BAB 1

PENDAHULUAN

1.1. Latar Belakang Masalah

Saat ini dunia memasuki era digital, dimana segala informasi ada dalam bentuk digital yang wadahnya bermacam-macam. Pesatnya perkembangan TI memiliki dampak positif diberbagai bidang, salah satunya adalah bidang teknologi web. *Website* merupakan salah satu wadah informasi yang tidak pernah surut kepopulerannya. Teknologi web saat ini sangat penting untuk penyebaran informasi tanpa batas. Dengan begitu banyak lembaga membangun *webserver* tanpa memperhatikan apakah *webserver* yang dibangun memenuhi standar keamanan. Risiko keamanan merupakan aspek penting dari sistem informasi. Namun, ancaman keamanan sering kali tidak dianggap penting. Jika hal ini memengaruhi pengoperasian sistem, keamanan sering kali terancam. Hal ini berbanding terbalik dengan meningkatnya jumlah kerentanan, khususnya pada keamanan situs web, yang ditemukan oleh pakar keamanan dan tersebar luas di Internet. Namun, dalam banyak kasus, kejahatan dunia maya hanya menimbulkan kesan negatif, rasa malu, atau ketidaknyamanan (misalnya pencemaran nama baik).

Seperti dikutip Tribunnews, Jumat 21 September 2018, data yang dikumpulkan oleh *International Data Corporation* (IDC), dan beberapa perusahaan ASEAN masih berkonstrasi pada proyek keamanan inti yang belum tercapai Tingkat kontrol dan optimalisasi yang baik. Sekitar 69,4% Perusahaan ASEAN, termasuk perusahaan Indonesia,

dengan hanya kecuali 0,2% telah mencapai tingkat optimal, meskipun ada serangan dan keamanan sistem komputer (IS) meningkat dan berkembang pesat. Ancaman sepanjang tahun 2018 datang dari empat faktor, mulai dari malware, serangan rantai pasokan, hingga *ransomware*. Munindra, *Senior Director of Consulting Research* dan Managing Director International Data Corporation (IDC) Indonesia, mengatakan: "Hampir 40 perusahaan global menganggap teknik deteksi canggih sebagai metode yang paling efisien untuk menemukan ancaman keamanan siber saat ini "*Transformation Journey*" yang diselenggarakan Telkomtelstra bekerja sama IDC berada dijakarta, pada hari Rabu, 19 September 2018 (Malvyandie Haryadi, 2018).

Jika website Anda memiliki tingkat keamanan yang rendah, peretas dapat dengan mudah mengakses data penting Anda. Karena teknologi yang tersedia saat ini semakin canggih, peretas dapat menggunakan teknik peretasan dengan lebih cerdas untuk mendapatkan keuntungan pribadi dari serangan peretasan. Oleh karena itu, penting untuk melakukan pengujian penetrasi mandiri untuk menguji kerentanan situs web Anda. Ini secara berkala memperbarui tingkat keamanan situs web Anda dan mencegah serangan peretas. Keamanan website merupakan kebutuhan yang mendesak jika menyangkut data pribadi (*privasi),* integritas, hak akses atau verifikasi (*authentication*), kerahasiaan (*secrecy*), dan ketersediaan (*availability*).

Menurut berita yang dimuat oleh (Aneh Unik, 2019), memberitakan beberapa kasus peretasan diantaranya perusahaan besar yaitu, LinkedIn, jaringan sosial terbesar bagi para profesional yang didirikan pada tahun 2012, juga tidak kebal terhadap insiden

peretasan. Peretas tak dikenal itu berhasil memperoleh informasi login dan kata sandi pelanggan pada tahun 2016 dan menjualnya di pasar gelap digital. Berikutnya adalah Adobe yang bergerak di bidang bisnis *software* komputer. Produk Adobe yang sudah kami gunakan adalah dari Adobe Photoshop ke Adobe Reader. Namun, pada tahun 2013, dilaporkan bahwa Adobe diretas dan informasi akun lebih dari 38 juta pelanggan dicuri. Berdasarkan banyaknya kejadian peretasan dari berita yang diumumkan di atas, maka penulis ingin melakukan investigasi keamanan website pada website online PPDB SMK Nurul Bayan. *Website* online PPDB SMK Nurul Bayan Kalapanunggal merupakan sumber informasi bagi civitas akademika yang menyimpan data-data sekolah seperti data informasi pendaftaran, data syarat pendaftaran, dan lain-lain. Dengan mempertimbangkan betapa pentingnya data yang disimpan, maka harus dilakukan uji keamanan pada website PPDB Online SMK Nurul Bayan. Pengujian keamanan ini dilakukan untuk mengukur keamanan. sehingga kita dapat memprediksi serangan dari pihak yang tidak bertanggung jawab dan menganalisis dampak yang ditimbulkan oleh kerentanan tersebut.

Menurut permasalahan diatas, diperlukan penelitian yaitu dengan melakukan analisis celah keamanan website PPDB Online SMK Nurul Bayan dengan menggunakan Metode *Penetration Testing* dan *Vulnerability Assessment*. Bertujuan untuk mengidentifikasi dan mengevaluasi celah keamanan pada aplikasi berbasis web, Keduanya digunakan untuk memastikan bahwa *system* dan aplikasi web terlindungi dengan baik dari serangan yang dilakukan oleh pihak yang tidak bertanggung jawab. Kombinasi dari kedua

Teknik ini, yaitu pengujian penetrasi dan *Vulnerability Assessment* dapat memberikan gambaran yang lebih lengkap tentang keamanan aplikasi berbasis web dan membantu pengembangan untuk memperbaiki celah keamanan yang teridentifikasi.

Uraian tersebut menunjukkan bahwa serangan dapat terjadi kapan saja tanpa diketahui pemilik sistem. Oleh karena itu, penulis berharap bahwa penelitian yang akan datang dapat menyelesaikan masalah yang mungkin terjadi pada website PPDB Online SMK Nuurul Bayan.

1.2. Identifikasi Masalah

Berdasarkan konteks masalah yang telah dipaparkan, perlunya melakukan penelitian terkait keamanan website PPDB Online SMK Nuurul Bayan agar diketahui tingkat kerentanan website serta mengamankan penyerangan dari pihak yang tidak bertanggung jawab.

1.3. Batasan Masalah

Batasan-batasan masalah harus dibuat agar penelitian ini tidak melenceng dan tetap focus. Batasan yang ditetapkan untuk masalah penelitian adalah sebagai berikut :

1. Penelitian ini digunakan untuk memahami celah keamanan dari website SMK Nuurul Bayan Kalapanunggal.
2. Proses analisis celah keamanan dengan Pemindaian kerentanan menggunakan *acunetix* dan OWASP ZAP

1.4. Rumusan Masalah

Mengingat permasalahan yang telah diuraikan kemudian dapat diturunkan beberapa rumusan masalah berikut.

1. Bagaimana proses pengujian celah keamanan pada website PPDB Online SMK Nuurul Bayan dengan metode *Penetration Testing* dan *Vulnerability Assessment?*
2. Bagaimana menganalisis hasil pengujian tingkat keamanan aplikasi web dengan metode *Penetration Testing* dan *Vulnerability Assessment* ?
3. Bagaimana meningkatkan keamanan aplikasi web melalui pengujian keamanan menggunakan *Penetration Testing* dan *Vulnerability Assessment* ?

1.5. Tujuan Penelitian

Tujuan penelitian ini, berdasarkan latar belakang masalah sebelumnya, adalah :

1. Mengevaluasi keamanan website dengan menggunakan metode *Vulnerability Assessment* dan *Penetration Testing.*
2. Mengidentifikasi kerentanan *(vulnerability)* yang mungkin terdapat pada website yang diuji.
3. Melakukan simulasi serangan *(penetration testing)* terhadap website untuk menguji ketahanan sistem terhadap upaya eksploitasi kerentanan yang ditemukan.
4. Menganalisis hasil *vulnerability assessment* dan *penetration testing* untuk memberikan rekomendasi perbaikan atau mitigasi terhadap kerentanan yang ditemukan.

5. Meningkatkan keamanan website dengan menerapkan langkah-langkah perbaikan yang direkomendasikan dari hasil analisis.

1.6. Manfaat Penelitian

Berdasarkan latar belakang masalah yang dipaparkan, Adapun keuntungan yang diharapkan dari penelitian ini yaitu :

1. Hasil penelitian tersebut dimanfaatkan sebagai pengetahuan ilmiah untuk mengetahui kerentanan pada sebuah website.
2. Hasil penelitian ini digunakan sebagai referensi bacaan untuk penelitian berikutnya terhadap *Penetration Testing* dan *Vulnerability Assessment.*
3. Memberikan kontribusi dalam peningkatan keamanan dan penanganan dalam pengelola website sehingga dapat mengoptimalkan kinerja, pemeliharaan dan pengujian website.