# BAB I PENDAHULUAN

## I.1 Latar Belakang

Dalam era digital yang semakin maju, penggunaan *Website* sebagai media utama untuk mendistribusikan informasi, berkomunikasi, dan menyediakan layanan berbasis internet semakin meningkat. *Website* tidak hanya digunakan oleh individu atau perusahaan untuk memperluas jangkauan pasar, tetapi juga oleh organisasi pemerintah dan sektor publik untuk memberikan layanan yang lebih cepat dan efisien kepada masyarakat. Seiring dengan peningkatan pemanfaatan website, ancaman keamanan siber juga meningkat secara signifikan, terutama yang berkaitan dengan eksploitasi kerentanan yang terdapat dalam aplikasi web.

Menurut data yang dirilis oleh lembaga keamanan siber global, insiden pelanggaran keamanan data yang disebabkan oleh kerentanan aplikasi web terus mengalami peningkatan setiap tahunnya. Beberapa serangan yang umum terjadi meliputi *Cross-Site Scripting* (XSS), *SQL Injection*, dan serangan *Distributed Denial of Service (DDoS)*. Serangan-serangan tersebut umumnya berawal dari kerentanan yang tidak terdeteksi atau tidak teratasi pada tahap pengembangan website. Oleh karena itu, metode yang efektif untuk mengidentifikasi dan menutup celah keamanan pada website sangatlah dibutuhkan.

*Vulnerability Assessment* dan *Penetration Testing* adalah dua pendekatan yang umum digunakan dalam mengidentifikasi, mengevaluasi, dan mengatasi kerentanan pada aplikasi web. *Vulnerability Assessment* berfungsi untuk mendeteksi dan memprioritaskan kerentanan yang ada, sementara *Penetration Testing* bertujuan untuk menguji seberapa jauh kerentanan tersebut dapat dieksploitasi oleh pihak tidak bertanggung jawab. Kombinasi dari kedua pendekatan ini dapat memberikan gambaran yang komprehensif mengenai status keamanan sebuah *website* dan langkah-langkah yang diperlukan untuk mengamankannya.

Dalam konteks ini, penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi proses *Vulnerability Assessment* dan *Penetration Testing* pada

*website* X perusahaan layanan teknologi informasi, dengan urgensi ada banyaknya orang yang keluar masuk dalam jaringain perushaan layanan teknologi informasi tersebut dikarenakan ada banyaknya vendor yang menggunakan jaringan yang sema dengan *website* X perusahaan layanan teknologi informasi tersebut. Oleh karena itu dilakukannya VAPT pada *website* X terbsebut untuk meminimalisir kerentanan yang ada,  serta memberikan rekomendasi keamanan berdasarkan hasil yang diperoleh. Melalui penelitian ini, diharapkan dapat memberikan kontribusi bagi pengembangan metode pengujian keamanan web yang lebih efektif dan membantu organisasi dalam mengelola risiko keamanan pada aplikasi web mereka.

## I.2 Perumusan Masalah

penelitian ini merumuskan beberapa pertanyaan utama sebagai berikut:

1. Bagaimana proses *Vulnerability Assessment* dan *Penetration Testing* dapat diterapkan pada *website* X perusahaan layanan teknologi informasi untuk mengidentifikasi kerentanan keamanan yang ada?
2. Jenis-jenis kerentanan apa saja yang ditemukan pada *website* X perusahaan layanan teknologi informasi berdasarkan hasil *Vulnerability Assessment* dan *Penetration Testing*?
3. Bagaimana rekomendasi perbaikan yang dapat diberikan untuk mengatasi kerentanan yang ditemukan dan meningkatkan keamanan *website* X perusahaan layanan teknologi informasi?

## I.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Menerapkan metode *Vulnerability Assessment* dan *Penetration Testing* pada *website* X Perusahaan layanan teknologi informasi untuk mengidentifikasi dan mengevaluasi kerentanan yang ada.
2. Menganalisis jenis-jenis kerentanan yang ditemukan pada *website* X perusahaan layanan teknologi informasi melalui proses *Vulnerability Assessment* dan *Penetration Testing*.

3. Memberikan rekomendasi perbaikan keamanan untuk mengatasi kerentanan yang ditemukan dan meningkatkan perlindungan terhadap potensi ancaman siber pada *website* X perusahaan layanan teknologi informasi.

## I.4 Batasan Penelitian

Adapun batasan-batasan yang ditetapkan dalam penelitian ini adalah sebagai berikut:

1. Lingkup *Website*: Penelitian ini hanya akan fokus pada *website* X perusahaan layanan teknologi informasi dan tidak mencakup aplikasi atau sistem lain yang terintegrasi di luar website tersebut.
2. Metode Pengujian: Penelitian ini akan menggunakan metode *Vulnerability Assessment* dan *Penetration Testing* untuk mengidentifikasi dan menguji kerentanan keamanan, tanpa membahas aspek lain seperti *security monitoring* atau *incident response* secara mendalam.

## I.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Bagi Pengelola Website

   Memberikan wawasan mengenai kerentanan keamanan yang ada pada *website* X perusahaan layanan teknologi informasi dan rekomendasi langkah-langkah perbaikan untuk meningkatkan tingkat keamanan dan ketahanan sistem terhadap potensi ancaman siber.
2. Bagi Pengembang Aplikasi *Web*

   Menjadi referensi bagi pengembang website dalam memahami pentingnya *Vulnerability Assessment* dan *Penetration Testing* sebagai bagian dari proses pengembangan aplikasi yang aman, serta memberikan pemahaman tentang jenis-jenis kerentanan yang sering ditemukan di aplikasi web.
3. Bagi Peneliti dan Akademisi

Sebagai kontribusi terhadap penelitian keamanan siber, khususnya yang berkaitan dengan pengujian kerentanan dan uji penetrasi pada *website*, yang dapat dijadikan dasar untuk penelitian lanjutan di bidang yang sama.