BAB I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada masa ini berkembang sangat cepat dan berperan penting untuk mempermudah manusia dalam mengatasi berbagai masalah sehari-hari. Dikutip dari situs Hootsuite (2022), jumlah pengguna internet di dunia mencapai angka 4,95 milyar orang atau setara dengan 63,5% jumlah populasi dunia dan akan diperkirakan akan terus mengalami kenaikan di tahun-tahun berikutnya. Di Indonesia sendiri, menurut hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) (2022), pada tahun 2022 pengguna internet di Indonesia sudah mencapai angka 210 juta orang atau setara dengan 77% jumlah populasi Indonesia. Salah satu alasan orang banyak menggunakan internet adalah penggunaan *website*. *Website* telah menjadi salah satu sarana penting dalam menyediakan informasi dan layanan bagi masyarakat umum. Selain itu penggunaan *website* memberikan kemudahan dalam memperbaharui informasi.

Pemanfaatan *website* dengan berbagai keunggulannya membuat baik individu, perusahaan swasta, maupun instansi pemerintah terus berusaha mengembangkan website untuk mencapai efisiensi dalam proses bisnis mereka. *Website* dapat digunakan di berbagai sektor seperti kesehatan, budaya, perbankan, bisnis, dan pendidikan. Selain untuk tujuan bisnis, penerapan *website* juga harus memperhatikan aspek keamanan untuk meningkatkan kepercayaan pengguna dalam mengakses dan menggunakan *website* tersebut. Keamanan *website* menjadi sangat penting seiring meningkatnya volume pertukaran data di internet. Setiap organisasi atau instansi yang menggunakan *website* harus selalu menjaga kerahasiaan, integritas, dan otentikasi data sesuai dengan standar keamanan. Kurangnya keamanan pada *website* dapat menyebabkan dampak negatif seperti eksploitasi kerentanan *website*.

Kerentanan merupakan kelemahan pada aplikasi atau sistem yang disebabkan oleh *bug* maupun cacat design yang dapat menyebabkan seorang penyerang membahayakan penggunakan aplikasi. Kerentanan adalah potensi risiko pada sistem. penyerang menggunakan kerentanan ini untuk mengeksploitasi sistem dan mendapatkan akses informasi yang tidak sah.

Contoh celah keamanan yang kerap terjadi pada sebuah website antara lain seperti *SQL Injection, Broken Authentication and Session Management, Cross Site Scripting (XSS), Insecure Direct Object Reference, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross Site Request Forgery (CSRF), Using Components with Known Vulnerabilities, dan Unvalidated Redirects and Forwards (OWASP, 2022)*. Maraknya kasus pembobolan dan bocornya data yang terjadi belakangan ini dikutip dari Tempo.co (2023), BSSN mendeteksi 207 dugaan kebocoran data di Indonesia pada tahun 2023. Berdasarkan Laporan tahunan yang dikeluarkan oleh Id-SIRTII/CC dan Badan Siber dan Sandi Negara melalui Lanskap Keamanan Siber Indonesia 2022, total trafik anomali di Indonesia selama tahun 2022 sebanyak 976.429.996 anomali yang terdeteksi.

Website digunakan sebagai salah satu strategi untuk mengembangkan penyebaran informasi secara sistematis melalui langkah-langkah yang praktis dan terukur. Namun, keterbukaan dan kemudahan pertukaran serta pengelolaan informasi pada *website* bisa menjadi titik lemah atas data yang disimpan yang bisa berupa informasi sensitif yang berkaitan dengan cara kerja instansi akademik. Oleh karena itu, keamanan dan perlindungan sangat penting dalam membangun *website* untuk mencegah informasi tersebut jatuh ke tangan yang salah. Salah satu metode yang dapat digunakan untuk mengamankan situs web adalah dengan melakukan pengujian keamanan dengan *penetration testing*.

Penetration testing pada *website* bertujuan untuk menemukan celah-celah keamanan yang bisa dikategorikan sebagai risiko kerentanan. Proses *penetration testing* terdiri dari berbagai modul yang sesuai dengan standar atau *framework* yang ada. *Framework* ini digunakan oleh *tester* agar hasil pengujian valid dan dapat dipertanggungjawabkan.

Pengujian keamanan yang akan dilakukan pada Website AAA adalah berdasarkan *Open Web Application Security Project Web Security Testing Guide* (*OWASP WSTG*). *OWASP WSTG* merupakan *framework* yang dirilis oleh *OWASP Foundatiton* yang berisikan tahapan-tahapan yang perlu dilakukan dalam melakukan analisis keamanan pada sistem berbasis *website*. WSTG digunakan sebagai panduan komprehensif dalam pengujian keamanan aplikasi dan layanan *website*. Dilansir dari OWASP (2022), OWASP sebagai organisasi non-profit yang bertujuan meningkatkan keamanan *website*, membuat sebuah guidelines untuk menguji keamanan sebuah website yang disebut *Security Project Web Security Testing Guide (WSTG)*. *OWASP WSTG* versi 4.2 memilki 12 kategori resiko teratas untuk mengevaluasi *website* (OWASP, 2022).

Kemudian, hasil dari dilakukannya pengujian keamanan tersebut akan menghasilkan analisis kerentanan yang berguna untuk mengetahui tingkat keamanan dan menjadikan saran bagi pengembang dalam meningkatkan keamanan sistem di masa mendatang.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, terdapat rumusan masalah pada penelitian ini yaitu sebagai berikut:

1. Bagaimana mengidentifikasi dan mengevaluasi kerentanan keamanan *website AAA* berdasarkan *Web Security Testing Guide* dari *OWASP*?
2. Bagaimana menilai risiko yang ditimbulkan oleh kerentanan yang ditemukan dan memberi rekomendasi mitigasi dan perbaikan kemanan untuk meningkatkan keamanan *website*?

1.3 Tujuan Penelitian

1.3.1 Tujuan Umum

Tujuan umum dari penelitian ini yaitu untuk mengetahui celah kerentanan keamanan pada *website AAA*.

1.3.2 Tujuan Khusus

a. Melakukan pengujian dan menganalisis untuk mengetahui kondisi serta melakukan pengukuran tingkat kerentanan sistem informasi website AAA.

b. Menjabarkan celah serta mengukur tingkat kerentanan yang perlu diperbaiki sehingga dapat membantu untuk memitigasi kegagalan dalam mempertahankan keamanan sistem *website AAA*.

1.4 Manfaat Penelitian

Manfaat yang diharapkan pada penelitian adalah sebagai berikut :

1) Diharapkan dengan adanya penelitian ini, dapat membuat pengembang *website AAA* mengetahui celah keamanan yang memungkinkan sistem dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab.
2) Diharapkan dengan adanya penelitian ini dapat menilai dan memberi mitigasi serta perbaikan keamanan kepada pengembang *website AAA*.