**ANALISIS STUDI KASUS UAS - CIE406: Keamanan Informasi**

**Nama Mahasiswa**: Wahyu Cahya Bagus Pamungkas  
**NIM**: 20230801035  
**Mata Kuliah**: CIE406 - Keamanan Informasi  
**Dosen Pengampu**: Dr. Hani Dewi Ariessanti S.Kom, M.Kom  
**Studi Kasus**: Aplikasi Pendaftaran Seminar Online

**1. Deskripsi Umum Aplikasi**

Aplikasi ini dirancang untuk memudahkan mahasiswa dalam melakukan pendaftaran seminar secara online. Terdapat dua role utama yaitu **Admin** dan **User**. Admin dapat mengelola data seminar dan melihat peserta. User dapat melakukan registrasi akun, login, melihat daftar seminar, serta mendaftar seminar.

**2. Tujuan Keamanan Informasi**

Aplikasi ini dirancang dengan memperhatikan tiga pilar utama keamanan informasi:

* **Kerahasiaan (Confidentiality)**: Melindungi data pribadi pengguna seperti nama, NIM, email, dan nomor HP dari akses yang tidak sah.
* **Integritas (Integrity)**: Menjamin data yang disimpan tidak dimodifikasi secara ilegal atau tanpa izin.
* **Ketersediaan (Availability)**: Menjamin sistem tetap dapat diakses oleh pengguna yang berhak.

**3. Potensi Ancaman dan Solusi**

|  |  |
| --- | --- |
| **Ancaman** | **Solusi Pengamanan** |
| SQL Injection | Gunakan Query Builder/Eloquent ORM Laravel |
| Cross Site Scripting (XSS) | Escape output, validasi input, dan hindari HTML injection |
| Cross Site Request Forgery | Gunakan CSRF token default dari Laravel |
| Session Hijacking | Gunakan middleware auth, cookie secure, session timeout |
| Data Leakage (Sensitive Info) | Enkripsi password (bcrypt), hindari menampilkan .env, dll |
| Akses tidak sah (role abuse) | Gunakan middleware role-based access control (RBAC) |

**4. Struktur dan Alur Sistem**

**Entitas:**

* **User**: name, email, password, NIM
* **Admin**: name, email, password (dibuat dari seeder)
* **Seminar**: judul, deskripsi, tanggal, kuota
* **Pendaftaran**: user\_id, seminar\_id, waktu\_daftar

**Alur Umum:**

1. User melakukan signup & login
2. User melihat daftar seminar dan mendaftar
3. Admin login, kelola data seminar
4. Admin melihat daftar peserta per seminar

**5. Framework & Tools**

* **Laravel 12**: Backend development
* **Filament v3**: Dashboard admin berbasis panel otomatis
* **GitHub**: Version control dan tempat pengumpulan file

**6. Kesimpulan dan Rekomendasi Keamanan**

Berdasarkan analisis studi kasus dan pengujian keamanan pada aplikasi pendaftaran seminar online, ditemukan beberapa **kerentanan** yang dapat membahayakan keamanan informasi jika tidak ditangani dengan tepat. Kerentanan dan cara mitigasinya dijelaskan sebagai berikut:

A screenshot of a computer

AI-generated content may be incorrect.

**🔥 1. Session Cookie Tanpa Secure Flag**

**Kerentanan:**

* Cookie sesi dikirim tanpa Secure flag, yang membuatnya dapat disadap di koneksi HTTP.

**Solusi:**

* Aktifkan HTTPS dan atur konfigurasi di config/session.php:

php

SalinEdit

'secure' => env('SESSION\_SECURE\_COOKIE', true),

* Tambahkan di .env:

ini

SalinEdit

SESSION\_SECURE\_COOKIE=true

**⚠️ 2. Tidak Ada Pembatasan Akses Berdasarkan Role**

**Kerentanan:**

* User biasa bisa mengakses panel atau fitur admin jika tidak dilakukan pengecekan role.

**Solusi:**

* Tambahkan kolom role pada tabel users (admin, user).
* Gunakan middleware atau beforeCreate untuk validasi role:

php

SalinEdit

if (auth()->user()->role !== 'admin') {

abort(403);

}

**🛡️ 3. Data Pribadi Tidak Dilindungi Secara Menyeluruh**

**Kerentanan:**

* NIM, email, dan nomor HP rentan dibaca publik jika tidak dikontrol tampilannya.

**Solusi:**

* Gunakan ->visible() atau ->hidden() di Filament:

php

SalinEdit

->visible(fn () => auth()->user()->role === 'admin')

* Jangan tampilkan data pribadi di halaman terbuka.

**❗ 4. Input Tidak Divalidasi dengan Ketat**

**Kerentanan:**

* Input seperti deskripsi seminar atau pendaftaran tidak divalidasi maksimal, berpotensi menyebabkan **XSS** atau data tidak sah.

**Solusi:**

* Gunakan validasi Laravel/Filament:

php

SalinEdit

Textarea::make('deskripsi')->required()->maxLength(255)

**🧱 5. Formulir Rentan Cross-Site Request Forgery (CSRF)**

**Kerentanan:**

* Jika CSRF token tidak digunakan, user bisa menjadi target CSRF attack.

**Solusi:**

* Laravel sudah otomatis menyertakan token CSRF. Pastikan form Anda menggunakan @csrf atau memakai form builder Filament (yang sudah otomatis aman).

**🗃️ 6. Akses Tidak Terkontrol ke Data (Mass Assignment)**

**Kerentanan:**

* Field seperti user\_id, role, waktu\_daftar bisa diisi sembarangan jika tidak dilindungi.

**Solusi:**

* Pastikan di model hanya fillable field yang diperbolehkan:

php

SalinEdit

protected $fillable = ['seminar\_id', 'user\_id', 'waktu\_daftar'];

**🔐 7. Tidak Ada Enkripsi Data Sensitif**

**Kerentanan:**

* Meskipun password sudah terenkripsi (bcrypt), data lain seperti email atau NIM bisa disimpan dalam bentuk plain text.

**Solusi:**

* Simpan data sensitif hanya jika perlu.
* Gunakan enkripsi Laravel (opsional):

php

SalinEdit

encrypt($data);