fix(security): Private Prompt Access Control Fixes #1104

Merged f merged 3 commits into `f:main` from `mdisec:fix-private-prompt-history`

2 weeks ago

mdisec commented 3 weeks ago • edited by coderabbitai bot — Contributor

Hi,

This PR fix 5 security vulnerability once for all. They all are almost identical and related with each other.

Production test: Use this prompt that is marked as private but versions etc is publicly accessible.

https://prompts.chat/api/prompts/cmn4mg8or0001l804tn74dqmr/versions

Overview

Multiple API endpoints and the prompt page metadata lacked `isPrivate` checks, allowing unauthorized users to access data belonging to private prompts. All fixes enforce a consistent policy: **if a prompt is private, only the owner and admins can access its associated resources.**

Fixed Endpoints

1. GET /api/prompts/[id]/versions — Version History Leak

File: `src/app/api/prompts/[id]/versions/route.ts`

Issue: No privacy check. Anyone could list all version history (content + author) of a private prompt.

Fix: Added `isPrivate` + `authorId` lookup before querying versions. Returns 403 for unauthorized users.

---

2. GET /api/prompts/[id]/changes — Change Request List Leak

File: `src/app/api/prompts/[id]/changes/route.ts`

Issue: No privacy check. Anyone could list all change requests (including `originalContent` and `originalTitle`) for a private prompt.

Fix: Added prompt privacy lookup. Returns 403 for unauthorized users.

---

3. GET /api/prompts/[id]/changes/[changeId] — Change Request Detail + Current Content Leak

File: `src/app/api/prompts/[id]/changes/[changeId]/route.ts`

Issue: No privacy check. The query included `prompt.content`, leaking the **current live content** of a private prompt to anyone with a change request ID.

Fix:

- Replaced `content` with `isPrivate` and `authorId` in the prompt select (stops current-content leak).
- Added privacy gate. Returns 403 for unauthorized users.

---

4. GET /api/prompts/[id]/examples — Examples Leak

File: `src/app/api/prompts/[id]/examples/route.ts`

Issue: No privacy check. Anyone could enumerate user-submitted examples (with user info) for private prompts.

Fix: Added `isPrivate` + `authorId` to the existing prompt query. Returns 404 for unauthorized users (no oracle).

---

5. POST & DELETE /api/prompts/[id]/vote — Vote Oracle + State Mutation

File: `src/app/api/prompts/[id]/vote/route.ts`

Issue: No privacy check on either handler. Any authenticated user could vote/unvote on private prompts and use differential responses (404 vs "already voted" vs success) as an existence oracle.

Fix:

- **POST:** Added `isPrivate` + `authorId` to existing prompt query. Returns 404 for unauthorized users.
- **DELETE:** Added prompt privacy lookup. Returns 404 for unauthorized users.

Both return 404 (not 403) to prevent information leakage about prompt existence.

---

6. generateMetadata — Title/Description Leak via HTML Meta Tags

File: `src/app/prompts/[id]/page.tsx`

Issue: `generateMetadata` fetched and rendered `title` and `description` for private prompts in `<title>` and `<meta description>` tags, even though the page body correctly called `notFound()`.

Fix: Added `isPrivate` to the select. Returns generic "Prompt Not Found" metadata when the prompt is private.

Summary by CodeRabbit

- **New Features**
  - Enforced prompt privacy across pages and APIs: private prompts are viewable only by owners and admins.
  - Unauthorized requests for private prompts now receive a "not found" response.
  - Privacy checks applied consistently to prompt versions, examples, change requests, voting, and page metadata.
- **Tests**
  - Added tests covering visibility and access responses for public and private prompts.

coderabbitai bot commented 3 weeks ago • edited

▶ 📝 Walkthrough

▶ 🚥 Pre-merge checks | ✅ 2 | ❌ 1

▶ ✨ Finishing Touches

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.

`fix unit tests` ✓ `20c6c26`

coderabbitai bot reviewed 3 weeks ago

View reviewed changes

coderabbitai bot left a comment

> **Caution**
>
> Some comments are outside the diff and can’t be posted inline due to platform limitations.
>
> ▶ ⚠️ Outside diff range comments (1)

▶ 🧹 Nitpick comments (1)

▶ 🤖 Prompt for all review comments with AI agents

▶ ℹ️ Review info

`fix the prompt view perm issue for admin and adding unit tests` ✓ `d887c49`

coderabbitai bot reviewed 3 weeks ago

View reviewed changes

coderabbitai bot left a comment

Actionable comments posted: 1

▶ 🤖 Prompt for all review comments with AI agents

▶ ℹ️ Review info

`src/__tests__/lib/prompt-access.test.ts`

```
88 +   });
89 +
90 +   it("should return 404 for private prompt when user is not owner", asyn
91 +     vi.mocked(auth).mockResolvedValue({ user: { id: "other", role: "USER
```

coderabbitai bot 3 weeks ago

⚠️ *Potential issue* | 🟡 *Minor*

▶ 🧩 Analysis chain

Replace `as never` casts with properly typed session fixtures.

The `as never` casts on lines 91, 98, and 104 bypass TypeScript's strict type checking and mask incomplete mock objects. Replace these with typed fixtures using `satisfies Session`.

However, the Session interface (augmented in `src/lib/auth/index.ts`) requires these fields: `id`, `email`, `username`, `locale`, `role`, and optionally `name` and `image`. The current fixtures are missing required fields. Create complete fixtures that satisfy the full Session contract:

▶ Corrected refactor

Also applies to: 98-98, 104-104

▶ 🤖 Prompt for AI Agents

f merged commit `233858f` into `f:main` 2 weeks ago

3 checks passed

View details

Reviewers

coderabbitai[bot]

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