BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era digital yang semakin berkembang, aplikasi web telah menjadi bagian penting dari infrastruktur teknologi informasi modern. Berbagai layanan kritis seperti e-commerce, perbankan online, hingga sistem manajemen rumah sakit kini banyak bergantung pada aplikasi berbasis web [1], [2]. Web server berperan sebagai komponen utama yang memungkinkan pengguna mengakses berbagai layanan tersebut, termasuk transaksi online banking, pembelian daring, serta layanan email berbasis web [3]. Pertumbuhan sektor e-commerce juga meningkat pesat sejak pandemi Covid-19, yang membuka peluang bisnis baru namun sekaligus memperbesar potensi ancaman keamanan siber. Laporan dari Cybersecurity and Infrastructure Security Agency (CISA) menyebutkan bahwa lebih dari 70% organisasi di dunia mengalami setidaknya satu insiden keamanan siber sepanjang tahun 2023 [2].

Seiring dengan meningkatnya ketergantungan terhadap aplikasi web, berbagai penelitian menunjukkan bahwa banyak sistem masih memiliki kerentanan keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Penelitian mengenai pengujian keamanan aplikasi web menggunakan metode penetration testing menemukan sejumlah kerentanan seperti Cross-Site Scripting (XSS), konfigurasi keamanan yang tidak tepat, serta kelemahan pada mekanisme perlindungan aplikasi web [1, 2]. Temuan tersebut menunjukkan bahwa implementasi keamanan pada banyak sistem web masih belum optimal sehingga berpotensi membuka celah bagi serangan siber.

Salah satu bentuk serangan yang masih sering ditemukan pada aplikasi web adalah SQL injection (SQLi), dengan jumlah serangan yang diperkirakan mencapai sekitar 340 juta kasus setiap tahun [4]. SQL injection merupakan kerentanan yang memungkinkan penyerang memanipulasi perintah database melalui input yang tidak divalidasi dengan baik [5]. Meskipun kerentanan ini telah lama diketahui dan banyak dibahas dalam literatur keamanan informasi, SQL injection masih menjadi masalah yang cukup umum. Berdasarkan laporan OWASP Top 10 (2025), kategori Injection masih menjadi salah satu kerentanan keamanan aplikasi web yang signifikan dengan cakupan pengujian mencapai 100% aplikasi, total

62.445 CVE, serta lebih dari 1,4 juta kejadian kerentanan yang tercatat. Tingkat insiden maksimum kerentanan ini mencapai 13,77% dengan rata-rata 3,08%, yang menunjukkan bahwa serangan berbasis injeksi, termasuk SQL Injection, masih menjadi ancaman penting terhadap keamanan aplikasi web [6]. Hal tersebut disebabkan oleh beberapa faktor seperti kurangnya validasi input, praktik pengembangan perangkat lunak yang kurang aman, serta semakin berkembangnya teknik serangan yang digunakan oleh pelaku kejahatan siber [5]. Melalui teknik ini, penyerang dapat mengakses atau memodifikasi data secara tidak sah, merusak integritas data, hingga memperoleh hak akses administratif pada sistem database [7].

Dampak dari serangan SQL injection dapat menimbulkan kerugian yang sangat besar bagi organisasi maupun pengguna. Beberapa kasus nyata menunjukkan bagaimana serangan ini dapat mengekspos data sensitif dalam jumlah besar. Sebagai contoh, serangan terhadap National Job Portal di India menyebabkan kebocoran data pribadi sekitar 30 juta pencari kerja [5]. Penelitian terbaru juga menunjukkan bahwa kerentanan SQL injection dapat menghasilkan skor CVSS hingga 9.1 (kategori Critical), yang menandakan potensi dampak yang sangat serius terhadap kerahasiaan, integritas, dan ketersediaan data [4].

Salah satu pendekatan yang dapat dilakukan untuk mengetahui tingkat keamanan suatu sistem adalah melalui penetration testing. Metode ini digunakan untuk mengidentifikasi dan mengevaluasi kerentanan yang terdapat pada web server atau aplikasi web sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab [3]. Namun, proses mendeteksi dan mencegah serangan SQL injection tidak selalu mudah, terutama pada sistem yang memiliki struktur kompleks atau ukuran yang besar [5]. Berbagai tools keamanan seperti SQLMap dapat membantu dalam mengotomatisasi proses identifikasi dan eksploitasi kerentanan SQL injection [7].

Dalam proses analisis kerentanan keamanan, Common Vulnerability Scoring System (CVSS) sering digunakan sebagai standar untuk menilai tingkat keparahan suatu kerentanan [8] . Namun, penelitian dari Kholilul Andrian menunjukkan bahwa penggunaan CVSS masih memiliki keterbatasan, terutama ketika dokumentasi teknis yang tersedia tidak cukup lengkap [4]. Selain itu, penelitian lain juga menunjukkan bahwa analisis kerentanan sering kali belum melakukan kajian mendalam terhadap parameter CVSS secara individual serta belum mengintegrasikan hasil eksploitasi dengan penilaian tingkat keparahan kerentanan secara komprehensif [5]. Di sisi lain, berbagai penelitian mengenai kerentanan SQL Injection pada aplikasi web umumnya masih berfokus pada

proses identifikasi atau demonstrasi eksploitasi kerentanan tanpa disertai evaluasi risiko yang terukur secara sistematis[3, 9]. Hal ini menunjukkan bahwa kajian yang mengintegrasikan proses eksploitasi SQL Injection dengan analisis tingkat keparahan kerentanan menggunakan standar CVSS masih relatif terbatas.

Oleh karena itu, diperlukan penelitian yang tidak hanya melakukan eksploitasi kerentanan SQL Injection tetapi juga menganalisis tingkat keparahan dan risiko yang ditimbulkan menggunakan pendekatan yang terukur. Penelitian ini bertujuan untuk menganalisis risiko keamanan yang ditimbulkan oleh kerentanan SQL Injection melalui pendekatan yang menggabungkan proses eksploitasi praktis dengan evaluasi risiko secara sistematis. Penelitian dilakukan dalam lingkungan laboratorium yang sengaja dirancang rentan agar proses pengujian dapat dilakukan secara aman dan terkontrol. Eksploitasi SQL Injection dapat dilakukan menggunakan teknik manual ataupun tools otomatis seperti SQLMap untuk memperoleh akses terhadap data sensitif pada basis data aplikasi. Selanjutnya, tingkat keparahan kerentanan dianalisis menggunakan standar Common Vulnerability Scoring System (CVSS) v3.1 dengan mempertimbangkan parameter Attack Vector, Attack Complexity, Privileges Required, User Interaction, serta dampaknya terhadap aspek Confidentiality, Integrity, dan Availability.

Hasil perhitungan skor CVSS selanjutnya digunakan untuk menginterpretasikan tingkat risiko dari kerentanan yang ditemukan. Hasil penelitian ini diharapkan dapat memberikan pemahaman mengenai dampak keamanan yang ditimbulkan oleh kerentanan SQL Injection, serta menghasilkan rekomendasi mitigasi yang dapat diterapkan oleh pengembang aplikasi web untuk mengurangi risiko serangan tersebut.

1.2 Rumusan Masalah

1. Kerentanan *SQL Injection* apa saja yang dapat diidentifikasi dan dieksploitasi pada aplikasi web menggunakan metode *penetration testing*, dan bagaimana dampaknya terhadap keamanan data?
2. Bagaimana tingkat keparahan dan risiko kerentanan SQL Injection yang ditemukan apabila dianalisis menggunakan standar Common Vulnerability Scoring System (CVSS) v3.1?

1.3 Batasan Permasalahan

1. Eksploitasi kerentanan SQL Injection dilakukan menggunakan tools SQLMap.
2. Analisis tingkat keparahan kerentanan dilakukan menggunakan standar Common Vulnerability Scoring System (CVSS) v3.1.
3. Penelitian hanya berfokus pada analisis kerentanan dan penilaian tingkat risiko tanpa membahas implementasi perbaikan sistem secara mendalam.
4. Pengujian dilakukan pada testing environment yang digunakan sebagai objek penelitian.
5. Eksploitasi tidak dilakukan secara destruktif dan tidak merusak sistem target.
6. Tidak dilakukan tahapan lanjutan seperti privilege escalation, maintaining access, dan covering tracks.

1.4 Tujuan Penelitian

1. Mengidentifikasi dan mengeksploitasi kerentanan *SQL Injection* pada aplikasi web menggunakan metode *penetration testing*, serta menganalisis dampaknya terhadap keamanan data.
2. Menganalisis tingkat keparahan dan risiko kerentanan yang ditemukan menggunakan metode CVSS v3.1.

1.5 Manfaat Penelitian

1. Memberikan pemahaman mengenai proses eksploitasi kerentanan SQL Injection pada aplikasi web.
2. Memberikan gambaran mengenai tingkat keparahan kerentanan keamanan menggunakan metode CVSS v3.1.
3. Menjadi referensi bagi peneliti selanjutnya dalam melakukan analisis keamanan aplikasi web yang mengintegrasikan proses eksploitasi kerentanan dengan evaluasi tingkat risiko.

4. Memberikan wawasan bagi pengembang sistem mengenai pentingnya pengujian keamanan untuk meminimalkan risiko kerentanan pada aplikasi web.

1.6 Sistematika Penulisan

Berisikan uraian singkat mengenai struktur isi penulisan laporan penelitian, dimulai dari Pendahuluan hingga Simpulan dan Saran.

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Bab ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan yang digunakan dalam penyusunan laporan.

- Bab 2 LANDASAN TEORI
  Bab ini membahas teori-teori yang mendukung penelitian, meliputi konsep dasar keamanan aplikasi web, SQL Injection, jenis-jenis SQL Injection, serta metode penilaian kerentanan menggunakan Common Vulnerability Scoring System sebagai dasar analisis.

- Bab 3 METODOLOGI PENELITIAN
  Bab ini menjelaskan metode yang digunakan dalam penelitian, meliputi tahapan penelitian, proses pengujian kerentanan menggunakan tools *SQLMap*, serta metode penilaian kerentanan menggunakan *Common Vulnerability Scoring System* (CVSS).

- Bab 4 HASIL DAN DISKUSI
  Bab ini menyajikan hasil pengujian yang telah dilakukan, analisis terhadap kerentanan yang ditemukan, serta perhitungan skor kerentanan menggunakan metode CVSS berdasarkan hasil pengujian yang diperoleh.

- Bab 5 KESIMPULAN DAN SARAN
  Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan serta saran untuk pengembangan penelitian selanjutnya.