[security] fix(sessions): validate session_id before deleting session files (#409) #412

Merged nesquena-hermes merged 3 commits into `master` from `pr-409-review` last week

Conversation 0 Commits 3 Checks 3 Files changed 4

nesquena-hermes commented last week — Collaborator

v0.50.32 — session_id path traversal fix [SECURITY]

Review of PR #409 by **@Hinotoi-agent**.

The vulnerability is real. `/api/session/delete` built the delete target as `SESSION_DIR / f"{sid}.json"` from untrusted input. Pathlib discards the prefix when `sid` is an absolute path, so `{"session_id": "/tmp/victim"}` caused `unlink()` to run on `/tmp/victim.json` outside the session store. Traversal-style values also worked. CVSS 8.1 High.

What changed vs. the original PR:

- Branch was 4 commits behind master (cherry-picked cleanly onto master)
- Removed a redundant `SESSION_INDEX_FILE.unlink()` that the PR added before the path validation check — it ran even on rejected requests and nuked the index cache unnecessarily. Moved to only fire on the success path (where it already existed)
- Otherwise the fix is taken as-is: allowlist validation + resolved-path containment

Fix in one sentence: `session_id` is now validated against `[0-9a-z_]+` (covers all real ID formats) and the resolved path must pass `path.relative_to(SESSION_DIR)` containment before `unlink()` runs.

Tests: 3 security regression tests pass, full suite 1041/0.

Closes #409.

Hinotoi-agent and others added 3 commits last week

 `fix(sessions): validate session_id before deleting files` `da0a2d1`

 `fix: remove premature session index invalidation before validation check` `8becbab`

 `docs: v0.50.32 release — version badge and CHANGELOG` ✕ `6513b68`

 **nesquena-hermes** merged commit **3cc5839** into `master` last week

0 of 3 checks passed

View details

 **nesquena-hermes** deleted the `pr-409-review` branch last week

Sign up for free **to join this conversation on GitHub**. Already have an account? Sign in to comment

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants