# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Keamanan merupakan faktor esensial dalam evolusi teknologi informasi, terkhusus pengembangan *website*. Struktur keamanan yang kokoh menurut Da Veiga dkk. (2020), memainkan peran vital untuk memangkas risiko insiden siber di suatu instansi. Perguruan tinggi, sebagai institusi, tidak diragukan lagi memiliki sistem terkomputerisasi yang dirancang bangun untuk memfasilitasi kegiatan operasional di lingkungan kampus. Sistem Informasi Pegawai milik Universitas Malikussaleh secara partikular digunakan seluruh pegawai (dosen dan staf) untuk mengakses berbagai informasi komprehensif seperti; data pegawai, laporan, absensi, dan lain-lain secara daring. Memastikan keamanannya menjadi sangat krusial sebab menyimpan kredensial pengguna. Bila pembobolan terjadi menurut Purbo (2020), data rahasia terungkap, yang kerap kali menempatkan pengguna pada konsekuensi pencurian identitas, merusak reputasi, dan hampir selalu memaksa organisasi bertanggung jawab atas pelanggaran tersebut. Sementara di tahun 2022, menurut Mathilda (2023), Badan Siber dan Sandi Negara (BSSN) memaparkan persentase kebocoran data yaitu 14,75 persen dari total jumlah 976.429.996 serangan siber.

SIMPEG UNIMAL dirancang menggunakan bahasa seperti HTML, CSS, dan JavaScript. Pemilihan bahasa tersebut dalam membangun antarmuka, memunculkan potensi bagi penyerang mendeteksi atau bahkan mengeksploitasi kerentanannya. Menurut Liu (2019), umumnya, celah ditampilkan dengan menyuntikan kode berbahaya pada halaman atau *form*. Namun, penyerangan menurut Aydos dkk. (2022), juga dapat dilakukan pada lokasi beragam dengan bermacam taraf skala dan kompleksitas. Sebab itu, peneliti melakukan pengujian berdasarkan *framework* WSTG (*Web Security Testing Guide*) versi 4.2 dikembangkan OWASP, melalui pendekatan *Client-side Testing* yang berorientasi dari perspektif pengguna. Pemanfaatannya sebagai panduan menurut Abdan (2022), karena menyediakan deskripsi kerentanan, tata cara, poin-poin, dan objektifitas terbarukan selaras dengan perkembangan teknologi *web*.

Pada penelitian ini, evaluasi akan dioptimalkan dengan menerapkan Metode Kualitatif yang memuat 3 fase yaitu *Vulnerability Scanning*, *Penetration Testing*, dan *Reporting*. Di tahap awal, peneliti melakukan *Vulnerability Scanning*, kemudian *Penetration Testing* akan dilakukan berdasarkan hasil temuan dari tahap sebelumnya dengan memakai *Client Role* sebagai Dosen serta didukung Burp Suite, OWASP ZAP, dan perangkat opsional tambahan lainnya. Pengimplementasian metodologi ini menargetkan hasil untuk ditata ke dalam WSTG *Checklist Report* guna menyajikan informasi yang eksplisit terkait celah yang ditemukan dan juga identifikasi saran perbaikannya.

Bersandarkan penjabaran di atas, peneliti menetapkan judul penelitian ini yaitu, **"Uji Keamanan Sistem Informasi Berbasis *Web* Berdasarkan *Framework* OWASP WSTG v4.2: *Client-side Testing* (Studi Kasus: SIMPEG UNIMAL)".**

## 1.2 Rumusan Masalah

Berlandaskan dari latar belakang yang telah dijabarkan, penulis merumuskan permasalahan sebagai refleksi dari kompleksitas dalam penelitian ini, yaitu:

1. Bagaimana kerentanan pada sisi klien *website* SIMPEG UNIMAL, dapat diidentifikasi dengan pengujian berdasarkan *Framework* OWASP WSTG v4.2: *Client-side Testing*?
2. Setelah dilakukannya pengujian keamanan, kerentanan apa saja yang mungkin ditemukan?
3. Apa saja rekomendasi perbaikan untuk mengatasi celah keamanan yang ditemukan?

## 1.3 Batasan Masalah

Merujuk pada perumusan masalah yang telah dijelaskan sebelumnya, penulis memperapat cakupan permasalahan dalam penelitian ini, yaitu:

1. Penelitian menggunakan Metode Kualitatif.
2. Pengujian keamanan berdasarkan *framework* WSTG v4.2: *Client-side Testing*.
3. Sistem yang diuji adalah *website* SIMPEG UNIMAL.

4. Pengujian memakai *Client Role* sebagai Dosen.
5. Pengujian terbagi menjadi 3 fase yaitu; *Vulnerability Scanning*, *Penetration Testing*, dan *Reporting*.
6. Ada 13 tipe pengujian berdasarkan *framework* yang digunakan yaitu; *Testing for* DOM-*Based Cross Site Scripting*, *Testing for* JavaScript *Execution*, *Testing for* HTML *Injection*, *Testing for Client-side* URL *Redirect*, *Testing for* CSS *Injection*, *Testing for Client-side Resource Manipulation*, *Testing Cross Origin Resource Sharing*, *Testing for Cross Site Flashing*, *Testing for Clickjacking*, *Testing* WebSockets, *Testing Web Messaging*, *Testing Browser Storage*, dan *Testing for Cross Site Script Inclusion*.
7. Pemindaian kerentanan menggunakan alat OWASP ZAP dan Burp Suite serta didukung *Browser* Google Chrome dan Mozilla Firefox.
8. Celah keamanan atau kerentanan hanya untuk ditemukan dan dimunculkan, bukan dieksploitasi.
9. Solusi perbaikan hanya mencakup saran umum untuk mengatasi kerentanan yang telah ditemukan.

## 1.4 Tujuan Penelitian

Selain untuk memenuhi syarat penulisan Laporan Tugas Akhir Program Studi Sistem Informasi Universitas Malikussaleh, penelitian ini memiliki tujuan yang diharapkan sebagai berikut:

1. Menguji keamanan SIMPEG UNIMAL berdasarkan *framework* OWASP WSTG v4.2: *Client-side Testing,* dengan fokus pada identifikasi kerentanan pada sisi klien.
2. Mengetahui kerentanan apa saja yang mungkin ditemukan setelah melakukan pengujian keamanan.
3. Memberikan rekomendasi perbaikan untuk mengatasi celah keamanan yang ditemukan.

## 1.5 Manfaat Penelitian

Penelitian ini diharapkan akan memiliki manfaat berupa informasi bagi pengembang untuk mengetahui kerentanan yang ada atau berpotensi pada SIMPEG

UNIMAL melalui pengujian keamanan berdasarkan *framework* OWASP WSTG v4.2: *Client-side Testing* serta memberi informasi identifikasi solusi perbaikan untuk mengatasi kerentanan yang ditemukan.

## 1.6 Sistematika Penulisan

Adapun sistematika penulisan Tugas Akhir ini adalah sebagai berikut:

**BAB I PENDAHULUAN**

Bab ini menguraikan informasi mengenai latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

**BAB II TINJAUAN PUSTAKA**

Bab ini berisi ringkasan teori-teori yang relevan yang berkaitan dengan judul.

**BAB III METODOLOGI PENELITIAN**

Bab ini menjelaskan tentang tahapan-tahapan yang dilakukan dalam penelitian.

**BAB IV HASIL DAN PEMBAHASAN**

Bab ini menguraikan data hasil penelitian dan membuat rekomendasi terhadap tiap permasalahan.

**BAB V KESIMPULAN**

Bab ini berisi kesimpulan dan saran dari penelitian yang dilakukan.

**DAFTAR PUSTAKA**

Berisikan daftar sumber yang telah digunakan untuk mendukung informasi yang disajikan.

**LAMPIRAN**

Lampiran adalah bagian tambahan yang berisikan informasi, data, atau materi pendukung yang relevan dengan Tugas Akhir ini.