Fix #1612 Refactor upload route to include session validation and improve error… #1611

Merged Anchel123 merged 1 commit into `staging` from `fix-upload-route` yesterday

Conversation 13 Commits 1 Checks 17 Files changed 1

Anchel123 commented 2 days ago • edited by coderabbitai bot — Contributor

… handling

Summary by CodeRabbit

- **Bug Fixes**
  - Upload endpoint now requires user authentication
  - Improved error handling with more descriptive messages
  - Enhanced file path validation to prevent invalid file operations
  - Consistent CORS header handling across all response scenarios
  - Better file processing and storage handling

`Refactor upload route to include session validation and improve error…` ✓ `5345b4e`

…

overcut-ai bot commented 2 days ago • edited

Completed Working on "Code Review"

✅ Review publishing complete. Posted comments from all chunks and submitted final review as COMMENT. Total comments: 3 across 1 files.

✅ Workflow completed successfully.

👉 View complete log

vercel bot commented 2 days ago • edited

The latest updates on your projects. Learn more about Vercel for GitHub.

Project	Deployment	Actions	Updated (UTC)
falkordb-browser	Ready	Preview, Comment	Apr 8, 2026 5:16pm

Review with Vercel Agent

Anchel123 requested a review from **gkorland** 2 days ago

coderabbitai bot commented 2 days ago • edited Contributor

Walkthrough

Modified the file upload endpoint to add session-based authentication, path traversal validation, and improved error handling. Restructured control flow with outer try/catch wrapper, filename sanitization via `path.basename()`, and verification that resolved file paths remain within the assets directory.

Changes

Cohort / File(s)	Summary
File Upload Security & Error Handling `app/api/upload/route.ts`	Added `getClient()` authentication check at handler entry; implemented path traversal guard verifying resolved `filePath` starts within `assetsDir`; restructured with outer try/catch for session/upload failures; improved filename handling with `path.basename()` and updated file path construction; preserved CORS headers across all response paths.

Estimated code review effort

🎯 4 (Complex) | ⏱️ ~45 minutes

Poem

> 🛡️ A guardian at the gate now stands,
> Checking tokens before files touch the lands,
> Path traversal schemes meet their match,
> Each `basename()` a careful catch,
> Errors wrapped, responses secured with care—
> Upload safety now thrives everywhere! ✨

▶ 📟 Pre-merge checks | ✅ 3

▶ ✨ Finishing Touches

> ⚠ Warning
>
> ## Review ran into problems
>
> ▶ 🔥 Problems

Thanks for using CodeRabbit! It's free for OSS, and your support helps us grow. If you like it, consider giving us a shout-out.

▶ ❤️ Share

Comment `@coderabbitai help` to get the list of available commands and usage tips.

vercel bot deployed to **Preview** 2 days ago — View deployment

overcut-ai bot reviewed 2 days ago

View reviewed changes

overcut-ai bot left a comment

Review Summary

Findings by importance

- BLOCKER: 0
- CRITICAL: 0
- MAJOR: 3

- MINOR: 0
- SUGGESTION: 0
- PRAISE: 0

Scope impact

- Total comments: 3
- Affected files: 1 (`app/api/upload/route.ts`)
- Blocking issues: none at blocker/critical level

Key themes

1. Response handling consistency: unauthorized path may bypass expected CORS behavior.
2. Error semantics: server-side write/I/O failures are currently returned as client errors.
3. Security hardening: raw internal error messages are exposed in API responses.

Actionable next steps

1. Ensure unauthorized responses include the same CORS headers as other upload responses.
2. Reclassify file write/stream failures to 5xx responses; keep 4xx for validation/input errors.
3. Replace client-facing raw exception messages with generic errors and keep detailed logging server-side.

`app/api/upload/route.ts` Show resolved

`app/api/upload/route.ts` Show resolved

`app/api/upload/route.ts` Show resolved

github-actions bot commented 2 days ago

🔒 Trivy Security Scan Results

```
Report Summary

┌──────────────────────────────────────────────────────────────────────────────┬────────────┐
│                                    Target                                    │    Type    │
│ Vulnerabilities │
├──────────────────────────────────────────────────────────────────────────────┼────────────┤
│ falkordb/falkordb-browser:test (alpine 3.22.3)                               │   alpine   │
│        0        │
├──────────────────────────────────────────────────────────────────────────────┼────────────┤
│ app/node_modules/@falkordb/text-to-cypher/package.json                       │ node-
```

```
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@img/colour/package.json                                    │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@img/sharp-libvips-linux-x64/package.json                   │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@img/sharp-libvips-linuxmusl-x64/package.json               │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@img/sharp-linux-x64/package.json                           │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@img/sharp-linuxmusl-x64/package.json                       │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@js-temporal/polyfill/package.json                          │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@next/env/package.json                                      │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@redis/bloom/package.json                                   │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@redis/client/dist/package.json                             │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@redis/client/package.json                                  │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@redis/json/package.json                                    │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@redis/search/package.json                                  │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@redis/time-series/package.json                             │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/@swc/helpers/package.json                                   │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/client-only/package.json                                    │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/cluster-key-slot/package.json                               │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/detect-libc/package.json                                    │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
│ app/node_modules/falkordb/package.json                                       │ node-
pkg │        0        │
├──────────────────────────────────────────────────────────────────────────────┼──────────┤
```

```
| app/node_modules/jsbi/package.json                                    | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/lodash/package.json                                  | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/next/dist/compiled/@edge-runtime/cookies/package.json | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/next/dist/compiled/@edge-runtime/ponyfill/package.json | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/next/dist/compiled/@edge-runtime/primitives/package.json | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/next/dist/compiled/react-is/package.json             | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/next/dist/compiled/regenerator-runtime/package.json  | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/next/package.json                                    | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/react-dom/package.json                               | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/react/package.json                                   | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/redis/package.json                                   | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/semver/package.json                                  | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/sharp/package.json                                   | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/node_modules/styled-jsx/package.json                              | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| app/package.json                                                      | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| opt/yarn-v1.22.22/package.json                                        | node-
pkg |        0        |
├──────────────────────────────────────────────────────────────────────┼──────────┤
| usr/local/lib/node_modules/corepack/package.json                      | node-
pkg |        0        |
└──────────────────────────────────────────────────────────────────────┴──────────┘

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)
```

coderabbitai bot reviewed 2 days ago

View reviewed changes

coderabbitai bot left a comment — Contributor

Actionable comments posted: 4

▶ 🤖 Prompt for all review comments with AI agents

▶ 🪄 Autofix (Beta)

▶ ℹ️ Review info

`app/api/upload/route.ts` — Show resolved

`app/api/upload/route.ts` — Show resolved

`app/api/upload/route.ts` — Show resolved

`app/api/upload/route.ts` — Show resolved

Anchel123 linked an issue yesterday that may be closed by this pull request

security #1612 — Closed

Anchel123 changed the title **Refactor upload route to include session validation and improve error… Fix #1612Refactor upload route to include session validation and improve error…** yesterday

Anchel123 changed the title **Fix #1612Refactor upload route to include session validation and improve error… Fix #1612 Refactor upload route to include session validation and improve error…** yesterday

barakb approved these changes yesterday

View reviewed changes

Anchel123 merged commit **84de2d1** into `staging` yesterday

19 checks passed

View details

Anchel123 deleted the `fix-upload-route` branch yesterday

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

Reviewers

- **coderabbitai[bot]**
- **overcut-ai[bot]**
- **barakb**
- **gkorland**

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

security

2 participants