BAB I
PENDAHULUAN

1.1. Latar Belakang

Pengguna Internet saat ini mengalami peningkatan dengan jumlah yang signifikan. Hal ini terlihat dari meningkatnya permintaan pengguna *website* untuk kebutuhan institusi, pendidikan, organisasi atau pribadi. Berdasarkan laporan terbaru dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pengguna internet di Indonesia pada tahun 2024 telah mencapai 221.563.479 jiwa. Angka ini merepresentasikan 79,5% dari total populasi Indonesia pada tahun 2023 yang mencapai 278.696.200 jiwa. Hasil survei penetrasi internet Indonesia 2024 yang dirilis APJII ini menunjukkan adanya kenaikan penetrasi sebesar 1,4% dibandingkan periode sebelumnya. Peningkatan ini melanjutkan tren positif sejak tahun 2018, di mana penetrasi internet tercatat 64,8%. Angka tersebut terus naik menjadi 73,7% di tahun 2020, 77,01% di tahun 2022, dan 78,19% di tahun 2023 (Asosiasi Penyelenggara Jasa Internet Indonesia, 2024). Oleh karena pengguna internet yang semakin mengalami peningkatan, maka keamanan dalam penggunaan internet menjadi faktor penting yang harus diperhatikan (Mulyanto & Haryanti, 2021).

Aplikasi *web server* yang sebagian besar bergantung pada internet, berisiko tinggi terhadap serangan dari individu tak bertanggung jawab seperti *hacker* atau *cracker*. Para peretas ini seringkali mencari celah keamanan pada *server web* dengan tujuan mendapatkan informasi sensitif tentang organisasi atau perusahaan, yang kemudian dapat mereka gunakan untuk merugikan pihak lain (Elanda & Lintang Buana, 2020) . Sehingga perlunya untuk melakukan analisis keamanan guna mengetahui bagaimana tingkat kualitas dari keamanan *website* yang ada.

SMK XYZ menyediakan berbagai macam informasi melalui *website*, baik informasi mengenai pengenalan sekolah hingga informasi mengenai pendaftaran peserta didik baru secara online. *Website* Penerimaan Peserta Didik Baru (PPDB) SMK XYZ merupakan website yang digunakan oleh pihak sekolah untuk melakukan pendaftaran peserta didik baru, dimana pada *website* tersebut memuat

data penting seperti data calon peserta didik dan wali murid. Oleh karena itu, perlunya penguatan dari segi keamanan *website*. Sistem keamanan *website* yang lemah dapat menjadi sasaran para pihak yang tidak bertanggung jawab. Pihak yang tidak bertanggung jawab dapat mencuri data penting yang ada pada *website* PPDB SMK XYZ seperti data *username* dan *password*, dan data pribadi calon peserta didik.

Penetration testing menggunakan *Open Web Application Security Project (OWASP)* penting untuk dilakukan karena dapat membantu SMK XYZ untuk mengidentifikasi kerentanan keamanan yang terkait dengan aplikasi web. Ini juga membantu SMK XYZ untuk menilai tingkat efektivitas solusi keamanan yang sudah diterapkan. Hal ini penting dilakukan untuk meminimalkan risiko keamanan dan biaya yang terkait dengan tindakan peretasan yang berhasil. Dengan mengikuti rekomendasi *OWASP*, organisasi/perusahaan dapat meningkatkan keamanan aplikasi web mereka dan mengurangi risiko peretasan. *OWASP* dipilih penulis dalam penelitian kali ini karena *OWASP* memiliki beberapa keunggulan dibanding *framework* lain. Keunggulan *OWASP* dibanding *framework* lain adalah komprehensif, mudah digunakan, dan akurat. Selain itu, *OWASP* juga mempunyai lebih dari 250 proyek di seluruh dunia yang dapat digunakan untuk analisis keamanan *website*. *OWASP* juga memiliki banyak cabang komunitas yang sangat aktif yang dapat membantu pengembang dalam mencari solusi untuk masalah keamanan (OWASP Foundation, 2023).

Berdasarkan kondisi yang ada, maka perlu dilakukan penelitian untuk mengetahui dan menganalisis tingkat keamanan yang digunakan pada *website* PPDB SMK XYZ. Ada beberapa parameter keamanan yang digunakan dalam melakukan penelitian ini, antara lain parameter authentication *website* yang kuat, enkripsi data pada *website* yang kuat sehingga tidak dapat diretas oleh pihak yang tidak bertanggung jawab. Dalam penelitian ini, penulis melakukan pengujian terhadap *website* PPDB yang dimiliki SMK XYZ menggunakan metode *Penetration Testing* (*Pentest*) dengan pendekatan *Open Web Application Security Project (OWASP)*. Hasil dari penelitian yang dilakukan akan menjadi saran, rekomendasi, dan solusi kerentanan *website* yang dapat digunakan oleh pengelola *web* PPDB SMK XYZ agar dapat meningkatkan keamanan dari *website* tersebut.

1.2. Rumusan Masalah

Berdasarkan penjelasan latar belakang yang ada diatas, maka rumusan masalah yang dapat diuraikan dalam penelitian kali ini adalah sebagai berikut:

1. Bagaimana mengetahui kualitas dari keamanan *website* PPDB SMK XYZ*?*
2. Bagaimana rekomendasi keamanan yang dihasilkan dari *penetration testing website* PPDB SMK XYZ*?*
3. Bagaimana cara mengimplementasikan rekomendasi keamanan yang dihasilkan dari penetration testing *website* PPDB SMK XYZ*?*

1.3. Tujuan Penelitian

Penelitian ini memiliki beberapa tujuan penting yang dapat diuraikan sebagai berikut:

1. Mengetahui berbagai kerentanan keamanan dari *website* PPDB SMK XYZ berdasarkan *OWASP TOP 10 2017*
2. Memberikan rekomendasi perbaikan untuk keamanan dari *website* PPDB SMK XYZ mengacu pada *OWASP TOP 10 2017*
3. Mengimplementasikan rekomendasi keamanan dari hasil pengujian penetration testing dengan pendekatan *OWASP TOP 10 2017*

1.4. Batasan dan Asumsi Penelitian

Batasan masalah dalam analisis keamanan *website* PPDB SMK XYZ menggunakan *penetration testing* dengan pendekatan *OWASP* adalah sebagai berikut:

1. Analisis keamanan hanya dilakukan pada *website* PPDB SMK XYZ.
2. Analisis keamanan hanya dilakukan menggunakan pendekatan *OWASP Framework*.
3. Analisis keamanan tidak meliputi keamanan fisik *server website* PPDB SMK XYZ.
4. Analisis keamanan tidak meliputi keamanan jaringan yang digunakan untuk mengakses *website* PPDB SMK XYZ.

1.5. Manfaat Penelitian

Manfaat dilakukan analisis keamanan *website* PPDB SMK XYZ menggunakan *penetration testing* dengan pendekatan *OWASP* dapat dijabarkan pada beberapa point dibawah ini:

1. Dapat mengidentifikasi kelemahan – kelemahan yang ada pada aspek keamanan *website* PPDB SMK XYZ yang belum diketahui sebelumnya.
2. Dapat membantu dalam pengambilan keputusan untuk meningkatkan keamanan *website* PPDB SMK XYZ.
3. Dapat mengurangi risiko serangan keamanan yang dapat merugikan *website* PPDB SMK XYZ.
4. Dapat membantu dalam menjaga integritas dan keamanan informasi yang tersimpan pada *website* PPDB SMK XYZ.
5. Dapat meningkatkan kepercayaan pengguna terhadap *website* dan meningkatkan loyalitas mereka terhadap *website* tersebut.