

## **BAB I**

### **PENDAHULUAN**

#### **1.1. Gambaran Umum**

Pertumbuhan ekosistem kerelawanan di Indonesia menunjukkan tren yang sangat positif, dilandasi oleh kuatnya budaya kederewanan di tengah masyarakat. Fenomena ini tercermin pada skala platform digital utama seperti Indorelawan, yang telah berhasil menghimpun partisipasi lebih dari 250.000 relawan dan 5.000 organisasi [1]. Motor penggerak utama dari gelombang partisipasi sosial ini adalah generasi muda. Sebuah survei menegaskan bahwa 88,6% dari total relawan berada di rentang usia produktif 18-30 tahun, dengan mahasiswa sebagai kelompok mayoritas [2]. Apabila diproyeksikan terhadap total populasi pemuda Indonesia yang mencapai 64,22 juta jiwa, terlihat adanya potensi sumber daya manusia yang luar biasa besar untuk berbagai aksi sosial [3]. Akan tetapi, potensi masif ini belum dapat teroptimalkan sepenuhnya karena terhalang oleh kendala fundamental, yaitu adanya diskoneksi informasi dan inefisiensi dalam proses yang ada.

Diskoneksi tersebut berdampak pada dua pemangku kepentingan utama. Bagi para calon relawan, tantangan utamanya adalah kesulitan dalam mengakses informasi kegiatan yang terverifikasi dan sesuai minat, lantaran sumber informasi yang ada bersifat fragmentaris dan tersebar di berbagai kanal media sosial [4]. Sebaliknya, para penyelenggara kegiatan sosial juga menghadapi kendala dalam menemukan dan merekrut relawan yang memiliki kompetensi serta komitmen yang dibutuhkan [5], [6]. Urgensi permasalahan ini telah menjadi perhatian luas di tingkat nasional, yang dibuktikan dengan adanya inisiatif "Riset Kerelawanan 2024" oleh Indorelawan dan Australian Volunteers Program untuk memetakan tantangan tersebut secara komprehensif [7]. Lebih lanjut, ketergantungan pada metode rekrutmen konvensional menciptakan kerentanan terhadap modus penipuan berkedok acara sosial (*event scam*). Terdokumentasinya kasus-kasus semacam ini pada akhirnya berpotensi mengikis kepercayaan publik terhadap ekosistem kerelawanan [8], [9].

Sebagai respons terhadap serangkaian tantangan tersebut, dirancanglah sebuah solusi berupa platform digital berbasis web bernama Volunteerin.id (<https://volunteerin.id>). Secara definitif, Volunteerin.id adalah sebuah ekosistem digital terintegrasi yang berfungsi sebagai jembatan antara relawan dengan penyelenggara kegiatan kerelawanan. Platform ini diposisikan sebagai mediator digital yang bertujuan untuk membangun koneksi yang lebih efisien, transparan, dan aman antara pencari dan penyedia kesempatan kerelawanan di Indonesia.

Tampilan antarmuka halaman utama platform, yang dapat dilihat pada Gambar 1.1, dirancang sebagai portal terpusat. Melalui halaman ini, pengguna dapat secara efisien melakukan pencarian dan penyaringan berbagai kegiatan berdasarkan kategori, seperti Sosial, Pendidikan, dan Lingkungan. Dengan menyediakan ekosistem terpusat yang didukung oleh fitur-fitur inovatif inilah, Volunteerin.id berupaya memitigasi inefisiensi dan masalah fragmentasi informasi yang selama ini terjadi dalam proses mobilisasi dan manajemen potensi relawan.



Gambar 1.1. Platform Volunteerin.id

Sebagai bentuk validasi awal terhadap konsep dan kelayakan teknisnya, pengembangan platform ini diikuti sertakan dalam berbagai kompetisi tingkat nasional. Hasilnya, Volunteerin berhasil meraih sejumlah pengakuan. Pertama, platform ini meraih Juara 1 dalam kompetisi Hackathon ITFEST 5.0 2025 yang

diselenggarakan oleh Universitas Paramadina Jakarta. Ajang tersebut menantang kemampuan pemrograman dan inovasi peserta untuk mengembangkan solusi perangkat lunak fungsional yang berkontribusi pada Sustainable Development Goals (SDGs) [10]. Kedua, Volunteerin meraih Juara 3 pada kompetisi Business Plan GENETIC 2025 di Universitas Semarang. Kompetisi ini berfokus pada perancangan model bisnis berbasis teknologi yang inovatif dan berkelanjutan. Pencapaian ini merupakan validasi eksternal yang kuat terhadap urgensi masalah yang diangkat serta relevansi solusi yang ditawarkan oleh platform, baik dari sisi kelayakan teknis maupun keberlanjutan bisnis [11]. Pencapaian ini merupakan validasi eksternal yang kuat terhadap urgensi masalah yang diangkat serta relevansi solusi yang ditawarkan oleh platform, baik dari sisi kelayakan teknis maupun keberlanjutan bisnis.

Untuk mewujudkan visi sebagai platform yang efisien, transparan, dan terutama terpercaya, arsitektur sistem harus dirancang dengan fondasi keamanan dan pengelolaan akses yang kokoh. Platform Volunteerin.id akan mengelola interaksi antara berbagai jenis pengguna dengan hak dan kapabilitas yang berbeda, seperti relawan, penyelenggara kegiatan (*organizer*), dan administrator sistem. Kebutuhan ini menuntut implementasi mekanisme kontrol akses yang terstruktur untuk memastikan setiap pengguna hanya dapat mengakses data dan menjalankan fungsi yang sesuai dengan perannya.

Dalam rekayasa perangkat lunak, pendekatan standar untuk mengatasi tantangan ini adalah *Role-Based Access Control* (RBAC), yang formalisasinya tertuang dalam standar ANSI/INCITS 359-2004 [12]. RBAC menyederhanakan manajemen izin dengan mengasosiasikannya pada peran, bukan pada pengguna individual, sehingga mampu mencegah eskalasi hak akses (*privilege escalation*) dan meningkatkan tata kelola sistem secara keseluruhan.

Urgensi penerapan RBAC yang konsisten menjadi semakin krusial jika ditinjau dari perspektif keamanan siber. Laporan OWASP API Security Top 10 tahun 2023, yang menjadi rujukan utama keamanan API, menempatkan *Broken Object Level Authorization* (BOLA) pada peringkat pertama (API1:2023) dan

*Broken Function Level Authorization* pada peringkat kelima (API5:2023) [13]. Kedua kerentanan kritis ini timbul akibat kegagalan sistem dalam memvalidasi otorisasi pengguna terhadap sumber daya dan fungsionalitas. Dengan demikian, implementasi RBAC pada level *API RESTful* menjadi sebuah keharusan. Ini bukan sekadar pilihan desain, melainkan sebuah mekanisme pertahanan yang fundamental. Mekanisme ini bertujuan untuk memitigasi risiko keamanan yang telah diidentifikasi. Penerapannya akan memastikan Volunteerin.id dapat beroperasi sebagai platform yang aman dan andal. Pada akhirnya, langkah ini akan menjaga kepercayaan pengguna dalam ekosistem kerelawanan digital di Indonesia.

## **1.2. Rumusan Masalah**

Berdasarkan gambaran umum yang telah diuraikan, masalah-masalah utama yang akan diselesaikan dalam laporan ini dapat dirumuskan sebagai berikut:

1. Bagaimana merancang model *Role-Based Access Control* (RBAC) yang mampu merepresentasikan hak akses berbeda bagi peran *Volunteer*, *Partner*, dan *Admin* pada RESTful API platform Volunteerin.id secara efektif dan terstruktur?
2. Bagaimana implementasi RBAC pada RESTful API dapat memastikan bahwa setiap kategori pengguna hanya dapat mengakses fitur dan data sesuai dengan kewenangannya masing-masing di dalam platform Volunteerin.id?
3. Bagaimana menguji dan mengevaluasi fungsionalitas serta aspek keamanan dari sistem RBAC yang telah diimplementasikan untuk memastikan efektivitas pembatasan akses antar peran pengguna?

## **1.3. Batasan Masalah**

Untuk menjaga agar laporan ini tetap fokus dan terarah, ditetapkan batasan-batasan masalah sebagai berikut:

2. Laporan ini berfokus pada implementasi mekanisme otorisasi di sisi backend, yaitu pada *RESTful API* yang dikembangkan menggunakan *Node.js* dengan

- kerangka kerja *Express.js*. Laporan tidak mencakup perancangan maupun implementasi logika kontrol akses di sisi frontend atau antarmuka pengguna.
3. Sistem otentikasi pengguna, termasuk proses login dan penerbitan *JSON Web Token (JWT)*, diasumsikan telah tersedia dan berfungsi dengan baik. Fokus utama laporan terletak pada mekanisme otorisasi setelah proses otentikasi berhasil dilakukan.
  4. Implementasi kontrol akses dibatasi pada tiga peran utama dalam ekosistem *Volunteerin.id*, yaitu *Admin*, *Partner* (penyelenggara kegiatan), dan *Volunteer*.
  5. Manajemen peran dan hak akses dilakukan secara statis melalui konfigurasi kode program dan skema basis data. Laporan ini tidak mencakup pengembangan antarmuka dinamis untuk pengelolaan peran dan izin akses.
  6. Evaluasi sistem dibatasi pada pengujian fungsional guna memverifikasi skenario akses berbasis peran di lingkungan pengembangan. Fokus pengujian adalah memastikan setiap *endpoint API* hanya dapat diakses oleh peran yang berhak, tanpa mencakup analisis keamanan mendalam seperti *penetration testing* atau *vulnerability assessment*.

#### 1.4. Tujuan

Tujuan yang ingin dicapai melalui laporan dan pengembangan ini adalah:

1. Merancang model *Role-Based Access Control (RBAC)* yang secara efektif merepresentasikan hak akses bagi tiga peran utama pengguna pada platform *Volunteerin.id*, yaitu *Volunteer*, *Partner*, dan *Admin*, sesuai dengan kebutuhan interaksi dan tanggung jawab masing-masing peran di dalam sistem.
2. Menerapkan model RBAC pada *RESTful API* yang dikembangkan menggunakan *Node.js* dan *Express.js*, guna memastikan setiap pengguna hanya dapat mengakses data dan menjalankan fungsi sesuai dengan otorisasi yang dimilikinya.
3. Melakukan evaluasi terhadap fungsionalitas dan keamanan implementasi RBAC, melalui serangkaian pengujian fungsional untuk memverifikasi bahwa

setiap *endpoint API* hanya dapat diakses oleh peran yang memiliki izin sesuai aturan yang telah ditetapkan.

