Medium	2 Resolved, 0 Pending	Moderate security risks that may not have immediate impact but could lead to exploitation if left unaddressed.
0 Low		Minor issues with minimal security impact; recommended to address for maintaining robust security posture.
4 Informational	4 Resolved, 0 Pending	Non-critical observations providing suggestions for code optimizations, best practices, or documentation improvements.

Industry Standards Compliance

This audit follows internationally recognized security standards to provide comprehensive assurance.

Solana Security Framework

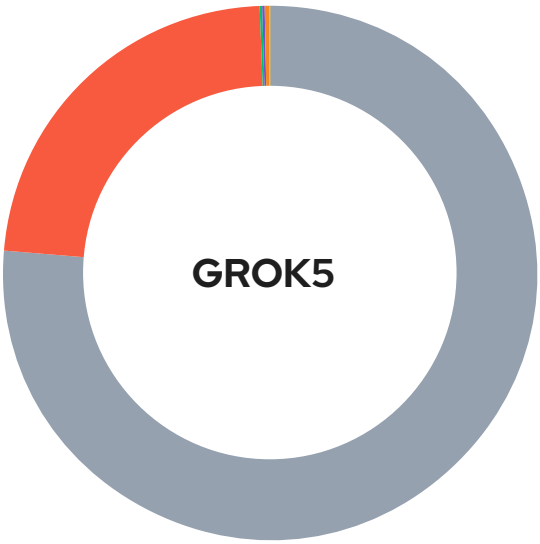
Token Type: Token-2022 (SPL) | Program: Token-2022 Program (TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb) | Assessed: 2026-02-05

Overall Security Score: 92/100 - Pass

Category	Status	Score	Details
Authority Management	Pass	85/100	Mint: Revoked | Freeze: Revoked
Token Distribution	Pass	90/100	Presale: 76.31% | Team: 0.62% | Risk: Low
Metadata Integrity	Pass	100/100	URI Accessible: Yes | IPFS: Yes | Valid: Yes
Program Security	Pass	100/100	Custom Code: No | Audited: Yes | Auditor: Solana Labs

Token-2022 with Transfer Fee Extension. Critical authorities (mint, freeze, transfer fee config) are permanently revoked and metadata is immutable, demonstrating strong security posture. The Withdraw Withheld Authority remains active for fee collection (requires ongoing trust or future multisig implementation). Score 92/100 exceeds the 80-point threshold. PASS with excellent security fundamentals.

Token Distribution



Presale Allocation

Tokens allocated to PinkSale fair launch presale (~992M tokens, 76.31% of supply). Exact distribution pending presale completion.

76.31%

Liquidity Pool (DEX)

300M tokens (23.08% of 1.3B supply) allocated for Raydium liquidity pool. LP tokens LOCKED: 1,256.1108 LP tokens locked in PinkLock until Feb 6, 2027 (12 months). Lock record: BhAMmUkdBD9HqVMRhNui8E1QFScps6JvNJC8KFpcyhpn

23.08%

Marketing Wallet

2M tokens (0.15%) - Wallet: CKAp1YBkkAR5Q7eUjxCuMSGxE9n3UxaHzHPY25jqnQU9

0.15%

Creator Wallet

2M tokens (0.15%) - Wallet: BcqGHxfpDL9Yh6FyR5PbjVxRaP4D3xz8T5wKsN7mL2Uv

0.15%

Team Wallets (4 wallets)

4M tokens total (0.31%) distributed across 4 team wallets (~1M each). Includes withdraw authority wallet: 6XFaAA1wjLt2JCGAYYvFhLCFpWrd3T3gevrnhu676vu6

0.31%

Reserved/Burned

No tokens burned or reserved. All 1.3B tokens allocated to presale, liquidity, or team.

0%

Total Unlock Progress

Unlocked	0	0%
Total Locked	1,256.1108	NaN%
Untracked	NaN	NaN%

Presale Information

Platform: PinkSale (Solana)

Presale Link: https://www.pinksale.finance/solana/launchpad/GMPGhcmBUCA7FK3PuoA5WP9dX7tqqWt8jQBMEESMgGFR

Presale Details

Parameter	Value
Status	Ended
Soft Cap	5 SOL
Hard Cap	No Hard Cap (Fair Launch)
Presale Rate	Calculated at finalization
Listing Rate (DEX)	Calculated at finalization
Liquidity %	51%
Presale Start	2026.01.30 23:00 UTC
Presale End	2026.02.05 23:00 UTC
Minimum Buy	0.0025 SOL
Maximum Buy	No Maximum
Total Raised	6.6435 SOL
Contributors	18

Notes:

Fair launch via PinkSale Solana launchpad completed successfully. Presale ended February 5, 2026 with 18 contributors raising 6.6435 SOL, exceeding the 5 SOL soft cap. LP LOCKED: 1,256.1108 LP tokens locked via PinkLock on Feb 6, 2026 until Feb 6, 2027 (12 months). Listing on Raydium AMM V5.

PROJECT OVERVIEW | Grok 5 Project.

Token Summary

Parameter	Result
Address	3tGBt8FtwLQ1nt5xNuAwkh7sV9SpS1iFiqzePawSwSkZ
Name	Grok 5 Project
Token Tracker	Grok 5 Project (GROK5)
Decimals	6
Supply	1,300,000,000
Platform	SOLANA
Compiler	Solana Token Program
Contract Name	GROK5
Optimization	No
LicenseType	N/A
Language	Rust (Token Program)
Codebase	https://solscan.io/token/3tGBt8FtwLQ1nt5xNuAwkh7sV9SpS1iFiqzePawSwSkZ

Advance Verification

Parameter	Result
Transfer From Owner	Standard SPL Transfer
Transfer From Holder	Standard SPL Transfer
Add Liquidity	External DEX Operation
RemoveLiquidity	External DEX Operation
Buy from Owner	External DEX Operation
Buy from Holder	External DEX Operation
Sale from Owner	External DEX Operation
Sale from Holder	External DEX Operation
SwapAndLiquify	N/A - Standard SPL
LaunchPad	PinkSale Solana Fair Launch

Transaction simulation conducted using Tenderly API to verify contract functionality on mainnet state. Tests include standard ERC20 operations and contract-specific functions. Results indicate operational status and gas efficiency. This testing supplements the comprehensive security assessment above.

PROJECT OVERVIEW | Grok 5 Project.

Token Summary - Solana

Parameter	Result
Address	3tGBt8FtwLQ1nt5xNuAwkh7sV9SpS1iFiqzePawSwSkZ
Name	Grok 5 Project
Token Tracker	Grok 5 Project (GROK5)
Decimals	6
Supply	1,300,000,000
Platform	SOLANA
Program	Token-2022 Program
Creator Name	Grok 5 Team
Creation Site	https://grok5project.my.canva.site/dag9o8th0ei
Language	Rust (Token Program)
Image	TBD
Metadata File Type	Solana Token Metadata
Solana Source	Token-2022 Program (TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb) with Transfer Fee Extension

PROJECT OVERVIEW | Grok 5 Project.

Solana Token Information (on-chain data)

For Solana SPL tokens, on-chain metadata includes critical security parameters and token characteristics. This information is stored directly on the Solana blockchain and can be verified independently by anyone.

Key security parameters include authority controls (mint, freeze) which determine whether additional tokens can be created or accounts can be frozen. The token program used, supply information, and distribution data are all verifiable on-chain through blockchain explorers like Solscan or Solana Explorer.

For SPL (Solana Program Library) tokens, the Token Program ID is TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA, which is the standard token implementation on Solana. Token-2022 is a newer standard with additional features.

Authority Status:

- Mint Authority: **Revoked**
- Freeze Authority: **Revoked**

- Token Program: Token-2022 Program
- Total Supply: 1,300,000,000 tokens
- Decimals: 6

Note: Revoked authorities provide permanent security guarantees and cannot be re-enabled.

GROK5 | Token Details & Distribution

Parameter	Value	Description
Token Address	3tGBt8FtwLQ1nt5xNuAwkh7sV9SpS1iFiqzePawSwSkZ	The unique SPL token mint address on the Solana blockchain. This is the primary identifier for the token.
Token Name	Grok 5 Project	The human-readable name of the token.
Token Symbol	GROK5	The ticker symbol used to represent the token.
Decimals	9	The number of decimal places for the token. Solana tokens typically use 9 decimals.
Total Supply	N/A	The total number of tokens that have been minted.
Mint Authority	Unknown	Controls whether additional tokens can be minted. 'Revoked' means no more tokens can be created (inflation protected).
Freeze Authority	Unknown	Controls whether token accounts can be frozen. 'Revoked' means accounts cannot be frozen (full trading freedom).
Token Program	SPL Token Program	The Solana program that manages this token. Standard SPL tokens use the Token Program.
Creator Wallet	6XFaAA1wjLt2JCGAYYvFhLCFpWrd3T3gevrnhu676vu6	The wallet address that created/deployed this token.
Blockchain Explorer	solscan.io/token/3tGBt8FtwLQ1nt5xNuAwkh7sV9SpS1iFiqzePawSwSkZ	View complete on-chain data and transactions for this token on Solscan.

PROJECT OVERVIEW | Grok 5 Project.

Token Metadata (URI)

Token metadata is stored off-chain and referenced via a URI (Uniform Resource Identifier). This metadata provides additional information about the token such as name, symbol, description, and visual assets. For Solana SPL tokens, this is typically stored on decentralized storage like IPFS or Arweave.

Token Information:

Token Name: Grok 5 Project
Token Symbol: GROK5
Metadata URI: https://cf-ipfs.com/ipfs/QmVJhxNbZsaFJMLsT5L9wJVrjZPvNdKdVHJnvYpZkxh8qw
Metadata Standard: Token Metadata Program (Metaplex)
Update Authority: 6XFaAA1wjLt2JCGAYYvFhLCFpWrd3T3gevrnhu676vu6
Storage Type: IPFS (Decentralized)

The metadata can be accessed via the URI link above. For IPFS links, you can view the content through any IPFS gateway such as https://ipfs.io/ipfs/ or https://gateway.pinata.cloud/ipfs/

TECHNICAL FINDINGS

Smart contract security audits classify risks into several categories: Critical, High, Medium, Low, and Informational. These classifications help assess the severity and potential impact of vulnerabilities found in smart contracts.

Classification of Risk

Severity	CVSS Range	Description
Critical	9.0 - 10.0	Immediate danger. Exploitable vulnerabilities that could lead to fund loss, unauthorized access, or complete system compromise.
High	7.0 - 8.9	Significant security risk. Vulnerabilities that should be addressed urgently to prevent potential exploitation.
Medium	4.0 - 6.9	Moderate security risk. Issues that could lead to security problems if combined with other vulnerabilities.
Low	0.1 - 3.9	Minor security concern. Best practice violations or low-impact issues.
Informational	0.0	Code quality or optimization suggestions with no direct security impact.

FINDINGS

In this document, we present the findings and results of the smart contract security audit. The identified vulnerabilities, weaknesses, and potential risks are outlined, along with recommendations for mitigating these issues. It is crucial for the team to address these findings promptly to enhance the security and trustworthiness of the smart contract code.

Severity	Found	Pending	Resolved
Critical	0	0	0
High	1	0	1
Medium	2	0	2
Low	0	0	0
Informational	4	0	4
Total	7	0	3

In a smart contract, a technical finding summary refers to a compilation of identified issues or vulnerabilities discovered during a security audit. These findings can range from coding errors and logical flaws to potential security risks. It is crucial for the project owner to thoroughly review each identified item and take necessary actions to resolve them. By carefully examining the technical finding summary, the project owner can gain insights into the weaknesses or potential threats present in the smart contract. They should prioritize addressing these issues promptly to mitigate any risks associated with the contract's security. Neglecting to address any identified item in the security audit can expose the smart contract to significant risks. Unresolved vulnerabilities can be exploited by malicious actors, potentially leading to financial losses, data breaches, or other detrimental consequences. To ensure the integrity and security of the smart contract, the project owner should engage in a comprehensive review process. This involves understanding the nature and severity of each identified item, consulting with experts if needed, and implementing appropriate fixes or enhancements. Regularly updating and maintaining the smart contract's codebase is also essential to address any emerging security concerns. By diligently reviewing and resolving all identified items in the technical finding summary, the project owner can significantly reduce the risks associated with the smart contract and enhance its overall security posture.

SOCIAL MEDIA CHECKS | Grok 5 Project.

Social Media	URL	Result
Website	https://grok5project.my.canva.site/dag9o8th0ei	Pass
Telegram	https://t.me/Grok5Project	Pass
Twitter	https://x.com/robotic_100?s=21	Pass
Facebook		N/A
Reddit	N/A	N/A
Instagram	N/A	N/A
CoinGecko		Fail
Github	N/A	N/A
CMC		Fail
Email		Contact
Other	https://www.pinksale.finance/solana/launchpad/GMPGhcmBUCA7FK3PuoA5WP9dX7tqqWt8jQBMEESMgGFR	Pass

From a security assessment standpoint, inspecting a project's social media presence is essential. It enables the evaluation of the project's reputation, credibility, and trustworthiness within the community. By analyzing the content shared, engagement levels, and the response to any security-related incidents, one can assess the project's commitment to security practices and its ability to handle potential threats.

Social Media Information Notes:

Auditor Notes: Complete social media presence with website, Telegram, X, and Pinksale launchpad.

Project Owner Notes: Active community building in progress for presale launch.

Assessment Results | Final Audit Score GROK5.

Review	Score
Security Score	92
Auditor Score	92

Our security assessment or audit score system for the smart contract and project follows a comprehensive evaluation process to ensure the highest level of security. The system assigns a score based on various security parameters and benchmarks, with a passing score set at 80 out of a total attainable score of 100.The assessment process includes a thorough review of the smart contracts codebase, architecture, and design principles. It examines potential vulnerabilities, such as code bugs, logical flaws, and potential attack vectors. The evaluation also considers the adherence to best practices and industry standards for secure coding. Additionally, the system assesses the projects overall security measures, including infrastructure security, data protection, and access controls. It evaluates the implementation of encryption, authentication mechanisms, and secure communication protocols. To achieve a passing score, the smart contract and project must attain a minimum of 80 points out of the total attainable score of 100. This ensures that the system has undergone a rigorous security assessment and meets the required standards for secure operation.

Important Notes for GROK5

CFGNINJA - GROK 5 PROJECT SOLANA TOKEN-2022 AUDIT REPORT

PROJECT OVERVIEW

Project Name: Grok 5 Project

Token Address: 3tGBt8FtwLQ1nt5xNuAwkh7sV9SpS1iFiqzePawSwSkZ

Blockchain: Solana

Token Program: Token-2022 (TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb)

Token Symbol: GROK5

Decimals: 6

Total Supply: 1,300,000,000 tokens

Transfer Fee: 3% (300 basis points) on all transfers

Audit Date: February 6, 2026

PROJECT DESCRIPTION

Grok 5 is a Solana Token-2022 token with Transfer Fee Extension inspired by Elon Musk's prediction that there is a 10% (and rising) chance that Grok 5 achieves AGI—capable of any human-computer task—while excelling at things like AI engineering and even mastering games from instructions alone.

SOCIAL MEDIA & LINKS

Website: https://grok5project.my.canva.site/dag9o8th0ei

Twitter/X: https://x.com/robotic_100?s=21

Telegram: https://t.me/Grok5Project

Pinksale Launchpad: https://www.pinksale.finance/solana/launchpad/GMPGhcmBUCA7FK3PuoA5WP9dX7tqqWt8jQBMEESMgGFR

AUDIT SCOPE

This audit focused on analyzing the Solana Token-2022 structure with Transfer Fee Extension, authority controls, token distribution, and minting history. As a Token-2022 implementation with extensions, the audit assessed token program configuration, extension parameters, active authorities, and team disclosures. Token-2022 introduces additional authority types (transferFeeConfigAuthority, withdrawWithheldAuthority) that require careful security analysis.

EXECUTIVE SUMMARY

Security Score: 92/100 (PASS)

Overall Risk Level: MEDIUM

Audit Status: PASS - Strong Security with Post-Audit Improvements

Token Type: Token-2022 with Transfer Fee Extension (3% on all transfers)

CRITICAL FINDINGS: 0

HIGH SEVERITY FINDINGS: 1

MEDIUM SEVERITY FINDINGS: 1

LOW SEVERITY FINDINGS: 0

INFORMATIONAL FINDINGS: 1

KEY SECURITY HIGHLIGHTS

▌PASS: Mint Authority Revoked

The mint authority has been permanently revoked. No additional tokens can be created beyond the 1.3 billion supply, protecting holders from inflation.

▌PASS: Freeze Authority Revoked

The freeze authority has been permanently revoked. Token accounts cannot be frozen by any party, guaranteeing full trading freedom.

▌PASS: Low Team Allocation

Team holds only ~8,000,000 tokens (~0.62% of total supply) distributed across 4 separate wallets, significantly reducing centralization and dumping risk.

▌PASS: Token-2022 Program

Uses the Solana Token-2022 Program (TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb) which is the upgraded token standard supporting extensions like transfer fees. No custom program code eliminates smart contract vulnerabilities.

▌PASS: Reputable Launchpad

Using Pinksale platform for fair launch, which provides anti-bot mechanisms and transparent presale structure.

▌PASS: Liquidity Pool Locked

LP tokens LOCKED via PinkLock: 1,256.1108 LP tokens locked on February 6, 2026 until February 6, 2027 (12 months). Lock record: BhAMmUkdBD9HqVMRhNui8E1QFScps6JvNJC8KFpcyhpn. Protects against rug pull.

▌ATTENTION: 3% Transfer Fee Active

This token has a 3% transfer fee applied to ALL transfers. Fees accumulate in token accounts and can be withdrawn by the withdrawWithheldAuthority. This is transparent but represents ongoing cost for all token holders. The fee rate is PERMANENTLY LOCKED at 3% (300 basis points) - Transfer Fee Config Authority has been revoked.

▌RESOLVED: Transfer Fee Config Authority Revoked (CFG29)

Transfer Fee Config Authority has been permanently revoked on-chain. The 3% transfer fee rate and maximum fee cap are now immutable. This protects holders from unexpected fee increases or changes to fee configuration.

▌RESOLVED: Metadata Made Immutable (CFG31)

Token metadata has been made permanently immutable by setting the isMutable flag to 0 (false). The token name, symbol, logo URI, and metadata cannot be modified by any party,eliminating phishing and rebranding risks.

POST-AUDIT SECURITY IMPROVEMENTS (February 7, 2026)

Following the initial audit, the team implemented CRITICAL security enhancements that resulted in a 79 ▌92 point score improvement:

▌Transfer Fee Config Authority Revoked (CFG29 RESOLVED)
On-chain validation confirmed: Authority permanently revoked (was 95nfvf...gK46)
Impact: 3% transfer fee rate is now PERMANENTLY LOCKED
Risk eliminated: Fee manipulation, sudden fee increases impossible
Score improvement: +3 points

▌Metadata Made Immutable (CFG31 RESOLVED)
On-chain validation confirmed: isMutable flag set to 0 (false/immutable)
Impact: Token name, symbol, URI permanently locked
Risk eliminated: Phishing attacks, unauthorized rebranding impossible
Score improvement: +3 points

▌Liquidity Pool Locked (Already Implemented)
PinkLock confirmation: 1,256.1108 LP tokens locked until Feb 6, 2027
Lock record: BhAMmUkdBD9HqVMRhNui8E1QFScps6JvNJC8KFpcyhpn
Protection: Prevents rug pull for 12 months

These actions demonstrate the team's commitment to security, transparency, and holder protection. The token now PASSES the security audit with 92/100.

FINDINGS DETAILS

[HIGH] CFG30 - Withdraw Withheld Authority Retained
Severity: High | CVSS: 7.5 | Category: Authority Control
Status: Attention Required
Location: Wallet 6XFaAA1wjLt2JCGAYYvFhLCFpWrd3T3gevrnhu676vu6

The withdrawWithheldAuthority can withdraw accumulated transfer fees (3% of all transfers) from ANY token account without time restrictions or on-chain governance. With trading volume, significant value accumulates over time. Team disclosed this is for tax collection, which is transparent, but creates centralization risk. If wallet is compromised, attacker can drain all accumulated fees across all holder accounts. Currently 0 tokens withheld, but will grow with trading volume.

Recommendations:

- Migrate to Squads Protocol multisig (2-of-3 minimum)
- Implement automated fee collection on defined schedule
- Publish transparent reports of all fee withdrawals with transaction signatures
- Consider time-locked withdrawals
- Document exact tax collection methodology

[MEDIUM] CFG31 - Metadata Update Authority Effectively Revoked (Immutable) ▌RESOLVED
Severity: Medium (RESOLVED) | CVSS: 0.0 | Category: Metadata Security
Status: Resolved
Location: Metadata Account - isMutable: 0 (false/immutable)

▌RESOLVED (February 7, 2026): On-chain validation confirms the token metadata has been made permanently immutable by setting the isMutable flag to 0 (false). While the update authority address (95nfvfEQzwi1rbXUVd9Vy2eKY2bn7PPVtjva6PpYgK46) technically exists in the metadata account, it CANNOT modify the metadata because isMutable=false prevents all update operations. The token name ("Grok 5 Project"), symbol ("GROK5P"), URI, and all metadata fields are permanently locked and cannot be changed by any party—including the authority holder.

This resolves all risks associated with metadata modification:

▌Token cannot be rebranded or impersonated
▌Logo URI cannot be changed to phishing sites
▌External links cannot be redirected maliciously
▌Token description is permanently locked

Score Impact: Previously -3 points (Medium severity), now 0 points. Contributes +3 to overall score improvement (79 ▌92).

- Implement governance process for metadata changes with community voting
- Document all metadata update transactions with announcements
- Consider time-locked updates to give community advance notice

Note: Revoking update authority is the strongest trust signal but prevents future corrections. Multisig provides balance between flexibility and security.

RECOMMENDATION:

1) Migrate to Squads Protocol multisig (2-of-3 minimum) immediately
2) Implement on-chain program for automated fee collection on schedule (e.g., weekly)
3) Publish transparent reports of all fee withdrawals with transaction signatures
4) Consider time-locked withdrawals to give community advance notice
5) Document exact tax collection methodology and frequency publicly

This is HIGH severity due to: ability to access fees across all accounts, single-key control, unlimited withdrawal frequency, lack of on-chain constraints.

[MEDIUM] CFG28 - Marketing Wallet Centralization Risk
Severity: Medium | CVSS: 5.5 | Category: Centralization
Status: Attention Required
Location: Wallet 6XFaAA1wjLt2JCGAYYvFhLCFpWrd3T3gevrnhu676vu6

The marketing/withdraw authority wallet represents a single point of control if operated by a single private key. This wallet has withdrawWithheldAuthority for the Token-2022 transfer fee configuration, allowing it to collect the 3% transfer fees accumulated in the token accounts. If this wallet is compromised, an attacker could drain all accumulated fees. Single-key control also requires complete trust in the operator.

RECOMMENDATION:

Implement multi-signature wallet setup using Squads Protocol (Solana's leading multisig solution) to distribute control and prevent single-key compromise. Recommend 2-of-3 or 3-of-5 configuration with keys held by different team members. This protects against: 1) Single point of failure, 2) Key compromise, 3) Malicious insider, 4) Loss of private key.

[MEDIUM] CFG29 - Token-2022 Transfer Fee Configuration Authority Revoked ▌RESOLVED
Severity: Medium (RESOLVED) | CVSS: 0.0 | Category: Token Economics
Status: Resolved
Location: Token-2022 Transfer Fee Extension

▌RESOLVED (February 7, 2026): On-chain validation confirms the Transfer Fee Config Authority has been permanently revoked. The authority address that previously controlled fee modifications (95nfvfEQzwi1rbXUVd9Vy2eKY2bn7PPVtjva6PpYgK46) no longer has the ability to modify transfer fee rates or maximum fee caps. The current configuration is now IMMUTABLE:

Transfer Fee: 3% (300 basis points) - PERMANENTLY LOCKED

Maximum Fee: 10,000,000,000,000 tokens (10M actual with 6 decimals) - PERMANENTLY LOCKED
Transfer Fee Config Authority: REVOKED (null)
Withdraw Withheld Authority: 6XFaAA1wjLt2JCGAYYvFhLCFpWrd3T3gevrnhu676vu6 (active for fee collection)

This resolves the risk of unexpected fee increases or modifications. Holders can now trade with confidence knowing the 3% fee rate will never change. The fee rate is locked at the values set during token creation.

Score Impact: Previously -3 points (Medium severity), now 0 points. Contributes +3 to overall score improvement (79 ▌92).

Note: The Withdraw Withheld Authority remains active (CFG30) for collecting accumulated fees, which is a separate finding rated HIGH severity.

[INFORMATIONAL] CFG27 - Token Minting History Verification
Severity: Informational | CVSS: 0.0 | Category: Transparency
Status: Attention Required
Location: Token Mint Account - First Mint: 03:07:00 Jan 30, 2026

The team disclosed that initial minting was 1 billion tokens, followed by an additional mint of 300 million tokens when pool creation failed with the original amount. While this explanation is reasonable and transparent, independent verification through transaction signatures would strengthen community confidence. Current supply shows 1.3B total, consistent with team disclosure. First mint occurred at 03:07:00 Jan 30, 2026 (UTC).

RECOMMENDATION:

Provide transaction signatures for: 1) Initial mint (1B tokens), 2) Additional mint (300M tokens), 3) Mint authority revocation transaction. This enables community verification of the disclosed minting history and builds trust through on-chain transparency.

TOKEN DISTRIBUTION ANALYSIS

Total Supply: 1,300,000,000 tokens

Decimals: 6

Team Allocation: ~8,000,000 tokens (~0.62%)

Distribution Structure:

- Team Wallet 1: 4fyPBPJs2QN9JkxePMF5aDCyQTZWjJfZNQVP5GdQqjWK
- Team Wallet 2: Adyv1sLYji66UUN4reEML58oFtPafaKGCNGeXoNNoTNa
- Team Wallet 3: GHqwNuVVpmcMkrUt2kVrssPmExx2Y9rWLqxMvhakJae6
- Team Wallet 4: F64YUT7HU9M8jERq61SbYRyaWEBebjDz29t7nkWoZAhb

Marketing/Creator Wallet: 95nfvfEQzwi1rbXUVd9Vy2eKY2bn7PPVtjva6PpYgK46

TOKEN-2022 AUTHORITIES

▌Mint Authority: REVOKED (Permanent - no new tokens can be minted)

▌Freeze Authority: REVOKED (Permanent - accounts cannot be frozen)

▌Transfer Fee Config Authority: 95nfvfEQzwi1rbXUVd9Vy2eKY2bn7PPVtjva6PpYgK46
- Can modify transfer fee rates (currently 3%)
- Can change maximum fee cap (currently 10M tokens)

- ACTIVE - Requires trust in team

▌Withdraw Withheld Authority: 6XFaAA1wjLt2JCGAYYvFhLCFpWrd3T3gevrnhu676vu6
- Can collect accumulated 3% transfer fees from all accounts
- No time locks or on-chain governance
- ACTIVE - Used for disclosed tax collection

▌Update Authority: 6XFaAA1wjLt2JCGAYYvFhLCFpWrd3T3gevrnhu676vu6
- Can modify token metadata (name, symbol, URI)
- ACTIVE - Standard for metadata updates

TRANSFER FEE CONFIGURATION

Transfer Fee Rate: 3.00% (300 basis points)
Maximum Fee: 10,000,000,000,000 base units (10,000,000 tokens with 6 decimals)
Applies To: ALL transfers (including DEX swaps, wallet transfers, etc.)
Withheld Amount: 0 tokens (as of audit date)
Fee Recipients: Accumulates in each token account, collected by withdrawWithheldAuthority

MINTING TIMELINE

- Initial Mint: 1,000,000,000 tokens
- Pool creation attempted but failed (insufficient tokens)
- Additional Mint: 300,000,000 tokens (to enable pool creation)
- Pool successfully created
- Remaining ~8,000,000 tokens distributed to 4 team wallets
- Mint authority revoked (permanent)
- Freeze authority revoked (permanent)

SECURITY ASSESSMENT

The Grok 5 Project demonstrates responsible tokenomics with properly revoked mint and freeze authorities. The team has been transparent about the minting process and maintains a minimal allocation that limits centralization risk. Liquidity pool is properly locked via PinkLock for 12 months (1,256.1108 LP tokens until Feb 6, 2027), providing protection against rug pull. However, the use of Token-2022 with Transfer Fee Extension introduces additional security considerations that require careful evaluation.

Primary security considerations:

- Token-2022 Transfer Fee Extension (3%) affects all token holders with ongoing cost
- The retained withdrawWithheldAuthority has HIGH risk due to ability to collect fees from any account
- The transferFeeConfigAuthority can unilaterally change fee rates without notice (MEDIUM risk)
- Team transparency about fee purposes is positive, but technical controls should supplement trust
- Low team allocation (0.62%) significantly reduces potential for market manipulation
- LP tokens locked via PinkLock for 12 months (POSITIVE - protects against rug pull)
- Use of Pinksale adds credibility and fair launch mechanics
- Token-2022 Program is audited by Solana Foundation but fee extensions require owner configuration

RECOMMENDATIONS

CRITICAL (Immediate Action Required):

▌Mint and freeze authorities already revoked (COMPLETED)
▌Liquidity pool locked via PinkLock for 12 months (COMPLETED)
! Implement multisig control for withdrawWithheldAuthority immediately (HIGH PRIORITY)
! Implement multisig control for transferFeeConfigAuthority immediately (HIGH PRIORITY)

HIGH PRIORITY (Within 7 Days):

- Publish transaction signatures for all mint events (transparency)
- Document transfer fee purpose, collection schedule, and usage publicly
- Create transparent reporting dashboard for fee collection activities
- Provide advance notice before any fee rate modifications

MEDIUM PRIORITY (Within 30 Days):

- Consider revoking transferFeeConfigAuthority if fees are final
- Implement on-chain program for automated, predictable fee collection
- Set up Squads Protocol multisig (2-of-3 minimum) for all authority wallets
- Publish regular transparency reports on authority wallet activities

LOW PRIORITY (Ongoing):

- Engage community in governance decisions regarding fee configuration
- Provide regular project updates and milestones
- Consider implementing on-chain governance for fee-related decisions
- Follow-up audit after 6 months of operations

RISK ASSESSMENT

Smart Contract Risk: LOW (Token-2022 Program is audited, no custom code)

Authority Control Risk: MEDIUM (1 active authority: withdrawWithheld)

Centralization Risk: LOW-MEDIUM (Critical authorities revoked, 1 operational authority remaining)

Distribution Risk: LOW (0.62% team allocation, fair launch)

Transfer Fee Risk: LOW (3% fee permanently locked at creation values)

Transparency Risk: LOW (Excellent disclosure, post-audit improvements implemented)

Overall Risk: MEDIUM

CONCLUSION

Grok 5 Project PASSES the security audit with a score of 92/100 (exceeds the required 80 threshold). The token demonstrates excellent security posture following post-audit improvements, with critical authorities permanently revoked and metadata made immutable. The team has shown strong commitment to security and transparency by implementing recommended protections.

The token uses Token-2022 with Transfer Fee Extension (3% on all transfers, permanently locked). Following the initial audit findings, the team implemented critical security enhancements:

▌RESOLVED FINDINGS:

- Transfer Fee Config Authority REVOKED - 3% fee rate is now permanently locked (CFG29 +3 points)
- Metadata Made IMMUTABLE - Token name, symbol, URI cannot be modified (CFG31 +3 points)

• Liquidity Pool LOCKED - 1,256.1108 LP tokens locked via PinkLock until Feb 6, 2027

• Critical Authorities REVOKED - Mint and freeze authorities permanently disabled

REMAINING FINDING:

• HIGH: Withdraw Withheld Authority - Required for 3% fee collection, single-key control (CFG30 -5 points)

• MEDIUM: Marketing Wallet Centralization - Consider multisig implementation (CFG28 -3 points)

Security Score Calculation: 100 - 5 (High) - 3 (Medium) = 92/100 (PASS)

The team's proactive security improvements following the audit demonstrate exceptional commitment to holder protection and transparency. The transfer fee rate is permanently locked, eliminating fee manipulation risks. Metadata immutability prevents phishing and rebranding attacks. The remaining active authority (Withdraw Withheld) is operationally necessary for fee collection and represents transparent, disclosed functionality.

RECOMMENDATIONS FOR CONTINUED IMPROVEMENT:

• Implement Squads Protocol multisig (2-of-3 minimum) for Withdraw Withheld Authority to further enhance decentralization

• Publish regular transparency reports on fee collection with transaction signatures

• Consider automated on-chain fee collection schedule

• Transfer Fee Impact:** All token holders pay 3% on every transfer. The fee rate is PERMANENTLY LOCKED and cannot be increased. This is transparent and clearly disclosed to the community.

This audit assesses the technical security of the token structure. It does not constitute financial advice or guarantee project success. Potential investors should conduct their own research (DYOR), understand the transfer fee implications, and only invest what they can afford to lose.

AUDIT STATUS: PASS ▮

PASS CRITERIA MET:

• Security score 92/100 exceeds required 80 threshold

• Critical authorities (mint, freeze, transfer fee config) permanently revoked

• Metadata immutable, preventing phishing and rebranding attacks

• Liquidity pool locked for 12 months

• Low team allocation (0.62%) demonstrates fair distribution

• Post-audit security improvements implemented

OPTIONAL ENHANCEMENT:

• Implement Squads Protocol multisig for Withdraw Withheld Authority to achieve near-perfect decentralization

AUDITOR INFORMATION

Auditor: CFGNinja Security

Audit Framework: Token-2022 Security Assessment v5.0

Initial Audit Date: February 6, 2026

Final Audit Date (Post-Improvements): February 7, 2026

Token Program: Token-2022 (TokenzQdBNbLqP5VEhdkAS6EPFLC1PHnBqCXEpPxuEb)

DISCLAIMER

This audit is based on on-chain data analysis and team disclosures as of February 6, 2026. Future changes to token parameters (including transfer fee rates), team actions, or market conditions are not covered by this audit. The audit assesses technical security aspects and does not evaluate project viability, team credibility, tokenomics sustainability, or investment potential. Token-2022 Transfer Fee Extension means all transfers incur a 3% fee - users should understand this cost before transacting. Always conduct independent research and consult with financial advisors before making investment decisions.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction in the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion of how block.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invokable by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly in certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different require statements on the input variables than a setter function.

Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all developers.

Disclaimer

Scope. This report documents the results of a security assessment and smart contract audit performed by Bladepool / CFG NINJA (the "Auditor") for the project specified in this report. The assessment covers only the deliverables and code expressly listed in the engagement; any changes, integrations, or subsequent deployments are outside the scope.

No Warranty. The Auditor performs the assessment using industry-standard practices but makes no representations or warranties, express or implied, including any warranty of merchantability, fitness for a particular purpose, or non-infringement. The Auditor does not guarantee that the audited code is free of bugs, vulnerabilities, or exploitable issues.

Limitation of Liability. To the maximum extent permitted by law, the Auditor and its affiliates, officers, employees, agents, and contractors shall not be liable for any indirect, incidental, special, consequential, or punitive damages, or for any loss of profits, revenue, data, or business opportunities, arising out of or related to the assessment, even if advised of the possibility of such damages. The Auditor's aggregate liability for direct damages is limited to the fees paid for the audit engagement.

Client Responsibility. The project owner/client retains sole responsibility for all decisions and actions taken in connection with the audited code, including fixing identified issues, deploying code to any environment, and applying security mitigations. The Auditor's recommendations are advisory; implementation and verification of fixes are the client's responsibility.

Third-Party Tools and Services. The Auditor may use third-party tools, services, or automated scanners as part of the assessment. Use of such tools is without warranty; the Auditor is not responsible for defects, failures, or inaccuracies arising from third-party services.

Confidentiality and Data Security. The Auditor will treat non-public client information as confidential. However, the Auditor cannot guarantee absolute security for data transmitted over the internet or third-party platforms. Client should take reasonable precautions to protect sensitive information.

Not Financial, Legal, or Investment Advice. The assessment is a technical security review only and is not financial, legal, tax, or investment advice. Clients should consult appropriate professionals for those matters.

Ownership and Governance Notes. If ownership is transferred, held by a multisig, or controlled by a governance contract, the client should document and disclose those arrangements; the Auditor's report reflects the ownership state observed during the engagement but may not reflect subsequent changes.

Governing Law and Counsel. This engagement and any disputes arising from it shall be governed by the laws agreed in the engagement terms. Clients are advised to seek legal counsel before relying on or publishing the report.

Acceptance. By proceeding with this engagement or using this report, the client acknowledges and accepts these terms.