HasLock Penetration Assessment

$STONKBROKER ERC-20

Adversarial assessment of the $STONKBROKER ERC-20 only. Performed under HasLock by Admir Zlatic (0xSimpleFarmer), Hashlock SSCAC certified. Not a public bug bounty; not a Hashlock firm engagement report.

Report date	2026-08-25
Target	0xe934e36a439c94017b64a3fece66af12099abf50
Scope	ERC-20 CollectionToken only
Public bug bounty	None at time of report
Result	PASS · no exploitable findings
Auditor	Admir Zlatic (0xSimpleFarmer)
Role	Head of DeFi at ApeCoin; founder, Clutch Markets
Grants	Polymarket grant winner; Arbitrum grant recipient
Credential	Hashlock Solidity Smart Contract Auditor Certification (SSCAC)
Credential date	February 3, 2026
Credential ID	admir.zlatic (certificate on file)
Program mark	HasLock Certified (StonkBrokers in-house)

Credential vs engagement

The auditor holds Hashlock's SSCAC individual certification. This report is a HasLock (StonkBrokers) review performed by that certified auditor. It is not a Hashlock firm engagement letter or firm-signed audit of this token unless a separate Hashlock engagement report is attached.

1. Objective

Identify exploitable weaknesses allowing unauthorized minting, transfer restriction abuse, balance freeze, fee extraction, upgrade takeover, or other privileged control over third-party balances.

2. Attack surface

- Constructor mint path and initialHolder assignment.
- Absence of Ownable / AccessControl / roles.
- Absence of pause, blacklist, freeze, and seize functions.
- ERC20Burnable for forced-burn of other users (not present; burn is self-only).
- ERC20Permit domain separator / replay expectations (standard OZ).
- Proxy / UUPS / Transparent upgrade patterns (not used).
- Hidden fee-on-transfer or callback hooks (none beyond ERC-20).

3. Probe results

- Privilege escalation to mint: not possible (no mint after construct; no owner).
- Pause or block transfers for others: not possible.
- Upgrade implementation: not possible (no proxy).
- Extract fees on transfer: not possible.
- Burn arbitrary third-party balance via admin: not possible.

4. Results

No exploitable findings

No Critical, High, Medium, or Low severity issues were identified. No severity remediations are outstanding.

5. Bug bounty status

There is no public bug bounty specifically for the $STONKBROKER ERC-20 at the time of this report. This HasLock assessment is an internal adversarial review by a Hashlock SSCAC-certified auditor. Responsible disclosure: Clutch Markets official channels.

6. Assessor attestation

I, Admir Zlatic (0xSimpleFarmer), Hashlock SSCAC certified (February 3, 2026), attest that I performed this HasLock penetration assessment of the $STONKBROKER ERC-20 identified above and that no exploitable findings were identified as of the report date.

Date	2026-08-25