BAB 1 PENDAHULUAN

1.1. Latar Belakang

Indonesia menempati posisi ketiga secara global dalam jumlah akun yang terdampak kebocoran data, dengan jumlah sekitar 12,7 juta akun yang mengalami kebocoran hingga kuartal III-2022 [1] . Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) terkait serangan pada aplikasi web tahun 2023, tercatat sebanyak 347 kasus serangan siber, yang terdiri dari 186 serangan pada aplikasi pemerintahan di bidang administrasi, 60 serangan pada sektor lainnya, 38 serangan pada sektor keuangan, 24 serangan pada sektor transportasi, 18 serangan pada sektor ESDM, 5 serangan pada sektor TIK, 5 serangan pada sektor kesehatan, 4 serangan pada sektor pangan, dan 2 serangan pada sektor pertahanan [2] . Meskipun jumlah serangan pada sektor lain relatif sedikit, keamanan aplikasi di bidang pendidikan tetap perlu mendapat perhatian serius. Hal ini disebabkan karena tanpa adanya sistem keamanan yang memadai, data perusahaan atau instansi akan lebih rentan diretas, sehingga berpotensi menurunkan kredibilitas dan citra institusi tersebut [3]. Oleh karena itu, penerapan keamanan aplikasi sejak tahap awal pengembangan akan lebih efektif dan hemat biaya dibandingkan dengan penanganan setelah terjadinya serangan, mengingat seiring waktu akan bermunculan permasalahan baru yang sebelumnya belum teridentifikasi [4].

Perusahaan dan instansi dari berbagai industri semakin memanfaatkan perkembangan teknologi dengan menciptakan aplikasi sebagai platform untuk terhubung dengan pengguna [4] . Salah satu contohnya adalah aplikasi S.E.E.D.S *(Student Enrollment and Education Data System)* milik Telkom University. Aplikasi berbasis web ini memudahkan mahasiswa baru untuk mendaftar ulang tanpa harus datang langsung ke kampus. Aplikasi S.E.E.D.S ini dibangun menggunakan kerangka kerja NestJS. Dimana kerangka kerja ini merupakan kerangka kerja yang berbasis nodejs dimana biasanya digunakan untuk membangun aplikasi pada sisi server. Keamanan aplikasi menjadi perhatian utama, mengingat data pribadi mahasiswa yang sensitif, seperti KTP, nomor rekening, alamat, dan nama orang tua, perlu dilindungi dengan ketat, terutama pada fitur registrasi yang memuat banyak informasi pribadi. Melalui wawancara yang

dilakukan dengan tim pengembang aplikasi S.E.E.D.S, diperoleh informasi bahwa aplikasi tersebut belum pernah menjalani pengujian keamanan, baik dengan metode OWASP maupun metode pengujian lainnya berita acara dapat dilihat pada [lampiran 1]. Hal ini menjadi perhatian serius mengingat potensi serangan siber yang dapat terjadi kapan saja, dengan dampak yang merugikan bagi privasi pengguna. Oleh karena itu, pengujian keamanan atau kerentanan aplikasi secara menyeluruh merupakan langkah krusial untuk mengidentifikasi potensi serangan sekaligus mencegah pencurian data. Mengingat aplikasi dapat diakses kapan saja dan di mana saja selama terhubung ke internet, menjaga keamanan data menjadi prioritas utama agar mahasiswa baru dapat melakukan pendaftaran dengan tenang tanpa kekhawatiran terhadap privasi mereka [3].

Dalam upaya menjaga keamanan aplikasi, diperlukan pengujian keamanan atau kerentanan untuk mengetahui apakah aplikasi memiliki kelemahan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab [5]. Adapun standar keamanan terkait aplikasi website yang populer diantaranya yaitu SANS/CWE Top 25 dan OWASP. SANS/CWE Top 25 merupakan daftar kelemahan yang biasa terjadi pada perangkat lunak [6] . OWASP *(Open Web Application Security Project)* merupakan organisasi non profit yang bertujuan untuk meningkatkan keamanan suatu aplikasi [7] . OWASP memiliki proyek bernama OWASP Top 10 dimana proyek ini merupakan daftar dari 10 serangan yang paling kritis pada keamanan aplikasi web [8]. Perbedaan dari OWASP dan SANS/CWE Top 25 yaitu OWASP lebih berfokus pada kerentanan atau serangan yang biasa terjadi pada aplikasi web sedangkan SANS/CWE Top 25 tidak berfokus pada aplikasi web saja melainkan kepada aplikasi non web juga seperti desktop, IoT dan lainnya di luar web. Pemilihan metode OWASP untuk pengujian keamanan aplikasi S.E.E.D.S didasarkan pada fokus utamanya pada aplikasi web dan tidak akan mengembangkkan aplikasi S.E.E.D.S selain aplikasi berbasis website[lampiran 1], yang sesuai dengan karakteristik S.E.E.D.S sebagai aplikasi berbasis web. Hal ini juga menjadi keunggulan OWASP dibandingkan standar lain seperti SANS/CWE Top 25, yang mencakup kelemahan perangkat lunak secara umum dan tidak secara spesifik berfokus pada aplikasi web [9] . Selain itu, jika dibandingkan, hanya sekitar delapan dari daftar SANS/CWE Top 25 yang relevan dengan

keamanan aplikasi web, sehingga penggunaan OWASP Top 10 sebagai dokumen pengujian aplikasi web menjadi pilihan yang lebih tepat [9] . OWASP digunakan dalam penelitian ini karena merupakan metode keamanan yang secara khusus memfokuskan pada aplikasi berbasis web. Mengingat S.E.E.D.S juga merupakan aplikasi web, penggunaan metode OWASP menjadi pilihan yang tepat dan relevan untuk mengidentifikasi serta mengatasi potensi kerentanan yang mungkin terjadi pada aplikasi tersebut. Dengan demikian, menggunakan OWASP Top 10 sebagai acuan pengujian keamanan aplikasi S.E.E.D.S adalah langkah terbaik untuk memastikan aplikasi diuji sesuai dengan standar yang paling relevan dan serangan yang paling umum terjadi.

Penelitian ini bertujuan menguji keamanan aplikasi S.E.E.D.S menggunakan panduan *OWASP Top 10* serta memberikan evaluasi dan rekomendasi mitigasi berdasarkan dokumen tersebut apabila ditemukan kerentanan. Hasil penelitian diharapkan dapat menunjukkan tingkat kepatuhan aplikasi S.E.E.D.S Telkom University terhadap standar keamanan *OWASP*, menjadi acuan peningkatan keamanan aplikasi berbasis web, serta mengidentifikasi peran kerangka kerja NestJS dalam melindungi keamanan aplikasi.

1.2. Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara mengidentifikasi kerentanan pada aplikasi S.E.E.D.S berdasarkan panduan *OWASP Top 10*?
2. Bagaimana rekomendasi mitigasi yang dapat diterapkan terhadap kerentanan yang ditemukan berdasarkan panduan *OWASP Top 10* pada aplikasi S.E.E.D.S?

1.3. Tujuan dan Manfaat

1. Mengetahui hasil identifikasi kerentanan pada aplikasi S.E.E.D.S berdasarkan panduan *OWASP Top 10*.
2. Mengetahui rekomendasi mitigasi terhadap kerentanan yang ditemukan setelah pengujian berdasarkan panduan *OWASP Top 10* pada aplikasi S.E.E.D.S.

1.4. Batasan Masalah

Penelitian ini akan melakukan pengujian keamanan pada aplikasi S.E.E.D.S dengan mengacu pada standar dokumentasi *OWASP Top 10*. Pengujian difokuskan untuk mengidentifikasi potensi kerentanan, kemudian memberikan rekomendasi mitigasi perbaikan apabila ditemukan celah keamanan, di mana rekomendasi tersebut sepenuhnya didasarkan pada pedoman *OWASP Top 10*. Selain itu, penelitian ini akan melakukan *literature review* untuk mengkaji sejauh mana kerangka kerja NestJS berpengaruh terhadap aspek keamanan aplikasi.

Batasan penelitian ini terletak pada ruang lingkup pengujian, yang hanya mencakup dua fitur utama pada aplikasi S.E.E.D.S yang digunakan oleh calon mahasiswa, yaitu **fitur registrasi ulang** dan **fitur undur diri**. Pemilihan kedua fitur ini didasarkan pada pertimbangan bahwa keduanya memproses, menyimpan, dan mengelola data pribadi mahasiswa, seperti identitas, informasi akademik, dan dokumen pendukung yang bersifat sensitif. Data pribadi tersebut memiliki risiko tinggi jika terekspos atau disalahgunakan, sehingga pengujian keamanan pada fitur-fitur ini menjadi prioritas utama. Dengan pembatasan ruang lingkup tersebut, penelitian ini diharapkan dapat menghasilkan evaluasi yang terfokus, mendalam, dan memberikan rekomendasi yang relevan untuk meningkatkan keamanan aplikasi S.E.E.D.S, khususnya pada fitur yang memiliki dampak besar terhadap perlindungan data pribadi mahasiswa.

1.5. Jadwal Pelaksanaan

Tabel 1.1 Jadwal Pelaksanaan Tugas Akhir

No.	Deskripsi Tahapan	Bulan 1	Bulan 2	Bulan 3	Bulan 4	Bulan 5	Bulan 6
1	Analisis kebutuhan						
2	Perencanaan pengujian						
3	Pembuatan skenario uji						
4	Pengaturan lingkungan uji						
5	Eksekusi skenario uji						
6	Evaluasi hasil pengujian						

7	Penyusunan Laporan/Buku TA						