🔐 SMART CONTRACT SECURITY AUDIT REPORT

Project Name: SALZJYUR
Token Symbol: SZUR
Blockchain: Polygon (PoS)
Contract Type: ERC-20 Token
Solidity Version: ^0.8.18
Audit Type: Free / Community Audit (Manual Review)
Audit Date: December 2025

📌 AUDIT SCOPE

The following smart contract was reviewed:

- **SALZJYUR.sol**

The audit focused on:

- Security vulnerabilities
- ERC-20 standard compliance
- Token transfer logic
- Tax and burn mechanisms
- Anti-bot and anti-whale systems
- Owner permissions and centralization risks
- Polygon DEX compatibility

🧠 AUDIT METHODOLOGY

The audit included:

- Manual line-by-line code review
- Logical flow analysis
- Known vulnerability pattern checks
- ERC-20 compliance verification
- Best-practice comparisons

⚠️ This audit does not guarantee the absence of bugs but highlights known risks and behaviors.

✅ POSITIVE FINDINGS

✔ No Critical Vulnerabilities

- No reentrancy risks
- No unchecked arithmetic (Solidity 0.8+)
- No unsafe external calls

✔ Supply Cap Enforced

- Maximum total supply capped at **200,000,000 SZUR**
- Minting cannot exceed cap

✔ Reasonable Token Tax (1%)

- Burn: 0.1%
- Liquidity Wallet: 0.45%
- Marketing Wallet: 0.45%

✔ Anti-Bot Protection

- Per-address cooldown mechanism
- Helps reduce bot activity during launch

✔ Anti-Whale Limits

- Max transaction: **0.5% of total supply**
- Max wallet holding: **1.5% of total supply**

⚠️ IDENTIFIED RISKS & OBSERVATIONS

🟡 MEDIUM RISK

1. Anti-Bot and DEX Compatibility

Anti-bot cooldown applies to sender addresses.
On decentralized exchanges, this may affect pair contracts and cause failed swaps if not excluded.

Recommendation:
Exclude DEX pair addresses from anti-bot logic.

2. Liquidity Tax Is Wallet-Based

The liquidity tax sends tokens to a wallet rather than automatically adding liquidity.

Impact:
Transparency concern (not a security vulnerability).

Recommendation:
Clearly disclose this as a treasury wallet or implement auto-liquidity.

🔴 HIGH RISK (CENTRALIZATION / TRUST)

3. Owner Minting Privilege

The owner can mint additional tokens up to the hard cap.

Impact:
Potential dilution risk.

Recommendation:
Disable minting permanently or renounce ownership after minting phase.

4. Owner Control Permissions

The owner can:

- Exclude addresses from tax and limits
- Change wallet addresses
- Rescue ERC-20 tokens sent to the contract

Impact:
Centralization risk (not a bug).

Recommendation:
Use a timelock or renounce ownership post-launch.

📊 RISK SUMMARY

Category	Status
Critical Vulnerabilities	None
Medium Risks	2
High Risks (Trust)	2
Overall Security	Stable

🛡️ FINAL ASSESSMENT

The SALZJYUR (SZUR) smart contract demonstrates **no critical security vulnerabilities**.
Primary risks relate to **owner privileges and centralization**, which should be transparently disclosed to users and investors.
