E13. Development-application configuration analysis

Ilja Krasnjanski
24 October 2026 · Edited evidence report
Historical evidence through 24 July 2026; later engineering checks identified separately.

This report synthesizes the cited case records. Exhibits distinguish retained artifact excerpts from secondary analytical records and claims whose original inputs are unavailable. Excerpts may be redacted or reformatted; extraction methods and limitations are stated locally. Fingerprints identify inputs, not the truth of their claims. Bracketed S labels identify the analysis records listed at the end.

Source and method

The 24 July analysis used stored response bodies from a research-service capture of a development application dated 25 July 2025. The captured frontend exposed readable source and configuration constants. The principal page bundle is recorded as 32,043,726 bytes with SHA-256 `6fb9559f5706f45bf026eb449ada34706aa42399d3764d35e83d9675c666a66a`. No recovered service credential was used in the follow-up described by the record. [S1]

The deployed frontend response bodies and raw chain-query responses are not retained among these exhibit inputs. Their sizes, hashes and findings below are historical claims from the analysis note. The retained encrypted archive does not independently substantiate them.

Configuration identity

The deployed bundle and an encrypted environment archive are not proven byte-equivalent. Variable names differ between the example configuration and the captured frontend. Some values are source constants and an RPC value is a fallback used when a build-time value is absent. Reading those constants did not decrypt the archive or establish its contents. [S1]

The captured configuration points to a Solana development network and a local backend address. A commented alternative endpoint does not establish production use. Service keys, wallet identifiers and provider-specific access values are omitted from this report.

Recorded chain observations

The case record describes follow-up using a researcher-controlled service credential. It reports a development-network program with retained upgrade authority, a deployment on 31 May 2025 and an upgrade on 21 July 2025. The recorded funding of an authority shortly before deployment is consistent with a deployment sequence. It does not establish the person's identity. One funding source was interpreted as shared faucet infrastructure, limiting its attribution value. [S1]

An earlier empty response from a public RPC service was superseded by archival results. An empty result can therefore reflect retention or service coverage, rather than an inactive address. These observations are historical case results and were not repeated for this document.

Assessment and limits

This is evidence about a separate development application. It is not a recovered backend for the administration wallet console, does not identify that console's recipient addresses, and does not prove mainnet theft. Test-network balances are not victim-loss amounts. The source's stronger operator-control conclusions remain hypotheses requiring corroboration beyond constants and development-network transactions.

Exhibits

Exhibit E13-1. Retained encrypted environment archive

Artifact: HoldNow-env.rar · 486 bytes · SHA-256
`3ff402b45f3b8548841fcbeb2e5189b9d5373b838f0462195489288614b658ac`
Location: signature at byte 0; visible `.env` name at byte 46 (0x2e).
Extraction: read the file as bytes; report length, the first eight bytes in hexadecimal, and the offset returned by `data.find(b'.env')`.
Supports: archive identity and visible member-name bytes, not decrypted configuration contents.

```
bytes: 486
signature: 526172211a070100
.env name offset: 46 (0x2e)
```

The signature identifies RAR5. The historical examination describes an encrypted `.env` member. No member plaintext was recovered in this check. Credential-derived encryption fields are omitted.

Correction: unsupported configuration schema

The previous exhibit attributed six configuration variable names to the encrypted member. That attribution was unsupported: visible archive headers do not reveal an encrypted member's variable names or values. The schema has been removed. Reading constants from a separately captured frontend neither decrypts this archive nor proves equivalence to its contents.

Claims without a retained primary artifact

The following E13 statements rest on the analysis notes and on a urlscan capture of the deployed `hold.diobenu2silva[.]com` bundle that is **not retained in the workspace** (the cited `app/page.js`, 32,043,726 bytes, SHA-256 `6fb9559f5706f45bf026eb449ada34706aa42399d3764d35e83d9675c666a66a`, and `main-app.js` are referenced but absent). They therefore have no retained primary artifact here:

- The principal page bundle's byte size and SHA-256 (the bundle file is not in the workspace).
- The recovered configuration constants: the active Helius devnet RPC key, the commented-out QuickNode mainnet endpoint/token, the `holdnow` on-chain program ID, the backend/fee-destination wallet, the Pinata gateway host, and the `hxxp://localhost:2001` dev backend URL. (All such values would be [REDACTED] in any case: live third-party secrets, connection strings, or operator wallet identifiers.)
- The Solana devnet / local-backend endpoints and the commented alternative endpoint.
- The on-chain observations: program deployment 2025-05-31, upgrade 2025-07-21, retained upgrade authority, wallet balances/funding traces, and the shared-faucet attribution caveat — these are recorded case results from a researcher-controlled RPC query, not reproduced here and not backed by a retained raw artifact in the workspace.

Correction applied

The archived environment and the reported deployed frontend are not proven equivalent. No assertion about the sealed member's configuration schema is made here.

Exhibit inputs

Retained inputs identified by size and SHA-256. These include artifacts and analytical records; each exhibit identifies its evidence type and extraction limitations. The files themselves are not distributed.

Operator launchpad encrypted environment archive — HoldNow-env.rar (sealed .env member) · 486 bytes

`SHA-256 3ff402b45f3b8548841fcbeb2e5189b9d5373b838f0462195489288614b658ac`

Source records and fingerprints

SHA-256 identifies the reviewed source bytes, not acquisition time or every artifact described. Restricted originals are not reproduced.

[S1] Development-application configuration analysis, 24 July 2026 · 7,017 bytes

`SHA-256 cedfd268264c15eebe0ac58f552ecf252edc987fe898b0af70596fba251b7a78`