BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Keamanan siber telah muncul sebagai salah satu masalah paling kritis karena fakta bahwa hampir semua orang di dunia tersentuh oleh pengaruh Internet atau *Internet of Things* dalam beberapa aspek kehidupan. Data pribadi orang-orang yang dibagikan melalui *World Wide Web* sangat besar berkat formulir yang mereka isi saat memanfaatkan layanan apa pun yang ditawarkan oleh pemerintah, perusahaan, atau organisasi. Ancaman keamanan siber tampak besar baik dari penjaga data pribadi pengguna dan peretas yang ada di luar sana untuk memanfaatkan celah dalam sistem dan proses untuk mencuri informasi penting dan merusak kekayaan dan ketenangan pikiran orang-orang melalui kegiatan peretasan (Srirang, 2021).

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. Pada awal tahun 2020 lalu berdasarkan data dari kaspersky, terdapat beberapa fasilitas dan situs vital yang menangani covid-19 menjadi target serangan di Indonesia. Menurut Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada awal tahun 2020 terdapat 88 juta serangan siber yang menyerang fasilitas negara dan non negara seperti industri dan kesehatan. Jumlah ini meningkat dari tahun sebelumnya yaitu 1,9 juta serangan (Faridi, 2021).

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 penyerang untuk memanfaatkan informasi yang dicuri melalui serangan kepada sistem (Zirwan, 2022).

Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Kerinci adalah sebuah instansi yang bertanggung jawab atas pengelolaan media informasi di lingkup Pemerintahan Kabupaten Kerinci. Keberadaan *website* sebagai media informasi menjadi kebutuhan yang sangat penting untuk menyampaikan informasi kepada masyarakat.

Dengan adanya *website*, informasi dan komunikasi antara pemerintah dengan masyarakat bisa dilakukan via internet. Banyak manfaat dari *website* yang digunakan di bidang pemerintahan diantaranya sebagai media penyampaian informasi resmi, memudahkan penyampaian aspirasi masyarakat, mempermudah masyarakat mendapatkan akses pelayanan publik, memudahkan sistem administrasi, menjadi media promosi, mendukung keterbukaan informasi, dan sebagainya.

Namun dengan semakin banyaknya fasilitas *website* yang disediakan untuk mendukung program kerja Diskominfo Kabupaten Kerinci dalam melayani masyarakat, ancaman akan kejahatan dunia maya pun menjadi salah-satu masalah yang harus dihadapi secara seksama. *Website* memiliki kerentanan yang bervarian. Kerentanan ini cukup berbahaya berhubung informasi dan data yang dimiliki suatu instansi pemerintah khususnya Diskominfo Kabupaten Kerinci tidak semuanya bersifat terbuka.

Penggunaan sistem informasi terkadang memiliki kelemahan pada aspek keamanan yang dapat dimanfaatkan oleh oknum tertentu. Keamanan informasi menjadi tantangan utama di era perkembangan informasi seperti saat ini (Aminudin, 2021). Mencegah hal tersebut terjadi, perlu dilakukan evaluasi keamanan sebagai upaya menemukan kelemahan dan celah keamanan dari suatu sistem yang dapat menjadi bahan rekomendasi perbaikan sistem itu sendiri (Handayani, 2020).

Berdasarkan hasil wawancara dengan Kepala Seksi Persandian dan Keamanan Informasi Diskominfo Kabupaten Kerinci, beliau menyatakan bahwa sudah pernah terjadi *Cyber Attack* yang dilakukan terhadap *website* yang dikelola oleh Diskominfo Kabupaten Kerinci. Penyerangan ini terjadi di tahun 2020 dengan tipe penyerangan berupa *web deface*, sehingga dibutuhkannya analisis kerentanan pada *website-website* yang dikelola oleh Diskominfo Kabupaten Kerinci, dengan tujuan agar dapat mengetahui kerentanan yang terdapat pada *website-website* tersebut, sehingga dapat mengurangi penyerangan terhadap *website* yang dikelola Diskominfo.

Penelitian ini akan melakukan analisis keamanan pada open *website* milik Diskominfo Kabupaten Kerinci dengan menggunakan dua metode yaitu metrode *Open Web Application Security Project* (OWASP) dan metode *Information Systems Security Assessment Framework* (ISSAF). Hasil analisis keamanan dari dua metode ini akan dibandingkan untuk dijadikan rekomendasi perbaikan pada sistem tersebut (Kuncoro, 2022).

Dalam penelitian yang dilakukan oleh Kadek Erik Diatmika dkk, yang diberi judul *Pendeteksian Keamanan Website SMA Greenschool Menggunakan Metode Owasp dengan Pengujian XSS* memberi kesimpulan bahwa metode OWASP dapat dijadikan sebagai standar penilaian keamanan aplikasi *web* yang baik.

Penelitian terkait penggunaan metode OWASP dan ISSAF dalam pengujian keamanan sistem telah banyak dilakukan, beberapa pengujian menyebutkan bahwa metode dan alat sangat berpengaruh terhadap langkah dan hasil dari pengujian keamanan sistem. Objek pengujiannya beragam, alat dan metodenya beragam. Setiap metode dan alat yang digunakan memiliki perbedaan, mulai dari tahapannya hingga hasil baik analisis maupun rekomendasinya.

Berdasarkan latar belakang masalah dan penelitian yang dilakukan sebelumnya, maka penulis tertarik untuk meneliti keamanan *website* Diskominfo Kabupaten Kerinci menggunakan dua metode analisis yaitu OWASP dan ISSAF, dengan mengangkat judul: "Analisis Keamanan *Open Website* Menggunakan Metode OWASP dan ISSAF (Studi Kasus Di Diskominfo Kabupaten Kerinci)".

1.2. Perumusan Masalah

Berdasarkan latar belakang yang disampaikan, terdapat beberapa masalah yang bisa diangkat. Dalam penelitian ini akan difokuskan pada dua perumusan masalah diantaranya sebagai berikut:

1. Bagaimana menganalisis keamanan open *website* menggunakan metode OWASP dan ISSAF?
2. Bagaimana menerapkan metode OWASP dan ISSAF dapat meningkatkan keamanan pada *website*?

1.3. Batasan Masalah

Pembatasan masalah dilakukan agar penelitian yang dilakukan lebih terarah dan mencapai sasaran yang ditentukan, maka penelitian ini akan diberi batasan masalah sebagai berikut :

1. Pengujian dilakukan pada 10 website resmi milik instansi-instansi Pemerintah Kabupaten Kerinci
2. Metode yang digunakan untuk menganalisis keamanan website adalah metode OWASP dan ISSAF.
3. Tempat penelitian di Diskominfo Kabupaten Kerinci

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah dan batasan masalah yang disampaikan, maka yang akan menjadi tujuan penulis dalam melakukan penelitian ini adalah sebagai berikut:

1. Melakukan analisis keamanan terhadap *website* yang dikelola oleh Diskominfo Kabupaten Kerinci.
2. Memberikan saran/rekomendasi sebagai standar yang dijadikan panduan untuk menangani kerentanan yang terdapat pada website yang terjadi di *website* yang dikelola oleh Diskominfo Kabupaten Kerinci.

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian yang hendak dicapai, maka penelitian ini diharapkan mempunyai manfaat baik secara langsung maupun tidak langsung. Adapun manfaat yang bisa diperoleh dalam penelitian ini adalah sebagai berikut:

1. Dapat menemukan kelemahan dan celah keamanan dari *website* yang dikelola oleh Diskominfo Kabupaten Kerinci.
2. Dapat memberi saran, rekomendasi atau informasi untuk menangani kerentanan yang terdapat pada *website*.

1.6 Sistematika Penulisan

Sistematika penulisan dilakukan agar lebih mudah untuk dibaca dan dimengerti, maka penulis berusaha menyusun laporan penelitian ini dengan tata urutan secara sistematis. Berdasarkan hal itu, peneliti mengklasifikasikan penelitian ini kedalam enam bab, di mana antara bab satu dengan bab yang lain saling berhubungan.

BAB I : PENDAHULUAN

Pada Bab I menjelaskan latar belakang, perumusan masalah, batasan-batasan masalah, tujuan dari penelitian, manfaat dari penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Pada Bab II menjelaskan tentang teori-teori pendukung yang berkaitan dengan penelitian dan penerapan metode yang digunakan dari literatur jurnal, artikel, makalah, dan lain-lain yang berkaitan dengan penelitian.

BAB III : METODE PENELITIAN

Pada Bab III menjelaskan tentang kerangka kerja, perangkat penelitian yang digunakan, menguraikan tahap-tahap analisis keamanan website menggunakan metode OWASP dan ISSAF

BAB IV : ANALISA DAN PERANCANGAN

Pada Bab IV menjelaskan tentang analisa data dan pembahasan hasil yang didapat dari analisis berdasarkan metode yang digunakan.

BAB V : IMPLEMENTASI DAN HASIL

Pada Bab V menjelaskan tentang tahap implementasi dan pembahasan hasil yang didapat dari analisis berdasarkan metode yang digunakan, pengujian sistem serta pembahasan risiko diserai saran/rekomendasi dalam menanggapi kerentanan *website*.

BAB VI : KESIMPULAN DAN SARAN

Pada Bab VI berisi kesimpulan dan saran yang berkaitan dengan hasil akhir yang diperoleh dari penerapan metode OWASP dan ISSAF dalam menganalisis keamanan *website*.