BAB I PENDAHULUAN

1.1 Latar Belakang

Pada era yang makin modern ini, perkembangan dalam teknologi informasi yang pesat merupakan suatu fenomena yang luar biasa bagi masyarakat (Bastian et al., 2020). Salah satu contoh hasil dari perkembangan ini adalah terciptanya *website*. *Website* ini juga telah mengalami perubahan mengikuti berkembangnya zaman, generasi pertama *website*, *Web* 1.0, hanya memungkinkan pengguna mencari (*searching*) dan melihat-lihat (*browsing*) informasi, lalu pada *Web* 2.0, para pengguna *website* sudah bisa melakukan komunikasi 2 arah, lalu *Web* 3.0, menawarkan penarikan kesimpulan dari data *online*(Himawan et al., 2020), dan yang terakhir *Web* 4.0, dikenal sebagai dengan istilah revolusi industri, perkembangan teknologi *website* mengarah pada pertukaran data secara mudah dan cepat yang mencakup sistem siber-fisik,, *internet of things*, *cloud computing* dan *cognitive computing*(Hendarsyah, 2019). Dengan kemajuan ini, terdapat beberapa keresahan yang dirasakan, baik dari sisi pengguna maupun pengembang. Keresahan dalam teknologi ini dapat berupa kerentanan keamanan yang dapat menimbulkan ancaman yang berdampak pada kerugian finansial dan merusak citra nama baik perusahaan(Al Vriano, 2023).

Terdapat beberapa kasus akibat kerentanan keamanan yang menyebabkan adanya celah untuk melakukan peretasan. Kasus pertama adalah Tokopedia mengalami peretasan mencapai 91 juta akun dan 7 juta *merchant*. Pelaku menjualnya dengan harga US$5.000 atau sekitar Rp74 juta di *darkweb*(CNN Indonesia, 2020). Lalu kasus kedua adalah bank BSI mengalami kebocoran data sebanyak 15 juta data nasabah, informasi karyawan, dan sekitar 1,5 terabita data *internal*.(Paramitha, 2023). Lalu kasus ketiga adalah Dukcapil Kementerian Dalam Negeri mengalami kebocoran data sebanyak 337 juta, yang dimana data tersebut berisi nama, NIK, No KK, tanggal lahir, alamat, nama ayah, nama ibu, NIK ayah, NIK ibu, No akta lahir/nikah, dan lain-lain(Wardani, 2023). Dan kasus terakhir, lebih dari 17.000 situs *WordPress* disusupi oleh *malware* yang bernama *Ballad Injector*, pelaku melakukan eksploitasi berbagai kerentananan *plugin*

WordPress untuk mengalihkan pengguna ke halaman penipuan(Andhika R, 2023).

Dengan contoh beberapa kasus yang disebutkan diatas, sudah seharusnya pihak pemerintah dan perusahaan mulai mengambil langkah khusus dalam meningkatkan keamanan pada aplikasi atau *website* yang terkait. Adapun salah satu cara untuk mengevaluasi dan membantu dalam meningkatkan keamanan adalah dengan mengamati bagaimana reaksi *website* dalam melawan serangan, untuk memastikan sistem aman adalah dengan mencoba pengujian penetrasi, dengan pengujian penetrasi ini dapat memungkinkan analisis keamanan dalam menemukan kerentanan baru(Zeebare et al., 2020).

Pengujian penetrasi atau *penetration testing* adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi kerentanan keamanan(Rabbani et al., 2020). Pengujian penetrasi ini merupakan proses eksploitasi sistem informasi sebagai upaya menemukan kelemahan dan celah keamanan dari suatu sistem yang dapat menjadi bahan rekomendasi perbaikan sistem itu sendiri(Handayani et al., 2020). Dalam pengujian penetrasi ini terdapat beberapa *framework* seperti ISSAF (*Information Systems Security Assessment Framework*), OWASP (*Open Web Application Security Project*), PTES (*Penetration Testing Execution Standard*), dan lain sebagainya.

PT XYZ merupakan perusahaan yang bergerak dalam layanan pendidikan, seperti penyedia konsultasi, pelatihan, pengembangan kepemimpinan, riset dan pendampingan berkelanjutan. Program XYZ yang ditawarkan juga beragam, seperti *School Leadership Program*, *Financial Management Training*, *Human Capital Development*, *Marketing School Bootcamp*, *School Development Program*, *School Accelerate Program*, dan lain-lain. Sebagai *website* penyedia *workshop*, *course*, dan pelatihan, terdapat *billing details* yang berisi data pribadi saat proses *check* out pembelian *course*, sehingga keamanan *website* mereka menjadi esensial. Selain itu, pada *website* XYZ ini sebelumnya belum pernah dilakukan pengujian penetrasi. Maka pentingnya melakukan pengujian penetrasi yang berguna sebagai pendeteksi kerentanan agar tingkat keamanan *website* dapat

terus diperbarui secara berkala untuk mencegah serangan dari *hacker*(Irawadi Alwi et al., 2020).

Pada penelitian ini akan dilakukan uji penetrasi untuk mencari tahu apakah protokol keamanan SSL(*Secure Socket Layer*) berfungsi dengan baik, serta mencari celah kerentanan yang dimiliki *website* XYZ yang berbasis *WordPress*. Dalam melakukan uji penetrasi, peneliti berpedoman pada OWASP Top 10 – 2021. OWASP Top-10 ini berisikan 10 daftar teratas celah keamanan *web* yang perlu diperhatikan oleh pengembang, untuk menghindari *attacker* mengeksploitasi kerentanan tersebut(Febriana, 2022). Penelitian ini menggunakan *framework* OWASP Top 10 dikarenakan *framework* ini tergolong sederhana pada tahapannya, dan juga hanya berfokus pada risiko keamanan aplikasi *website*. Hasil dari penelitian ini adalah untuk menemukan celah keamanan pada *website* XYZ yang akan digunakan untuk menganalisis, mengevaluasi, dan mengurangi risiko kerentanan keamanan, sehingga meningkatkan keamanan *website*.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan permasalahan untuk penelitian ini adalah:

1. Apa saja langkah-langkah yang dilakukan dalam melakukan pengujian penetrasi mengacu pada *framework* OWASP Top - 10 2021 pada *website* XYZ?
2. Bagaimana cara menganalisis hasil temuan dari pengujian penetrasi serta memberikan rekomendasi perbaikan untuk peningkatan keamanan *website*?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengidentifikasi celah keamanan dalam sistem melalui pengujian penetrasi dengan mengacu *framework* OWASP Top-10 2021
2. Mampu menganalisis hasil temuan pengujian penetrasi dan memberikan rekomendasi perbaikan.

1.4 Batasan Penelitian

Adapun batasan penelitian ini adalah, sebagai berikut:

1. Aplikasi yang diuji adalah *website* dengan url Abc.id.
2. Pengujian penetrasi ini menggunakan metode *black box testing* yang berarti tanpa mengetahui struktur atau *source code website* target.
3. Pengujian menggunakan beberapa *tools* keamanan *web* dari sistem operasi Kali Linux dan Windows.
4. Pengujian penetrasi pada penelitian ini hanya menggunakan *framework* OWASP Top – 10 2021.

1.5 Manfaat Penelitian

Manfaat penelitian ini:

1. Bagi penulis, penelitian ini dapat menambah pengetahuan terkait bagaimana mengidentifikasi celah keamanan suatu *website* melalui pengujian penetrasi dengan mengacu *framework* OWASP Top -10 2021
2. Bagi perusahaan, penelitian ini bermanfaat dalam membantu mengidentfikasi celah keamananan pada sistem *website* yang digunakan, sehingga dapat membantu dalam meningkatkan tingkat keamanan data perusahaan melalui langkah mitigasi berdasarkan hasil pengujian penetrasi yang mengacu *framework* OWASP Top – 10 2021.