BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan *website* menjadi aspek yang sangat penting diera digital saat ini. Semakin banyak data yang dipertukarkan melalui internet, mengharuskan setiap organisasi dan perusahaan menjaga dengan ketat kerahasiaan, integritas, serta otentikasi data pada *website* mereka sesuai dengan standar keamanan yang berlaku. Hal ini dipicu oleh tingginya ketergantungan masyarakat terhadap *website*, sehingga keamanan menyeluruh dari sistem harus senantiasa diukur dan ditingkatkan dari waktu ke waktu[1].

Kurangnya perhatian terhadap keamanan sistem *website* dapat membawa dampak buruk bagi pemilik *website*. Tanpa sistem keamanan yang memadai, para peretas dapat dengan mudah mengambil alih kontrol atas sistem yang telah dibangun. Kondisi ini dapat menimbulkan berbagai permasalahan, terutama terkait kebocoran data-data yang bersifat pribadi maupun informasi penting milik perusahaan atau lembaga, yang seharusnya tidak boleh diakses oleh pihak yang tidak berwenang. Namun, tanpa adanya perlindungan keamanan yang kuat, data-data sensitif tersebut dapat dengan mudah dibobol oleh para *hacker*[2].

Ancaman yang timbul dalam suatu sistem disebabkan oleh kesalahan yang muncul pada saat mendesain dan mengembangkan sistem. Beberapa pihak yang tidak bertanggung jawab memanfaatkan kerentanan sistem tersebut untuk melakukan serangan seperti *defacing, phising, denial of service, bruteforce attack*, dan lain sebagainya[3].

Perubahan yang sangat cepat, kadang meluputkan *developer* dalam melakukan pengujian keamanan terhadap aplikasi yang dibangun. Pengujian merupakan proses yang sangat penting didalam pengembangan perangkat lunak yang berkualitas tinggi, karena dari beberapa kesalahan yang dianggap tidak penting beresiko sangat berbahaya hal ini menjadi celah bagi *attacker* untuk memanfaatkan informasi yang dicuri melalui serangan kepada sistem[4].

Sistem informasi berbasis *website* memang banyak memberikan manfaat

serta kemudahan bagi penggunanya. Namun, hal itu tidak dapat menyingkirkan kenyataan bahwa sebuah *website* tetap rentan terhadap berbagai ancaman yang dapat menyerang sistem keamanannya, sehingga dapat mengakibatkan kerugian. Beberapa ancaman yang mungkin terjadi diantaranya *clickjacking, SQL injection, XML External Entity* (XXE), *Cross-Site Scripting* (XSS), dan *Brute Force* dan lainnya. Untuk mengantisipasi hal tersebut, perlu dilakukan pengujian terhadap sistem keamanan *website*, salah satunya melalui *penetration testing*[5].

Penelitian ini dilakukan pada *website* SMP Negeri 2 Bagan Sinembah yang beralamat di https://smpn2bagansinembah.sch.id, dengan menerapkan kerangka kerja *Information Systems Security Assessment Framework* (ISSAF). ISSAF merupakan panduan sistematis untuk menilai dan meningkatkan keamanan informasi melalui identifikasi risiko, evaluasi sistem yang ada, serta penerapan langkah-langkah perlindungan yang tepat. Kerangka ISSAF terdiri dari lima tahapan utama, yaitu *planning, assessment, treatment, accreditation*, dan *maintenance.* Dalam penelitian ini, setelah ditemukan celah kerentanan pada sistem, tahap *assessment* dilakukan untuk memastikan apakah kerentanan tersebut dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Selanjutnya, pada tahap *treatment,* solusi perbaikan diterapkan untuk menanggulangi celah yang ditemukan. Terakhir, tahap *maintenance* mencakup upaya pemeliharaan seperti peninjauan dan pemantauan ulang terhadap *website* guna memastikan sistem tetap terlindungi dari potensi serangan di masa mendatang.

Alasan penulis melakukan penelitian pada *website* SMP Negeri 2 Bagan Sinembah adalah karena sekolah tersebut menyediakan layanan pendaftaran siswa secara daring, namun belum pernah dilakukan analisis keamanan. Hal ini berpotensi menimbulkan celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Jika tidak segera diatasi, kondisi ini dapat mengganggu operasional sistem pada *website*, termasuk akses pengguna atau pengunjung. Oleh karena itu, penelitian ini dilakukan untuk menganalisis tingkat keamanan *website* serta mengusulkan solusi guna mencegah ancaman dan meningkatkan perlindungan sistem informasi sekolah.

Beberapa penelitian sejenis yang pernah dilakukan di antaranya berjudul

“Analisis Keamanan *Website* SMA Negeri 2 Sumbawa Besar Menggunakan Metode *Penetration Testing* (Pentest)”. Dalam penelitian tersebut, SMA Negeri 2 Sumbawa Besar menghadapi permasalahan keamanan *website* yang lemah sehingga rentan terhadap serangan peretas. Metode yang digunakan adalah *penetration testing* yang mencakup tahapan *footprinting, scanning, fingerprinting, exploit,* dan *reporting,* serta memanfaatkan alat OWASP ZAP. Hasil penelitian mengungkapkan 13 sub-file *vulnerability* dengan status *low* dan medium. Rekomendasi perbaikan disusun sebagai solusi untuk meningkatkan keamanan dan mencegah serangan *cyber criminal* dimasa depan[6].

Berikutnya, penelitian berjudul “Analisis Keamanan Open *Website* Menggunakan Metode OWASP dan ISSAF” membahas masalah keamanan pada *website* Diskominfo Kabupaten Kerinci. Penelitian ini menggunakan metode OWASP ZAP dan kerangka ISSAF untuk mengidentifikasi kerentanan seperti *Cross-Site Scripting* dan *SQL Injection*. Rekomendasi perbaikan kemudian diberikan, dan hasil akhir menunjukkan penurunan tingkat risiko dari "*high*" menjadi "*low*"[7].

Selanjutnya, penelitian berjudul “Analisis Celah Keamanan Pada *Website* Dengan Menggunakan Metode *Penetration Testing* dan *Framework* ISSAF Pada *Website* SMK Al-Kautsar” menyoroti celah keamanan seperti *SQL Injection, clickjacking, brute force,* dan *Cross-Site Scripting*. Penelitian ini menggunakan ISSAF dengan tiga tahapan: *planning and preparation, assessment*, dan *reporting.* Hasilnya menunjukkan bahwa *website* SMK Al-Kautsar rentan terhadap serangan *Denial of Service*, tetapi tidak terhadap serangan *Cross-Site Scripting* maupun melalui *port* terbuka[8].

Berdasarkan kajian terhadap beberapa penelitian terdahulu, meskipun topiknya sama-sama membahas analisis keamanan *website*, terdapat perbedaan yang cukup signifikan dibandingkan dengan penelitian penulis. Penelitian ini memiliki perbedaan mendasar, yaitu dalam penerapan kerangka kerja ISSAF secara menyeluruh serta fokus pada *website* tingkat SMP yang belum pernah diuji keamanannya. Tidak hanya mengidentifikasi celah keamanan, penelitian ini juga menyusun langkah-langkah penanganan dan pemeliharaan sebagai bagian dari

pendekatan menyeluruh terhadap keamanan sistem informasi.

1.2 Batasan Masalah

Agar penelitian ini tetap terarah dan tidak melebar dari ruang lingkup pembahasan, maka batasan masalah dalam penelitian ini ditetapkan sebagai berikut:

1. Penelitian ini hanya dilakukan pada *website* SMP Negeri 2 Bagan Sinembah yang beralamat di https://smpn2bagansinembah.sch.id.
2. Kerangka kerja yang digunakan untuk melakukan analisis keamanan adalah *Information Systems Security Assessment Framework* (ISSAF).
3. Fokus pengujian hanya terbatas pada identifikasi celah keamanan eksternal.
4. Pengujian dilakukan menggunakan metode *penetration testing* secara etis tanpa melakukan eksploitasi yang merusak atau mengganggu sistem secara permanen.
5. Solusi yang diberikan bersifat rekomendasi, yaitu berupa solusi peningkatan keamanan berdasarkan temuan dari tahap pengujian, bukan implementasi langsung pada sistem *website* sekolah tetapi implementasinya dilakukan pada aplikasi Tagihlite.

1.3 Tujuan

Berdasarkan rumusan masalah, tujuan dari penelitian ini adalah:

1. Menganalisis tingkat keamanan pada *website* SMP Negeri 2 Bagan Sinembah.
2. Melakukan pengujian untuk memastikan apakah celah-celah yang ditemukan dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.
3. Memberikan solusi perbaikan untuk meningkatkan keamanan *website* sekolah.

1.4 Manfaat

Penelitian ini diharapkan dapat memberikan:

1. Memberikan informasi mengenai kerentanan *website* SMP Negeri 2 Bagan Sinembah sehingga dapat meningkatkan kesadaran akan pentingnya

menjaga keamanan *website*.

2. Memberikan kontribusi dalam bidang keamanan informasi terutama pada pengembang teknologi keamanan.

1.5 Sistematika Penulisan

Bab I **Pendahuluan**

Pada Bab I Berisi latar belakang, batasan masalah, tujuan, manfaat, dan sistematika penulisan.

Bab II **Kajian Pustaka**

Pada Bab II Menjelaskan tentang bagian-bagian penting pada Kajian Pustaka.

Bab III **Desain Sistem**

Pada Bab III Menjelaskan tentang tahapan penelitian yang dilakukan untuk menganalisi keamanan pada *website*.

Bab IV **Eksperimen dan Analisis**

Pada Bab IV Berisi pembahasan proses dan hasil kegiatan penelitian yang dilakukan dengan tahapan-tahapan analisis keamanan *website*

Bab V **Penutup**

Pada Bab V Berisikan kesimpulan, dan saran penelitian.