

Module Security Checklist

Template tracking tiến độ hardening cho mỗi module.

Module: Authentication

| API Route | Meth-ods | handleE rrор | logger | guards | validat-or | Status | Ghi chú |
|--------------------|----------|--------------|--------|--------|------------|---------|---------------|
| /api/auth/login | POST | ✓ | ✓ | ✓ | ✓ | FULL | Done |
| /api/auth/register | POST | ✓ | ✓ | ✓ | ✓ | FULL | Done |
| /api/auth/logout | POST | ⚠ | ⚠ | ✓ | ✗ | PARTIAL | Cần logger |
| /api/auth/refresh | POST | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |
| /api/auth/me | GET | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |

Tổng kết Module:

- Tổng số routes: 15
- FULL: 2 (13%)
- PARTIAL: 3 (20%)
- BASIC: 10 (67%)
- Coverage: 13%

Ưu tiên tiếp theo:

1. /api/auth/refresh - CRITICAL (token security)
2. /api/auth/forgot-password - HIGH
3. /api/auth/reset-password - HIGH

Module: Submissions

| API Route | Meth-ods | handleE rrор | logger | guards | validat-or | Status | Ghi chú |
|-------------------------------|-------------------|--------------|--------|--------|------------|---------|----------------|
| /api/submis-sions | GET, POST | ✗ | ✗ | ✓ | ⚠ | PARTIAL | Cần log-ger |
| /api/submis-sions/[id] | GET, PUT, DE-LETE | ✗ | ✗ | ✓ | ✗ | BASIC | Cần harden-ing |
| /api/submis-sions/[id]/status | PATCH | ✗ | ✗ | ✓ | ✗ | BASIC | Cần harden-ing |
| /api/author/submis-sions | GET | ✗ | ✗ | ✓ | ✗ | BASIC | Cần harden-ing |

Tổng kết Module:

- Tổng số routes: 20
- FULL: 0 (0%)
- PARTIAL: 5 (25%)
- BASIC: 15 (75%)
- Coverage: 0%

Ưu tiên tiếp theo:

1. /api/submissions POST - CRITICAL (file upload)
2. /api/submissions/[id]/assign-reviewers - HIGH
3. /api/submissions/[id]/decision - HIGH

Module: Reviews

| API Route | Meth-ods | handleE rrор | logger | guards | validat-or | Status | Ghi chú |
|----------------------------|-----------|--------------|--------|--------|------------|--------|---------------|
| /api/reviews | GET, POST | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |
| /api/reviews/[id] | GET, PUT | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |
| /api/reviews/[id]/complete | POST | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |

Tổng kết Module:

- Tổng số routes: 10
- FULL: 0 (0%)
- PARTIAL: 2 (20%)
- BASIC: 8 (80%)
- Coverage: 0%

Ưu tiên tiếp theo:

1. /api/reviews POST - HIGH (review submission)
2. /api/reviews/[id]/complete - HIGH
3. /api/reviewer/match - MEDIUM

Module: Admin

| API Route | Methods | handleError | logger | guards | validator | Status | Ghi chú |
|----------------------------|---------|-------------|--------|--------|-----------|--------|---------------|
| /api/admin/users | GET | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |
| /api/admin/users/approve | POST | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |
| /api/admin/dashboard-stats | GET | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |

Tổng kết Module:

- Tổng số routes: 25
- FULL: 0 (0%)
- PARTIAL: 5 (20%)
- BASIC: 20 (80%)
- Coverage: 0%

Ưu tiên tiếp theo:

1. /api/admin/users/approve - CRITICAL
2. /api/admin/role-escalation - CRITICAL
3. /api/admin/users/toggle-active - HIGH

Module: Editor

| API Route | Methods | handleError | logger | guards | validator | Status | Ghi chú |
|-----------------------|---------|-------------|--------|--------|-----------|--------|---------------|
| /api/editor/dashboard | GET | ✗ | ✗ | ✓ | ✗ | BASIC | Cần hardening |

Tổng kết Module:

- Tổng số routes: 8
- FULL: 0 (0%)
- PARTIAL: 2 (25%)

- BASIC: 6 (75%)
 - Coverage: 0%
-

Cách sử dụng Checklist

1. Update sau mỗi lần hardening

```
# Chạy scan
yarn tsx scripts/diagnostics/security-scan.ts

# Cập nhật checklist dựa trên kết quả
```

2. Tracking tiến độ

- = Đã implement
- = Partial implementation
- = Chưa có

3. Priority

- CRITICAL: Auth, Admin, Submissions
- HIGH: Reviews, Editor, Users
- MEDIUM: Articles, Issues, Statistics
- LOW: Public routes, search

4. Status Definitions

- **FULL:** Tất cả 4 tiêu chuẩn (handleError, logger, guards, validator)
- **PARTIAL:** 2-3 tiêu chuẩn
- **BASIC:** Chỉ có guards hoặc try-catch
- **NONE:** Không có hardening

5. Workflow

1. Chọn module đang làm
 2. Chạy security-scan.ts
 3. Cập nhật checklist
 4. Hardening routes theo priority
 5. Test
 6. Commit
 7. Lặp lại cho module tiếp theo
-

Tổng kết Tất cả Modules

| Module | Total | FULL | PARTIAL | BASIC | Coverage |
|--------------|------------|----------|-----------|------------|-------------|
| Auth | 15 | 2 | 3 | 10 | 13% |
| Submissions | 20 | 0 | 5 | 15 | 0% |
| Reviews | 10 | 0 | 2 | 8 | 0% |
| Admin | 25 | 0 | 5 | 20 | 0% |
| Editor | 8 | 0 | 2 | 6 | 0% |
| Articles | 15 | 0 | 3 | 12 | 0% |
| Issues | 10 | 0 | 2 | 8 | 0% |
| Users | 12 | 0 | 2 | 10 | 0% |
| Other | 61 | 0 | 10 | 51 | 0% |
| TOTAL | 176 | 2 | 34 | 140 | 1.1% |

Target: 100% FULL coverage

Current: 1.1% FULL coverage

Next Milestone: 25% (Auth + Submissions modules)