BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan berkembangnya internet dan teknologi di dunia, web membawa dampak besar bagi masyarakat di Indonesia. Web sudah menjadi kebutuhan, semua dapat mengakses web dari berbagai kalangan, mulai dari anak-anak, remaja, maupun orang dewasa dapat mengakses web seperti, berita, e-commerce, streaming music/video, dan lainnya (R. Mayasari, 2020).

Keamanan faktor yang penting untuk dipertimbangkan dalam mengakses web. Web mungkin berisi kerentanan, berbagai jenis kerentanan seperti *Injection, Broken Authentication, Session Managemen, Cross-Site Scripting*, *insecure Direct Object References, Misconfiguration, Sensitive Data Exposure, Cross-site Request Forgery* dan lain sebagainya (Patil dkk, 2016).

Website atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara dan atau gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian yang saling terkait (Rusdiana, 2019).

Menurut data dari *Hootsute* terdapat 202,6 juta pengguna internet di Indonesia pada januari tahun 2021. Dengan pengguna yang banyak tidak meminimalisasi kemungkinan terjadi kejahatan *cybercrime* yang merugikan. *Cybercrime* adalah aktivitas illegal dengan meretas berbagai data, dan mengendalikan akun orang lain, mencuri data, mengeksploitasi, dan peretasan web, bahkan menimbulkan teror. Targetnya adalah website yang memiliki tingkat keamanan rendah (Gregory, 2005).

Contoh kasus tahun 2017 *website* Tiket.com dan Citilink diretas dengan mencuri kode *booking* tiket penerbangan dan menjualnya di *facebook*, lalu *website* telkomsel diretas dengan memajang kata-kata kasar. Tahun 2020, *website* DPR RI diretas dengan mengganti nama dan menyebabkan *server down*, untuk meminimalisasi tindak kejahatan *cybercrime*, sebuah website harus diuji keamanannya (*vulnerability*). *Vulnerability Assessment* (*VA*) atau penilaian kerentanan adalah sebuah sistem informasi untuk mengevaluasi akan pentingnya keamanan informasi yang seringkali menjadi prioritas kesekian dalam sebuah institusi (Priandono, 2006).

Penelitian ini, akan dilakukan perbandingan *Vulnerability Assessment* (*VA*) antara *Acunetix WVS* dan *OWASP ZAP* yang belum pernah dilakukan sebelumnya dalam mendeteksi hasil keamanan informasi website yang ada di kampus xyz.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana melakukan perbandingan antara *software Acunetix WVS* dan *Owasp Zap?*
2. Manakah yang efektif dalam memindai *Vulnerability Assesment (VA)* antara *software Acunetix WVS* dan *Owasp Zap*?

1.3 Batasan Masalah

Mengingat banyaknya perkembangan yang bisa ditemukan dalam permasalahan yang telah didefinisikan pada rumusan masalah, maka perlu adanya batasan-batasan masalah yang jelas. Adapun batasan-batasan permasalahannya adalah sebagai berikut :

1. Uji coba dilakukan terhadap *website* kampus xyz.
2. Aspek keamanan informasi berdasarkan hasil deteksi terhadap celah kelemahan *web* yaitu : *confidentiality, integrity, availability.*

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, maka tujuan dari penelitian ini adalah:

1. Melakukan perbandingan antara *software Acunetix WVS* dan *Owasp Zap*
2. Mengetahui efektifitas kedua *software* dalam melakukan *Vulnerability Assesment (VA)* pada *website* kampus xyz untuk mengetahui mana yang lebih baik untuk digunakan.

1.5 Manfaat Penelitian

Manfaat penelitian yang dapat diperoleh dengan tujuan penelitian diatas antara lain :

1. Manfaat bagi pengembangan ilmu pengetahuan

   Penelitian ini dapat membantu menilai sejauh mana kedua *software* ini mudah digunakan oleh tim keamanan atau pengembang.

2. Manfaat bagi masyarakat

   Penelitian ini dapat memberikan pengetahuan kepada masyarakat berkaitan dengan pentingnya keamanan pada suatu *website*.