BAB I
PENDAHULUAN

A. LATAR BELAKANG

Perkembangan teknologi informasi dalam jaringan komputer berkembang sangar pesat. Keamanan data menjadi aspek yang sangat penting dalam dunia teknologi informasi dan komunikasi. Ketika data dan informasi disimpan, diproses, dan dikirim melalui sistem komputer, perlindungan terhadap ancaman keamanan menjadi krusial. Kehilangan atau Penyalahgunaan data yang disebabkan oleh kelemahan sistem dapat memiliki konsekuensi serius, seperti kebocoran data, kehilangan kepercayaan, atau kerugian finansial yang signifikan.

Dalam era digital saat ini, website sering digunakan untuk mengelola berbagai jenis data, mulai dari informasi pribadi pengguna, transaksi keuangan, hingga data sensitif perusahaan. Oleh karena itu, memastikan keamanan data melalui website menjadi aspek penting dalam pengembangan dan pengelolaan aplikasi web. Untuk itu, keamanan website merupakan aspek penting yang harus diperhatikan.

Fakultas Teknik dan (FTS) Universitas Muhammadiyah Purwokerto menggunakan website fts.ump.ac.id sebagai platform utama untuk menyediakan informasi akademik, layanan administrasi, dan komunikasi antara mahasiswa, dosen, serta pihak fakultas. Sebagai website yang berfungsi strategis, keamanannya harus terjamin agar dapat melindungi data mahasiswa dan pihak terkait, serta memastikan layanan tetap berjalan tanpa gangguan. Salah satu metode untuk menguji aplikasi berbasis website adalah OWASP WSTG (*Web Security Testing Guide*) yang dikeluarkan oleh owasp.org, sebuah organisasi non-profit yang berdedikasi pada keamanan aplikasi berbasis web(Rochman & Salam, 2021).

Sebelum melakukan analisis keamanan aplikasi berbasis website, terlebih dahulu dilakukan studi literatur dan ditemukan beberapa penelitian terkait. Menurut Pratama & Wiradarma (2019) Langkah-

langkah yang harus dilakukan untuk melihat kerentanan sebuah website terdiri dari berbagai macam tahap, salah satunya adalah tahap pengumpulan informasi dimana penyerang akan mengumpulkan informasi seperti nama domain, alamat IP, informasi PORT, dan lain sebagainya. Pentes OWASP memiliki beberapa metode yang dapat digunakan, salah satunya adalah OWASP WSTG (Web Security Testing Guide) yang berfokus pada kemanan website.

Menurut Elanda & Buana (2020) Metode yang digunakan pada OWASP versi 4 adalah sebagai berikut : (1) Authentication Testing, Otentikasi merupakan tindakan membangun dan mengkonfirmasi sesuatu bahwa klaim yang dibuat adalah benar. (2) Authorization Testing, otorisasi adalah konsep yang memungkinkan akses ke sumber daya hanya bagi yang memiliki izin. (3) Session Management Testing, didefinisikan sebagai kumpulan kontrol yang mengatur interaksi penuh antara pengguna dan aplikasi berbasis web. Dalam tinjauan sistematis ini, dibahas hasil pengujian OWASP versi 4 dan tingkat keamanan sebuah server web berdasarkan beberapa jurnal penerbit.

Menurut Ghozali et al., (2019) Ada beberapa faktor yang menyebabkan kurangnya tingkat keamanan pada aplikasi website, diantaranya adalah kesalahan penulisan kode program dan misconfiguration. Kesalahan pada penulisan kode program dalam pembuatan aplikasi berbasis website sering dimanfaatkan oleh penyerang, dalam hal ini serangan yang sering dimanfaatkan oleh penyerang diantaranya adalah SQL Injection, Authentication dan XSS. Menurut Yunanri et al., (2018) Pada tahun 2013, OWASP menginformasikan adanya kerentanan. Baik secara Umum atau Exposures (CWE) bahwa Cross-Site Scripting (XSS) sebagai satu kerentanan yang paling serius dalam aplikasi web.

Metode yang digunakan adalah OWASP WSTG 4.2 (*Web Security Testing Guide*) yaitu kerangka kerja yang dirilis oleh OWASP yang berisikan tahapan-tahapan yang perlu dilakukan dalam melakukan analisis. OWASP WSTG digunakan sebagai panduan kenvensional dalam

pengujian keamanan aplikasi dan layanan *website.* OWASP WSTG memiliki berbagai macam versi yang selalu diperbarui setiap tahunnya, sampai saat ini versi yang terbaru dari adalah OWASP WSTG 4.2.

Berdasarkan latar belakang di atas, penelitian ini bertujuan untuk melakukan analisis keamanan website fts.ump.ac.id dengan menggunakan metode OWASP WSTG v4.2. Hasil dari penelitian ini diharapkan dapat memberikan gambaran mengenai tingkat keamanan website tersebut dan memberikan rekomendasi perbaikan untuk meningkatkan kualitas pengelolaan keamanannya.

B. RUMUSAN MASALAH

Berdasarkan latar belakang diatas, maka dalam pengerjaan proposal ini dirumuskan rumusan masalah tentang "Bagaimana tingkat keamanan website fts.ump.ac.id berdasarkan analisis menggunakan metode OWASP WSTG v4.2?"

C. BATASAN MASALAH

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

1. Penelitian ini menggunakan 12 tahapan yang berbeda untuk menganalisis keamanan website fts.ump.ac.id. Metode ini meliputi:
   a. *Information Gathering*
   b. *Configuration and Deployment Management Testing*
   c. *Identity Management Testing*
   d. *Authentification Testing*
   e. *Authorization Testing*
   f. *Session Managemen Testing*
   g. *Input Validation Testing*
   h. *Testing For Error Handling*
   i. *Testing For Weak Cryptography*
   j. *Business Logic Testing*
   k. *Client-Side Testing*

D. TUJUAN PENELITIAN

Adapun tujuan yang ingin dicapai dari penelitian adalah mengidentifikasi kerentanan pada website fts.ump.ac.id menggunakan metode OWASP WSTG v4.2.

E. MANFAAT PENELITIAN

Penelitian ini diharapkan dapat menjadi bahan referensi untuk meningkatkan keamanan pada website fts.ump.ac.id.