SnapSmack Security Audit — H

Date: 2026-05-05

Version scope: Alpha 0.7.43 → 0.7.45 (session-touched files)

Files audited: smack-globalvibe.php, smack-settings.php, smack-appearance-archive.php, smack-update.php, smack-menu.php, core/header.php, core/footer.php, core/meta.php, core/sidebar.php, smack-central/sc-release.php

FINDINGS

FIXED — MEDIUM: Masthead logo upload missing MIME validation (smack-globalvibe.php)

The `site_logo_file` upload handler (moved from smack-settings.php to smack-globalvibe.php this session) performed filename sanitization via `preg_replace` but did not validate the file's MIME type before calling `move_uploaded_file()`. A file named `evil.php` would have been saved as `{timestamp}_evil.php` in `assets/img/`, which has no `.htaccess` restricting PHP execution. An authenticated admin whose session was hijacked or whose browser was targeted by a CSRF attack could have used this to upload a web shell.

Context: The other two upload handlers in the same POST block (header logo, favicon) already used `finfo_file()` MIME validation. This handler was an oversight — the code was ported from smack-settings.php where the same gap existed.

Fix: Added `finfo_file()` MIME check and extension whitelist to match the other handlers. Upload only proceeds if both extension and MIME type are in the allowed image lists (`jpg, jpeg, png, gif, svg, webp`).

File: `smack-globalvibe.php` lines 145–163

CLEAN

sc-release.php preflight (key sync check)

New key sync check reads `core/release-pubkey.php`, compares to the derived pubkey from `sc-config.php`, emits an `['err', ...]` preflight entry on mismatch. Error text is passed through `htmlspecialchars()` at output. No user input reaches the preflight block — all strings are hardcoded or derived from controlled server config. Clean.

smack-update.php reapply fix

One-line `$stage_state = $_SESSION['update_state']` assignment. No new input paths introduced. CSRF token validated on all POST actions throughout the file. Clean.

smack-menu.php nav_menu_json

Raw JSON validated via `json_decode` before save; rejected on parse failure. Stored via prepared statement. In `core/header.php`, `$label` and `$url` both pass through `htmlspecialchars()` before echo. Dropdown appearance keys saved through a closed whitelist (`$dropdown_keys`). Clean.

smack-globalvibe.php settings save loop

INSERT … ON DUPLICATE KEY UPDATE via prepared statements throughout. No SQL interpolation. Mass-assignment risk (arbitrary keys accepted from POST) is structural and consistent with all other admin pages — admin authentication is the gate. Clean relative to baseline.

core/meta.php nav CSS vars

`nav_dropdown_bg` and `nav_dropdown_text` passed through `htmlspecialchars()` before output into `<style>` block. Both values originate from color picker inputs, not free-text fields. Clean.

core/header.php JSON nav renderer

`htmlspecialchars()` on label and URL before HTML output. `_snap_nav_resolve_url()` constructs URLs from whitelisted slug/type patterns; external URLs use `htmlspecialchars()`. Clean.

smack-settings.php $msg (line 203)

All assignments are hardcoded application strings ("Engine parameters updated successfully.", Akismet response strings). No user-controlled input reaches this variable. Clean.

File upload handlers — header logo, favicon

Both use `finfo_file()` MIME check + extension whitelist + `move_uploaded_file()`. Clean.

Authentication gate

All admin pages in scope open with `require_once 'core/auth.php'`. No gaps found.

DEFERRED / ACCEPTED RISK

---

assets/img/ has no .htaccess

No .htaccess restricts PHP execution in the image upload directory. With MIME validation now in place on all three upload handlers, the attack surface is narrow (finfo bypass or OS-level MIME spoofing). Recommended hardening: add `php_flag engine off` to `assets/img/.htaccess`. Deferred — server-specific; some hosts use fcgid and the syntax differs.

custom_css_public and footer_injection_scripts raw echo

Intentional admin-controlled injection. Accepted risk. Revisit if a non-admin editor role is ever introduced.

CSRF tokens

SameSite=Lax partial mitigation in place. Full token implementation deferred (HIGH severity, tracked separately).

Mass assignment in settings save loop

Any authenticated admin can POST settings[any_key] to insert arbitrary rows in snap_settings. Acceptable for single-admin installs. Revisit if role-based access is introduced.