Document Management System (DMS)
Backend — Technical Test Evidence

Mandatory Test Scenarios Evidence (REPLACE • Notifications • DELETE)

Author: Ichsan Saputra

Date: 17 Feb 2026 (UTC)

Repository: dms-backend-cybermax-v6

Contents

1. REPLACE Workflow Evidence

Scenario: a USER requests a document replacement. The system creates a permission request, locks the document (PENDING_REPLACE), and waits for an ADMIN to approve. After approval, the document is updated transactionally (fileUrl + version increment) and the user receives a notification.

1.1 Initial Upload (baseline document state)
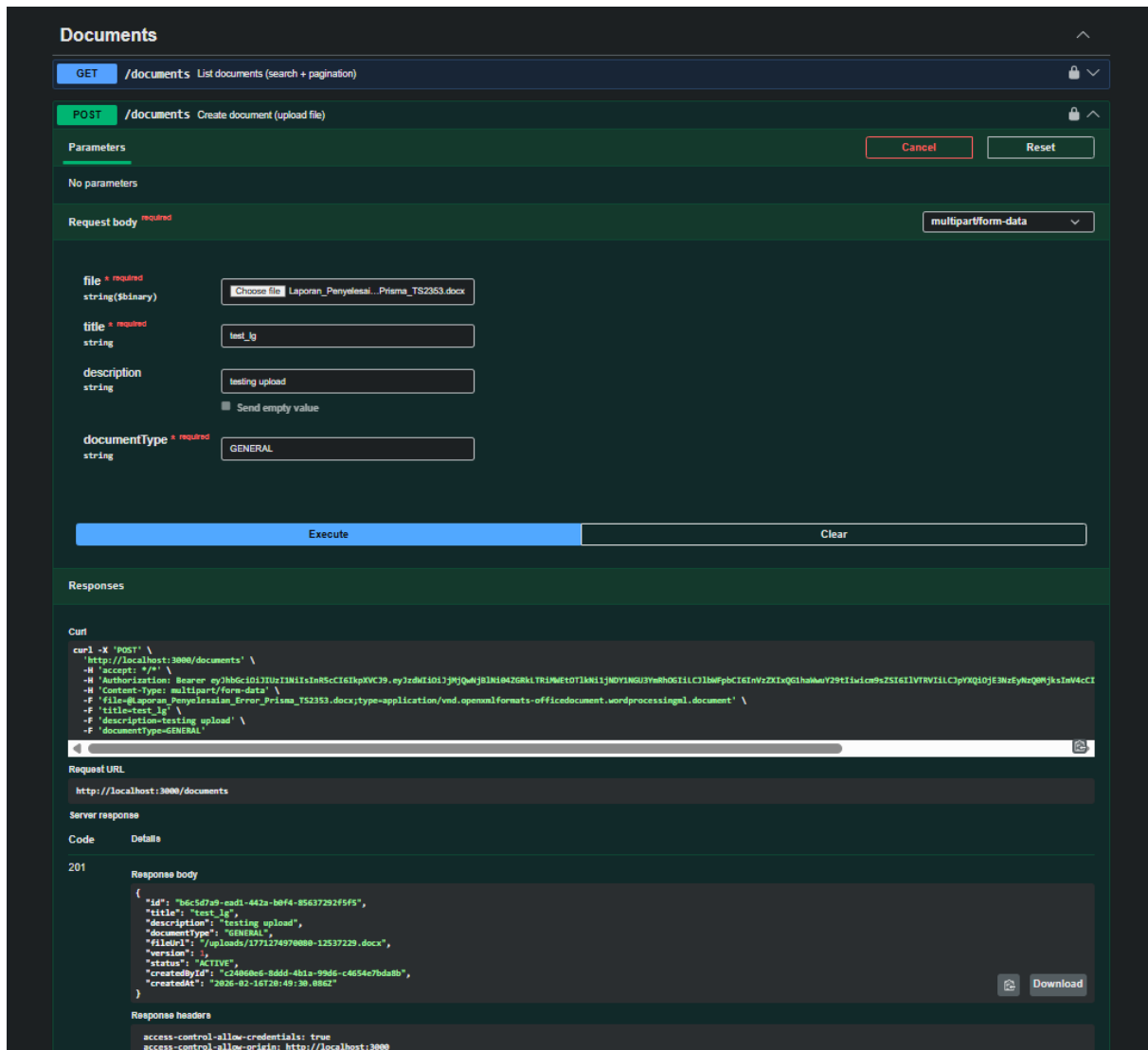

Figure 1 — Create document (upload) succeeded (HTTP 201).

1.2 USER creates REPLACE request
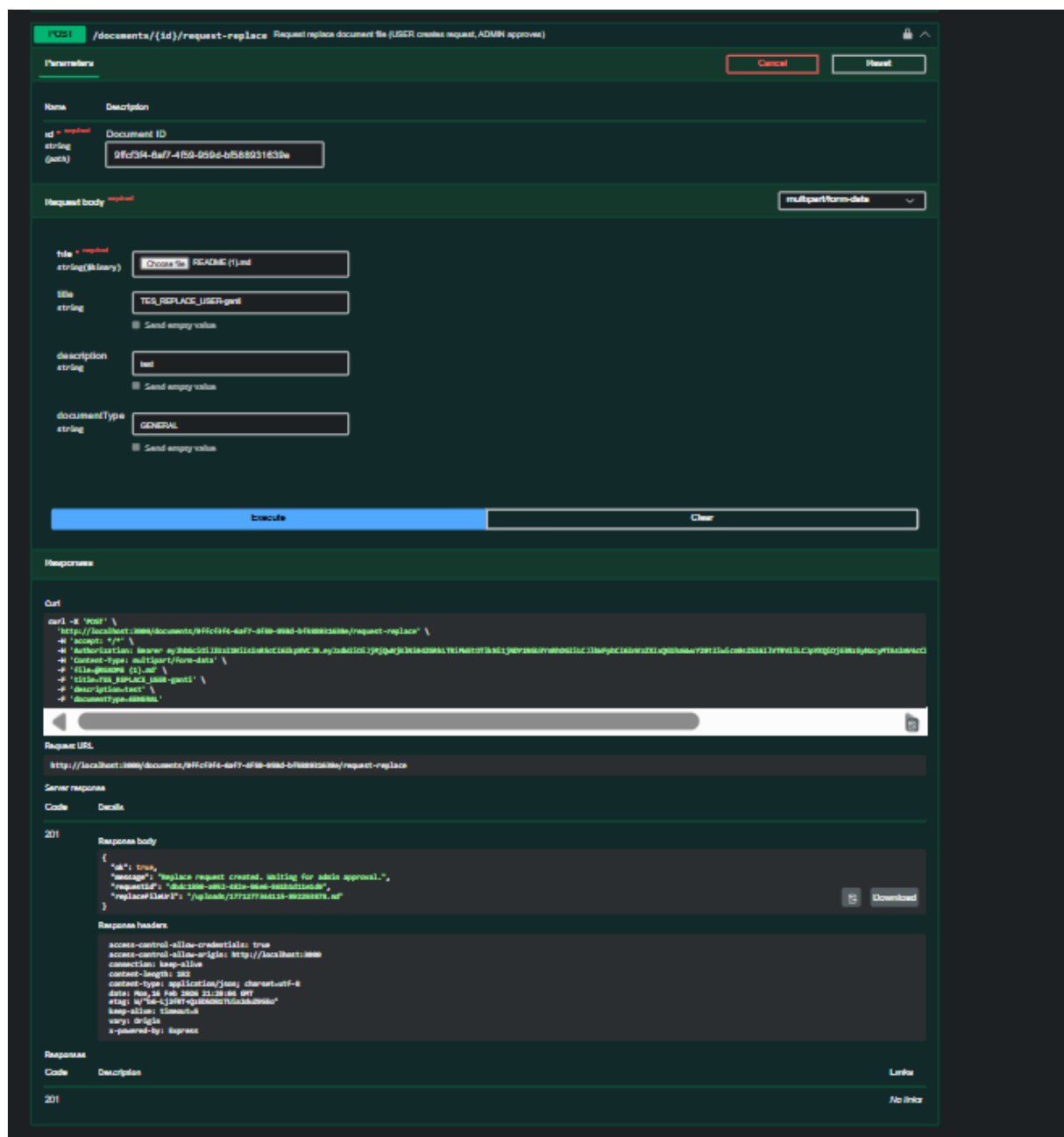
Figure 2 — USER calls /documents/{id}/request-replace (HTTP 201), request created and waiting for admin approval.

1.3 ADMIN sees pending request

Figure 3 — ADMIN calls /approvals/requests and sees the REPLACE request with status PENDING.
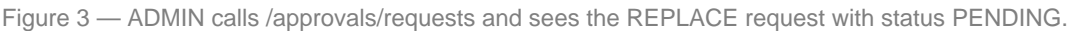
1.4 ADMIN approves REPLACE request

Figure 4 — ADMIN approves via /approvals/requests/{id}/approve (HTTP 201).

1.5 Verification after approval (document updated)

Verification points: (1) status returns to ACTIVE, (2) version increments, (3) fileUrl changes to replacement file.

Documents

GET /documents List documents (search + pagination)

Parameters   Cancel

Name   Description

q   Search query (title/description/type)
string
(query)   [q]

page   [1]
string
(query)

limit   [10]
string
(query)

| Execute | Clear |

Responses

Curl

```
curl -X 'GET' \
  'http://localhost:3000/documents?page=1&limit=10' \
  -H 'accept: */*' \
  -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...'
```

Request URL

```
http://localhost:3000/documents?page=1&limit=10
```

Server response

Code   Details

200   Response body

```
{
  "page": 1,
  "limit": 10,
  "total": 8,
  "totalPages": 1,
  "items": [
    {
      "id": "9ffcf3f4-6ef7-4f59-959d-bf588931630e",
      "title": "TES_REPLACE_USER-gxeti",
      "description": "text",
      "documentType": "GENERAL",
      "fileUrl": "/uploads/1771277344115-892283878.md",
      "version": 2,
      "status": "ACTIVE",
      "createdById": "c24060e6-8ddd-4b1a-99d6-c4654e7bda8b",
      "createdAt": "2026-02-16T21:23:00.718Z",
      "createdBy": {
        "id": "c24060e6-8ddd-4b1a-99d6-c4654e7bda8b",
        "email": "user3@mail.com",
        "role": "USER"
      }
    },
    {
      "id": "b6c5d7e0-aad1-442a-b0f4-85637292f5f5",
      "title": "TES_REPLACE_USER",
```

Response headers

```
access-control-allow-credentials: true
connection: keep-alive
content-length: 3198
content-type: application/json; charset=utf-8
date: Mon,16 Feb 2026 22:22:28 GMT
etag: W/"c7c-vNaNFQO4txCiivpUOPAbYEn7rkQ"
keep-alive: timeout=5
vary: Origin
x-powered-by: Express
```

Responses

Code   Description   Links

200   No links

Figure 5 — /documents list shows updated document (ACTIVE) with version increment and updated fileUrl.

2. Notification Verification (USER)

Scenario: after an ADMIN approves/rejects a permission request, a notification is created and can be retrieved by the corresponding USER.
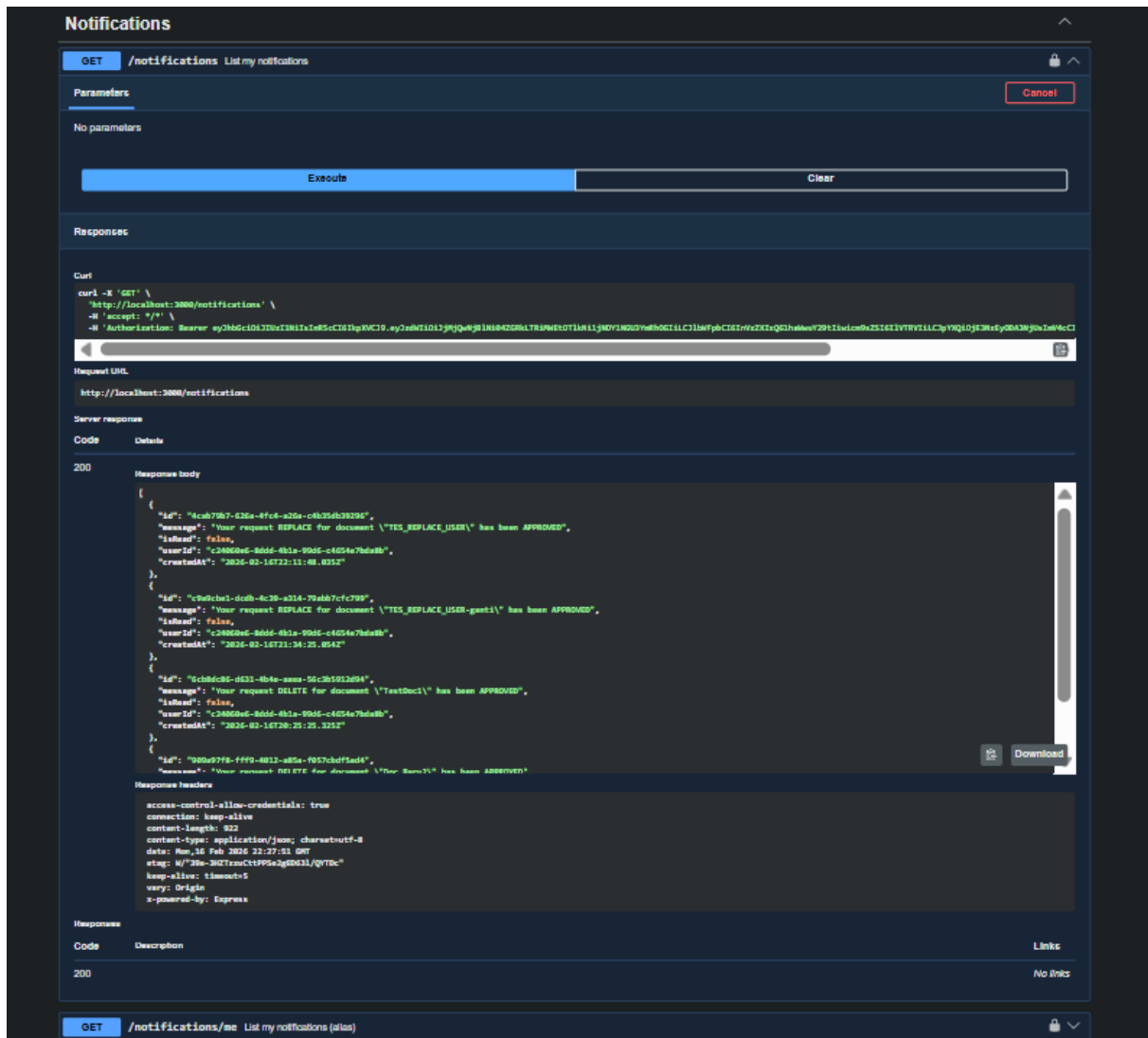

Figure 6 — USER calls /notifications and receives approval notifications (REPLACE and DELETE).

3. DELETE Workflow Evidence

Scenario: an ADMIN approves a DELETE permission request. The system deletes the document safely and notifies the user. The document should no longer be retrievable after deletion.

3.1 ADMIN approves DELETE request
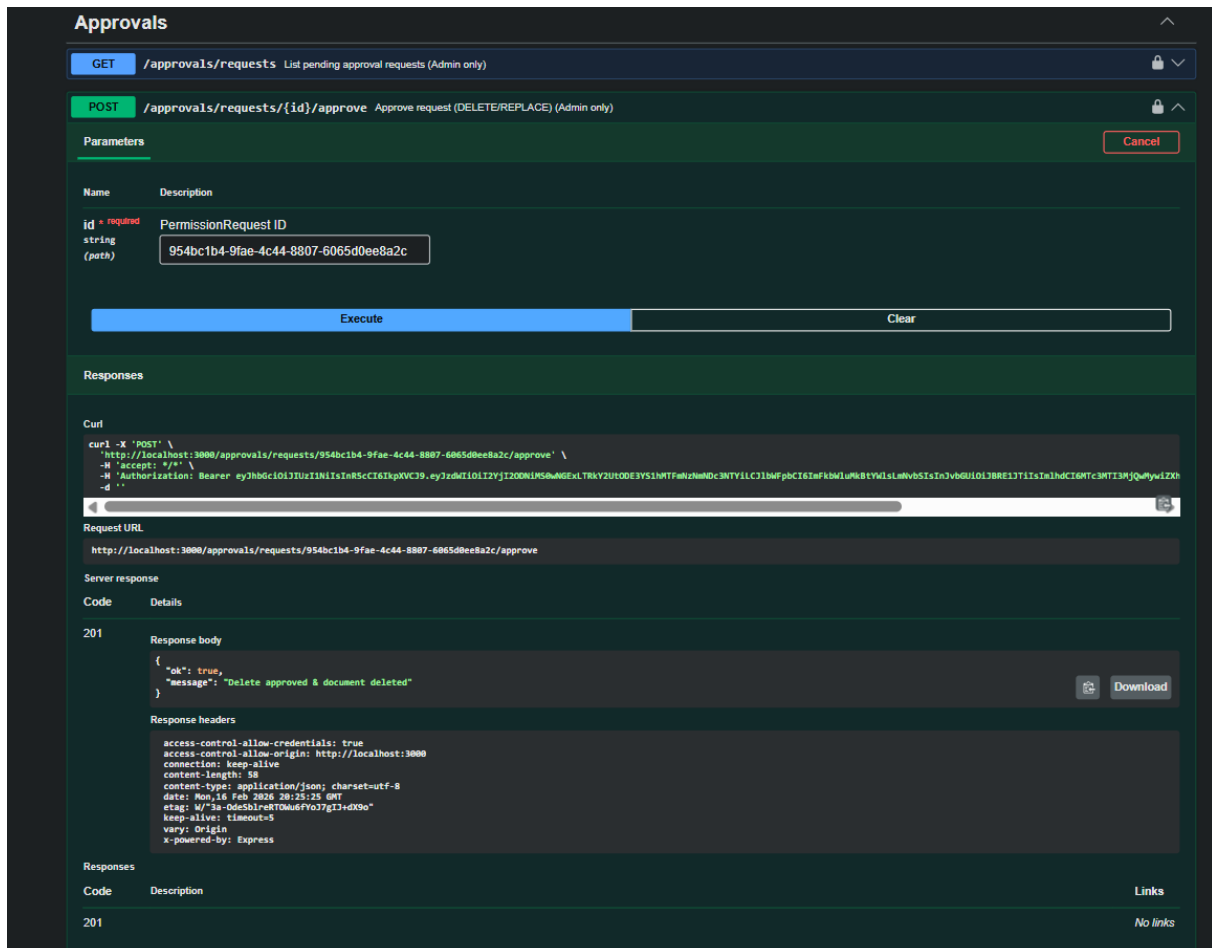
Figure 7 — ADMIN approves DELETE via /approvals/requests/{id}/approve (HTTP 201), document deleted.

3.2 Verification after deletion (document not found)

Figure 8 — Subsequent GET /documents/{id} returns 404 (Document not found), confirming deletion.

Appendix — RBAC / Security Checks (USER blocked)

To validate role-based access control, USER accounts must not be able to access ADMIN-only endpoints.
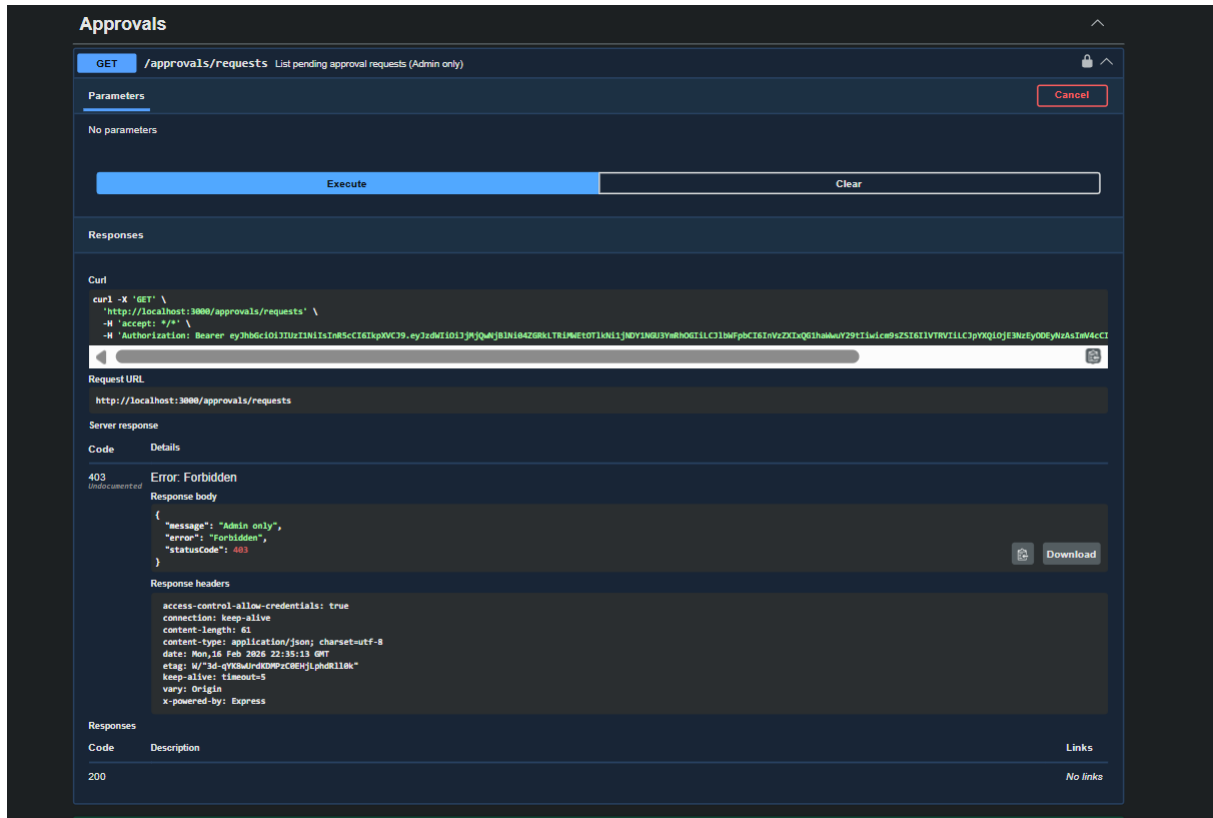

Figure A1 — USER calls /approvals/requests and gets 403 Forbidden (Admin only).

Figure A2 — USER calls /approvals/requests/{id}/approve and gets 403 Forbidden (Admin only).