

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini mengalami perubahan yang sangat pesat [1]. Hal ini dapat dilihat dari banyaknya pengguna *website* yang semakin meningkat, baik untuk keperluan instansi, pendidikan, organisasi, maupun keperluan pribadi. Universitas Bhayangkara Jakarta Raya sebagai salah satu institusi pendidikan tinggi di Indonesia, memanfaatkan *website* sebagai sarana untuk memberikan informasi, layanan akademik, dan interaksi dengan mahasiswa dan masyarakat luas. Keamanan sistem menjadi salah satu aspek penting dalam sistem informasi. Hal ini dapat dilihat dengan meningkatnya jumlah pengguna yang terhubung ke jaringan internet, risiko terjadinya tindak kejahatan siber oleh pihak yang tidak bertanggung jawab juga semakin tinggi [2].

Pembuatan sistem informasi dapat meningkatkan mutu dan kualitas suatu organisasi. Pentingnya nilai informasi yang dihasilkan dari sistem harus dibatasi pengaksesan oleh orang-orang tertentu agar nilai informasi yang disampaikan terjaga integritasnya. Informasi yang jatuh ke pihak lain yang tidak berwenang dapat menimbulkan kerugian bagi organisasi sehingga sistem yang dibuat harus mampu mengatasi tindakan-tindakan yang tidak diinginkan [3].

Website menjadi salah satu tujuan utama bagi pengguna internet, khususnya dalam memanfaatkan untuk melakukan aktivitas bisnis maupun mengakses informasi [4]. Sebagai *platform* akademik, skripsifasilkom.id memfasilitasi pengelolaan dokumen dan penjadwalan bimbingan. Namun, layanan berbasis *web*

rentan terhadap ancaman serangan siber, seperti *Cross-Site Scripting(XSS)* dan *SQL Injection* apabila tidak dikonfigurasi dengan benar.

SQL Injection menempati peringkat ketiga dalam OWASP Top 10 sebagai salah satu kerentanan paling kritis pada aplikasi *web* [5]. Teknik ini bekerja dengan menyuntikkan kode berbahaya ke dalam *string input* pengguna yang kemudian digabungkan dengan perintah SQL dan dijalankan oleh *database*. Jika terdapat celah keamanan, penyerang dapat memanipulasi *query* SQL untuk mendapatkan akses tidak sah ke *database*, yang memungkinkan mereka mencuri, memanipulasi, atau bahkan merusak data penting.

Serangan *SQL Injection* juga dapat menyebabkan gangguan operasional, pemadaman layanan, hingga kerusakan reputasi dan kepercayaan pengguna[6]. Serangan ini juga dapat menyebabkan kerugian finansial melalui penipuan atau pemerasan, tuntutan hukum, hingga penurunan bisnis. Pada beberapa kasus, *SQL Injection* menjadi pintu masuk untuk serangan lanjutan seperti *ransomware*, bahkan pengambilalihan sistem. Tanpa adanya mitigasi yang tepat, kerentanan ini akan terus dieksploitasi dengan teknik yang semakin canggih.

Meskipun teknik pencegahan seperti *parameterized queries* dan *input validation* telah banyak diterapkan, masih banyak pengembang dan perusahaan yang mengabaikan praktik keamanan, sehingga aplikasi *web* tetap rentan terhadap eksploitasi serangan ini. Dengan berkembangnya teknik penyerangan seperti *Blind SQL Injection* dan *Time Based Sql injection*, penyerang dapat dengan mudah melakukan eksploitasi tanpa meninggalkan jejak.

Oleh karena itu, penelitian dengan judul “Analisis Keamanan Jaringan *Web* Universitas Bhayangkara Jakarta Raya Dengan Metode *Penetration Testing*

Menggunakan OWASP” diharapkan dapat menganalisis lebih dalam mekanisme dan metode pencegahan terhadap serangan *SQL Injection*. Penelitian ini juga diharapkan dapat mengembangkan solusi yang lebih kuat untuk meminimalisir risiko serangan dan meningkatkan keamanan aplikasi *web* di masa mendatang.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan menunjukkan adanya indikasi kerentanan pada sistem, sehingga penting untuk mengidentifikasi masalah yang terjadi sebagai berikut :

1. *Website* skripsifasilkom.id berpotensi rentan terhadap serangan *SQL Injection* karena kurangnya konfigurasi keamanan yang memadai.
2. Serangan *SQL Injection* dapat menyebabkan kebocoran data sensitif, manipulasi *database*, dan gangguan operasional pada layanan akademik.
3. Minimnya penerapan praktik keamanan dasar oleh pengembang aplikasi *web* dan belum ada pengujian keamanan khusus untuk mendeteksi atau memitigasi risiko ini.

1.3 Rumusan Masalah

Berdasarkan latar belakang dan identifikasi masalah yang telah diuraikan, maka rumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana tingkat kerentanan *SQL Injection* yang terdapat pada skripsifasilkom.id berdasarkan standar OWASP Top 10?
2. Apakah *SQL Injection* dapat digunakan dalam mengeksploitasi *website* skripsifasilkom.id?
3. Berdasarkan hasil pengujian, rekomendasi apa yang dapat diberikan untuk meningkatkan keamanan sistem informasi di *website* skripsifasilkom.id?

1.4 Tujuan Penelitian

Tujuan penelitian “Analisis Keamanan Jaringan *Web* Universitas Bhayangkara Jakarta Raya Dengan Metode *Penetration Testing* Menggunakan OWASP (Studi Kasus: skripsifasilkom.id)” diantaranya:

1. Mengidentifikasi kerentanan *SQL Injection* yang terdapat pada skripsifasilkom.id menggunakan metode *Vulnerability Analysis* dengan tools OWASP ZAP, BurpSuite, dan SQLMap.
2. Mengidentifikasi teknik eksploitasi *SQL Injection* yang berpotensi digunakan terhadap aplikasi *website*.
3. Memberikan rekomendasi solusi mitigasi seperti penerapan *parameterized queries* dan *input validation*.

1.5 Manfaat Penelitian

1.5.1 Bagi Peneliti

1. Sebagai salah satu syarat untuk mendapatkan gelar Sarjana Komputer (S.Kom).
2. Peneliti dapat memiliki ilmu dan pengalaman baru serta meningkatkan kompetensi dalam melakukan *penetration testing* dan analisis resiko keamanan *website*.

1.5.2 Bagi Fakultas Ilmu Komputer

1. Sebagai rekomendasi teknis untuk meningkatkan keamanan fitur akademik, seperti implementasi sanitasi *input*.
2. Sebagai kontribusi karya ilmiah dalam disiplin ilmu di bidang Ilmu Komputer.
3. Pihak Fakultas Ilmu Komputer dapat memanfaatkan hasil penelitian ini menjadi panduan teknis untuk memperbaiki celah keamanan pada fitur akademik dan mencegah insiden seperti *SQL Injection* terjadi.

4. Menjadi studi kasus nyata tentang penerapan OWASP Top 10 dalam mengamankan fitur-fitur kritis pada *website* akademik.

1.5.3 Bagi Pembaca

1. Pembaca mendapatkan pemahaman praktis tentang ancaman siber di sistem akademik dan cara mendeteksinya.
2. Panduan kesadaran keamanan *digital*, terutama bagi mahasiswa yang menggunakan sistem *web* skripsifasilkom.id.
3. Referensi metodologi *penetration testing* berbasis OWASP Top 10 untuk penelitian sejenis.

1.6 Batasan Masalah

1.6.1 Metode

1. Metode pengumpulan data dalam penelitian ini menggunakan pengujian *vulnerability analysis* dan observasi langsung terhadap *website* skripsifasilkom.id, studi literatur mengadaptasi dari OWASP Top 10.
2. Metodologi pengujian mengadaptasi dari standar OWASP Top 10 yang terdiri dari 6 langkah diantaranya *Planning and Scoping*, *Information Gathering*, *Vulnerability Identification*, *Exploitation*, Analisis dan Evaluasi Risiko, dan *Reporting*.

1.6.2 Tools

1. Menggunakan Oracle VM VirtualBox dengan sistem operasi Kali linux.
2. Menggunakan tools OWASP ZAP untuk melakukan proses *scan manual* terhadap kerentanan pada fitur *login* dan tools SQLMAP untuk deteksi SQL *Injection*.

3. Menggunakan BurpSuite sebagai *proxy* dan *repeater* untuk melakukan *Intercepting and Modifying Request*.

1.6.3 Proses

1. Studi kasus pada penelitian ini adalah fitur kelemahan pada *form login* aplikasi web skripsifasilkom.id yaitu *SQL Injection(A03)*.
2. Tahapan metodologi yang digunakan mengadaptasi dari *standar* OWASP Top 10 yang terdiri dari *Planning and Scoping, Information Gathering, Vulnerability Identification, Exploitation, Analisis dan Evaluasi Risiko, dan Reporting*.
3. Pengujian pada penelitian ini mengacu pada standar OWASP Top 10 dengan pengujian berjenis *Vulnerability Analysis* tanpa melakukan eksploitasi lanjutan seperti penghapusan data atau eskalasi hak akses.

1.7 Sistematika Tugas Akhir

Berikut adalah sistematika yang terdapat pada penelitian ini yang terdiri dari 5 bab, diantaranya:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, identifikasi masalah, tujuan penelitian, manfaat penelitian, rumusan masalah, dan batasan masalah.

BAB II TINJAUAN PUSTAKA

Berisi tentang berbagai teori yang berkaitan dengan permasalahan yang akan dibahas, seperti teori keamanan jaringan, *penetration testing*, dan OWASP

BAB III METODOLOGI PENELITIAN

Adalah bab yang menjelaskan tentang lokasi penelitian, metode, pengumpulan data, metode analisis data, dan tahapan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan uraian hasil yang diperoleh dari pengujian yang dilakukan dan hasil pengujian dalam konteks teori penelitian sebelumnya.

BAB V PENUTUP

Berisi kesimpulan dan saran.

