Security Audit Closure Sweep — 2026-06-27

Consolidated closure record. Cross-references the open/deferred findings across the corpus against current code (verified on the real filesystem) and formally closes everything that is resolved. Genuinely-open items are listed transparently and stay in the repo — nothing here is hidden, by design.

Co-authored by Sean McCormick and Claude (Anthropic). Smack Public License v2.0.

1. The load-bearing fix: CSRF is implemented site-wide

The single recurring open item across the early corpus was **"CSRF tokens missing — DEFERRED (HIGH)."** It is now fully resolved, site-wide, with no per-page opt-in:

- `core/csrf.php` — token generation/verification engine.
- `core/auth-smack.php` — runs `csrf_check()` automatically on every admin POST.
- `core/admin-footer.php` — auto-injects the hidden CSRF field into every `<form method="POST">`.
- `assets/js/ss-engine-admin-csrf.js` — sends the `X-CSRF-Token` header on AJAX.

This closes the deferred-CSRF line in **001, 002, 003, 005, 006, 007, 008** and the **UZ-04** CSRF item in the Unzucker audits (`smack-api-keys.php` includes `auth-smack.php` and never calls `csrf_exempt()`, so its key-gen/revoke handlers are auto-validated).

2. Repo-exposure verification (the "leak" that wasn't)

- **004 / SUYB Google service-account key** — never committed. `git log --all --full-history` for the key is empty; it is gitignored (`*-drive-key-*.json`).
- **Release signing private key (`smack-central/sc-config.php`)** — never in the repo. Only `sc-config.sample.php` is tracked.
- **DB passwords, forum mod key, GitHub PAT (028-C inventory)** — not in HEAD.

No secret was exposed via git. No rotation is forced by repository state. (Operational key rotation remains good hygiene but is not driven by a repo leak.)

3. CLOSED — formally resolved as of this record

Report	Finding(s)	Resolution
001	All Crit/High	Fixed by 0.7.23; CSRF item folded into §1
002, 003, 005, 006, 007, 008	CSRF (deferred HIGH)	§1 — CSRF live site-wide
009, 010, 011	All	Fixed/verified <= 0.7.152
012	install.php Step-5 POST guard	Raised in error (per 021A); guard present at install.php:1061
013	Admin-creation 2FA bypass	Fixed 0.7.157
014	Orphan login.php	Deleted 0.7.155; in UPDATER_DEPRECATED_FILES
015	2 Low	Fixed 0.7.159
016	F1–F3	Fixed 0.7.169 (mesh design note -> §5)
018, 019	All	Fixed/by-design <= 0.7.184
021, 021A	F4–F7	All closed in 021A (0.7.203)
022	sodium-skip gap	Fixed 0.7.214
024, 024A	UZ-11 caption XSS, UZ-04 CSRF, UZ-03/08	Fixed (escape-then-linkify sink) + §1
029	Auto-deletion primitive	Removed; detect-only

Report	Finding(s)	Resolution
son-of-a-batch	F1, F2, F4, F5	Remediated 2026-06-25 (owner-consent gate + reauth_verify + 300/hr budget + path guard)

4. SMALL-FIX — contained changes that close the stragglers

1. **027 Finding C / 0.7.209-S2** — `smackback-manifest.json` reachable in webroot. Add a deny rule to `core/htaccess-template` (currently absent). One block.
2. **008** — `assets/img/` PHP execution. Add `assets/img/.htaccess` with `php_flag engine off` (fcgid variant noted). Defence-in-depth.

These two are queued as the next commit; they close 027-C, 0.7.209-S2, and the 008 residual.

5. OPEN — logged transparently, remain in the public repo

Stays visible by design. None are exposed secrets; all are known work items.

- **mesh-roster F4** — tool API keys stored plaintext at rest and `tool_api_key` shown in the settings UI. Needs at-rest encryption (hub-replayed keys) + UI masking.
- **025-S1** — skin-wide JS sweep: AURORA + The Grid externalised, other skins not yet swept for direct `<script>`.
- **026 residuals** — dead constants templates in install.php; non-atomic constants.php rewrite in `core/updater.php` (~1271) should be temp+rename + EOF check.
- **0.7.209-S1** — `smack-central/sc-skins.php` writes no per-skin manifest (mirror the `sc-release.php` pattern).
- **028-C** (UNCONFIRMED, operational) — verify no historical `sc-config.php` was ever FTP'd to a public spoke. Inspected spoke (lightafterdark.ca) had only inert `sc-version.php`. Until each spoke's FTP/access logs are checked this stays open; if any spoke ever served `sc-config.php`, treat the signing key as compromised, rotate, and redeploy `release-pubkey.php` fleet-wide (0.7.313 self-heal lands it in one update).
- **020** — push-it hub_controls stale-lock-on-disconnect (Low).
- **017** — file-integrity re-init false-positive residual (warning-gated by design).

6. Knock-on: BUZZERS page

The 002–008 reports were held off the public BUZZERS page only because of the CSRF-deferred line. With §1 closed, that set is now publishable there. Optional follow-up.