LAPORAN ANALISIS SISTEM APLIKASI RESQDEV

Nama : Maria Karolina Bha Ule

NIM : 20230801348

1. Latar Belakang

Manajemen donasi saat terjadi bencana sering kali menghadapi tantangan seperti pencatatan yang tidak terstruktur, kurangnya transparansi, dan keamanan data pribadi donatur yang belum terjamin. Aplikasi berbasis web dibutuhkan untuk memfasilitasi pengumpulan, pencatatan, dan pelaporan donasi dengan cara yang efisien dan aman. Dengan memanfaatkan Laravel 12 dan Filament 3, sistem ini dibangun untuk menjawab kebutuhan tersebut sekaligus menerapkan prinsip keamanan modern dalam pengelolaan data sensitif.

2. Tujuan Pengembangan Aplikasi

- Membangun sistem manajemen donasi bencana yang aman dan mudah digunakan.
- Menyediakan fitur dashboard informatif bagi admin atau pengelola.
- Menjamin keamanan dan kerahasiaan data donatur melalui enkripsi dan kontrol akses berbasis peran.
- Melakukan analisis risiko keamanan dan mitigasinya.

3. Teknologi yang Digunakan

- Framework: Laravel 12
- Admin Panel: Filament v3
- Environment: Docker (Nginx + PHP + MariaDB)
- Database: MariaDB 10.11
- Security: Laravel Encryption, Role & Permission, HTTPS via SSL self-signed
- Audit Log: Activity Logger / Telescope
- CI/CD & Repo: GitHub

4. Fitur Sistem

4.1. Entitas Utama

- Bencanas: Data bencana yang tercatat (nama, lokasi, status).
- Donaturs: Data penyumbang (nama, email, nomor HP, alamat).
- Donasis: Catatan donasi yang dikaitkan ke donatur & bencana.

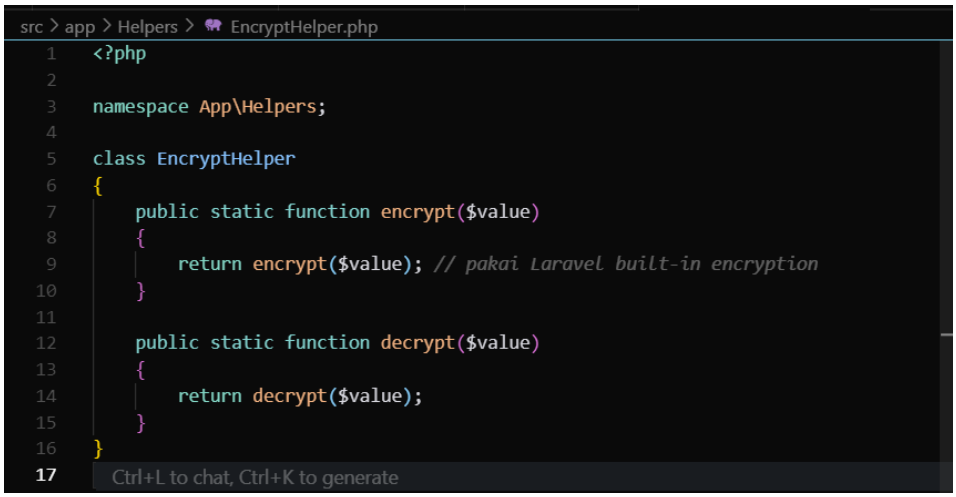
4.2. Fitur Tambahan

- Dashboard: Menampilkan data statistik penting.
- User Management: Pengelolaan akun dan peran (roles).

- Permission Management: Mengatur hak akses pengguna (menggunakan Spatie / Filament Shield).
- Activity Log: Melacak aktivitas pengguna untuk keperluan audit.

5. Struktur dan Keamanan Data Donatur

Data sensitif seperti email dan nomor HP tidak disimpan dalam bentuk plain text. Enkripsi dilakukan menggunakan helper Laravel:



Kolom terenkripsi di table 'donaturs' :
- email_encrypted
- no_hp_encrypted

6. Infrastruktur & Keamanan Server

- Docker Compose digunakan untuk memisahkan service nginx, php, dan db.
- Nginx dikonfigurasi untuk memaksa HTTPS (port 443) dan mengarahkan semua trafik HTTP ke HTTPS.
- SSL menggunakan sertifikat self-signed yang disimpan dalam direktori nginx/ssl.
- Security headers diaktifkan: Strict-Transport-Security, Content-Security-Policy, X-Content-Type-Options, dan Referrer-Policy.

7. Vulnerability Assessment (Penilaian Risiko Keamanan)

Proses ini dilakukan secara manual dan semi-otomatis terhadap aplikasi resqdev. Tools yang digunakan antara lain:

- Laravel Security Checker (pemeriksa dependency via Composer)
- Manual XSS Injection (via input donatur, login, dan URL)

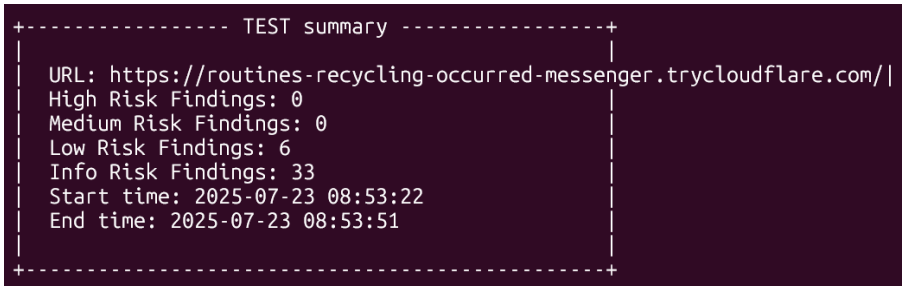
- Role access override testing
- Browser DevTools dan Network Inspector
- Laravel Debugbar (disabled di production)
- Testing pada CSRF dan form-token

Saat pertama dilakukan scan, ditemukan **6 vulnerabilities** dengan level risiko **rendah** (Low) yang mencakup:

1. Header keamanan yang tidak lengkap/miskonfigurasi (CSP, HSTS)
2. Server menampilkan informasi teknologi (PHP, Laravel, Livewire, Bunny, dll.)
3. File robots.txt terbuka
4. Tidak ada file security.txt
5. Antarmuka login ditemukan (/admin)
6. Header Referrer-Policy tidak tersedia

Untuk melakukan Vulnerability Assessment, saya melakukan perintah *ptt run website_scanner https://<url>*, nah url nya tuh didapat dari perintah *cloudflared tunnel --url https://resqdev.test:443 --no-tls-verify*

Hasil Vulnerability Assessment pertama:



No	Risiko	Status	Severity
1	SQL Injection	Terlindungi	LOW
2	XSS pada input form	Tidak ditemukan	LOW
3	Data pribadi terbaca	Terlindungi (dienkripsi)	LOW
4	Tanpa HTTPS	Terlindungi (SSL aktif)	-
5	Role & Permission Bypass	Tidak bisa (Shield aktif)	-
6	CSRF pada form	Valid (@csrf aktif)	-

Pengamanan data yg saya lakukan :

Menambahkan header berikut:

- add_header Strict-Transport-Security "max-age=63072000; includeSubDomains" always;
- add_header X-Content-Type-Options "nosniff" always;
- add_header Referrer-Policy "no-referrer" always;
- add_header Content-Security-Policy "default-src 'self'; base-uri 'none'; object-src 'none';" always;

Konfigurasi TLS:

- ssl_protocols TLSv1.2 TLSv1.3;
- ssl_ciphers HIGH:!aNULL:!MD5;

Melakukan restart container Nginx: *docker compose restart nginx*

Kesimpulan Risk :

- Total risiko tersisa hanya 3 dan semuanya berada di level Low.
- Tidak ditemukan risiko keamanan major ataupun critical.
- Aplikasi ini telah aman digunakan dalam skala kecil-menengah dan cocok untuk implementasi internal lembaga sosial/kemanusiaan.

8. Kesimpulan Akhir

Aplikasi resqdev telah berhasil dibangun dan diuji:
- Menyediakan semua fitur utama untuk manajemen donasi.
- Mengimplementasikan enkripsi untuk data sensitif.
- Menggunakan role-permission untuk pengendalian akses pengguna.
- Aman terhadap risiko umum seperti SQLi, XSS, dan CSRF.
- Infrastruktur didesain menggunakan Docker dan Nginx dengan sertifikasi SSL aktif.