

Verified by Sigillum **sig_1085e13fcd15**

Persisted Sigillum receipt for a real paid inspection and agent decision.

Proof Summary

Sigillum Risk Score: 43

Recommendation: BLOCK

Paid Amount: 0.000043 USDC

Decision: stop merge

Timestamp: Jul 4, 2026, 4:54 PM

Receipt Details

Action ID: act_d5f6bf0bf13f

Agent: ExternalCodeChangeAgent

Action Type: code_change

Rail: x402

Network: Arc testnet

Payment Reference: 9a175b83-8849-40dc-aec5-1d048c12a962

Transaction Hash:

0x0ecf123defd8d641e2c47fe3175c52f3c60c55ea3fecdc79b9866e06bd39db2

Receipt Hash:

sha256:4366a52ff05af3b224523f983a86028eb4bf8db7e1afa51886ce0920470e9356

Settlement Status: completed

Settlement Scope: individual

Settlement Source: gateway transfer payload

Batch Reference: Unavailable

Transaction Confirmed: Jul 4, 2026, 4:58 PM

Inspected Units

Changed Lines: 4

AST Nodes: 8

Dependency Changes: 0

Config Mutations: 0

Strings: 1

Agent Decision

Decision: stop_merge

Policy Matched: block_on.secret_exposure

Next Action: remove_secret_and_regenerate_patch

Reason: Critical secret exposure detected in the diff.

Patch Recommendation

Remove the exposed secret, rotate the credential, and regenerate the patch.

Findings

1. [CRITICAL] secret_exposure

Potential secret value is present in a sample environment file.

Location: src/example.ts:2

2. [INFO] syntax_structure_signal

Mixed code, config, and markdown surfaces parsed cleanly enough to produce bounded inspection signals.