SnapSmack Security Audit — 007

Date: 2026-05-03

Version scope: Alpha 0.7.22 → 0.7.39 (new and changed files)

Files audited: core/api-auth.php, probe-ban.php, privacy-policy.php, smack-privacy.php, smack-2fa.php, sybu-data.php, smack-cats.php, smack-albums.php, smack-collections.php

FINDINGS

FIXED — HIGH: DOM XSS in featured image picker (smack-cats.php, smack-albums.php, smack-collections.php)

Post titles and item names were inserted into `onclick` handler strings via concatenation. A title like `test',alert(1),'` could break the JS string literal and execute arbitrary JavaScript in the admin's browser.

Fix: Replaced all string-concatenation innerHTML patterns with `document.createElement()` / `dataset.*` / `addEventListener()`. No user-controlled data reaches HTML context via string building.

Files changed: smack-cats.php, smack-albums.php, smack-collections.php

CLEAN

core/api-auth.php — Parameterized queries, `hash_equals()` for timing-safe comparison, fail-closed. Clean.

probe-ban.php — Parameterized queries, safe IP extraction, no user input beyond IP header. Clean.

smack-2fa.php — `hash_equals()` for TOTP, recovery codes hashed, prepared statements throughout. Clean.

sybu-data.php — Parameterized queries, JSON output, no SQL interpolation. Clean.

DEFERRED / ACCEPTED RISK

privacy-policy.php raw HTML output

Admin-entered HTML rendered without escaping. Intentional design (admin needs rich text). Risk accepted: admin has full DB access; if the admin account is compromised the attacker can do far worse. Revisit if a non-admin role ever gains access to privacy policy editing.

CSRF tokens

SameSite=Lax mitigation in place. Full CSRF token implementation deferred (tracked from prior audit).

TOTP brute-force rate limiting

90-second window limits practical exposure. Low priority.

NOTES

Previous audits: 001 (2024-04-25), 002–006 (2026-04-25 to 2026-04-29).

Next audit recommended at 0.8.x (Closed Beta) or when new user-facing input handlers are added.