BAB I
PENDAHULUAN

A. LATAR BELAKANG

Perkembangan teknologi informasi dalam jaringan komputer berkembang sangat pesat dan fleksibel. Internet merupakan jaringan komputer yang lazim digunakan karena kemudahan aksesnya. Satu hal yang membedakan aplikasi jaringan komputer dengan teknologi lainnya adalah tidak adanya batasan dimensi ruang dan waktu. Seluruh informasi dapat tersebar luas dan cepat melalui internet. Oleh karna sifat dari internet adalah publik, informasi yang disebarkan dapat bersifat terbuka. Sifat publik pada internet banyak dimanfaatkan sebagai celah serangan oleh orang yang tidak bertanggung jawab. Hal ini akan beresiko terhadap persebaran informasi yang bersifat tertutup. Seiring dengan pesatnya perkembangan teknologi tersebut, semakin besar pula ancaman dan gangguan terhadap kinerja dalam teknologi tersebut. Untuk itu, keamanan sistem merupakan aspek penting yang harus diperhatikan.

Website riset online menjadi salah satu pilihan bagi *researcher*, karena dapat menutup kekurangan riset secara konvensional, tetapi riset online memiliki kekurangan yaitu kebocoran data berisi informasi pribadi yang dilakukan oknum yang tidak bertanggung jawab. Menurut Kepala Badan Siber dan Sandi Negara (BSSN), Hinsa Siburian mengatakan, selama tahun 2021 ini tercatat ada 888.711.736 serangan *cyber* (Rafeli et al., 2022). Oleh karena itu perlu dilakukan penetration testing terhadap website riset untuk melindungi data pribadi user website riset dan mengurangi kejahatan siber yang bisa menembus sistem keamanan yang ada.

Sistem informasi praktek kerja industri merupakan salah satu website yang dikelola oleh SMK Kesatrian Purwokerto, *website* sistem informasi praktek kerja industri digunakan sebagai sarana sistem informasi pelatihan bagi siswa SMK Kesatrian Purwokerto dalam dunia industri.

Namun selama ini digunakan, *website* belum pernah dilakukan pengujian celah keamanan untuk mengurangi resiko serangan *cyber*.

Penetration testing adalah kegiatan menilai keamanan sistem komputer dengan mensimulasikan serangan dari sumber yang tidak diketahui dan berbahaya serta merupakan aktivitas pengujian keamanan. Mensimulasikan serangan yang dibuat seperti peretasan, jailbreaking, dan lain-lain. Tujuannya adalah mengidentifikasi serta mengetahui jenis-jenis serangan yang dapat terjadi akibat kerentanan dan kelemahan pada sistem.

Metode yang digunakan adalah WSTG 4.2 (*Web Security Testing Guide*) yaitu kerangka kerja yang dirilis oleh OWASP berisikan tahapan-tahapan yang perlu dilakukan dalam melakukan analisis. WSTG digunakan sebagai panduan komprehensif dalam pengujian keamanan aplikasi dan layanan *website*. WSTG memiliki berbagai macam versi yang selalu diperbarui setiap tahunnya, sampai saat ini versi yang terbaru adalah WSTG v4.2.

Hasil uraian latar belakang yang telah disampaikan, maka akan dilakukannya analisis keamanan *website* prakerin.smkkesatrianpwt.sch.id yang bertujuan untuk mencari informasi kerentanan serta celah yang membahayakan pada website tersebut menggunakan metode WSTG 4.2 (*Web Security Testing Guide*).

B. PERUMUSAN MASALAH

Berdasarkan uraian latar belakang diatas, maka perumusan masalah yang dapat diambil dalam penelitian ini adalah "Bagaimana hasil pengujian dan analisis kerentanan *web server* prakerin.smkkesatrianpwt.sch.id menggunakan metode OWASP (*Open Web Application Security Project*)?"

C. BATASAN MASALAH

Sesuai dengan keadaan penelitian, metode yang akan digunakan adalah metode OWASP v4.2 yang berfokus pada identifikasi kelemahan keamanan jaringan.

1. Pada penelitian ini menggunakan 12 tahap berbeda untuk menganalisis keamanan website prakerin.smkkesatrianpwt.sch.id. Metode ini meliputi:
   a. *Information Gathering*
   b. *Configuration and Deployment Management Testing*
   c. *Identity Management Testing*
   d. *Authentication Testing*
   e. *Authorization Testing*
   f. *Session Management Testing*
   g. *Input Validation Testing*
   h. *Testing for Error Handling*
   i. *Testing for Weak Cryptography*
   j. *Business Logic Testing*
   k. *Client-side Testing*
   l. *API Testing*

D. TUJUAN PENELITIAN

Adapun tujuan yang diharapakan tercapai dalam melakukan penelitian pengujian celah keamanan ini adalah:

1. Mengidentifikasi kerentanan sistem pada *web server* prakerin.smkkesatrianpwt.sch.id.
2. Mengetahui hasil pengujian dan analisis pengujian keamanan *web server* menggunakan OWASP.

E. MANFAAT PENELITIAN

Berdasarkan perumusan masalah diatas, maka manfaat dari penelitian ini sebagai berikut:

1. Penelitian ini diharapkan dapat menjadi evaluasi bagi pihak pengelola prakerin.smkkesatrianpwt.sch.id untuk mengetahui tingkat kerentanan dari *web server* yang ada.
2. Penulis dapat mengetahui bagaimana menganilis keamanan website prakerin.smkkesatrianpwt.sch.id menggunakan metode OWASP.