Background

Bitrise Audits was commissioned by Kurai Metaverse to perform an audit of smart contracts:

View here

Audit Type: Security audit

The purpose of the audit was to check the following

- Manual code review
- Website overview
- Contract functions check
- Rugproof-analysis
- Owner privileges
- Liquidity lock check

Manual code review - **Passed**

✓ Integer Underflow

✓ Integer Overflow

✓ Correct Token Standards Implementation

✓ Timestamp Dependency for Randomness

✓ Unexposed Private Transfer Function

✓ Transaction-Ordering Dependency

The contract code is verified on **BSCScan**. Common vulnerabilities were not found in the token's Smart Contract as shown above.

Website overview - **Passed**

Desktop view - Tested & Verfied

Mobile view - Tested & Verified

✓ Mobile Friendly   ✓ No JavaScript Errors   ✓ Spell Check   ✓ SSL Certificate

Contract functions check - **Passed**

Mint, _mint, updateSwapAndLiquifyEnabled, updateTransferTaxRate,

Rug-proof analysis - **Passed**

LP Tokens Burned & Few are being held for FEGEX deployer

Risk factor : **Medium**

Owner privileges - **Passed**

In the period when the ownership is not renounced

- Owner can mint new tokens in contract
- Owner can mint new tokens to a specific address
- Owner can update swap settings
- Owner can change transaction fee

Liquidity lock check - **Passed**

Liquidity locking details are provided by the project owner :

View here

Download Audit Report

Bitrise Audit Note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by project owner