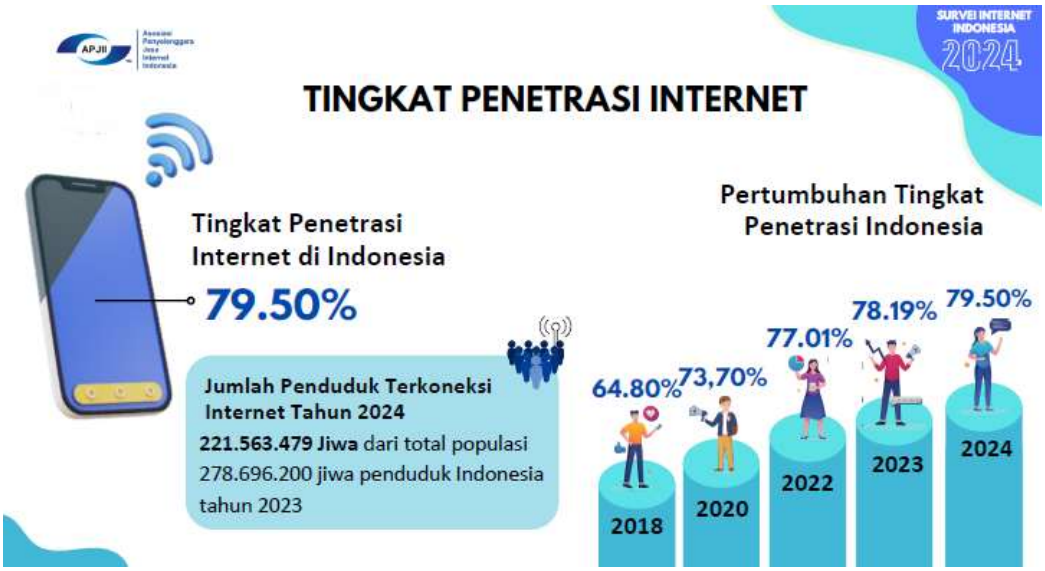
Bab 1

Pendahuluan

1.1 Latarbelakang

Dunia bisnis dan organisasi mengalami transformasi yang signifikan dari pertumbuhan pesat teknologi informasi dan sistem informasi dalam menjalankan kegiatan operasionalnya, pemanfaatan Teknologi Informasi dan Sistem Informasi (TI/SI) dapat sangat penting bagi keberlangsungan suatu organisasi (Andria, 2019). Website memberikan sejumlah keunggulan, antara lain kemampuannya untuk menyampaikan informasi, memfasilitasi interaksi, menjadi tolak ukur untuk menentukan aktif atau tidaknya kegiatan pemerintah, memungkinkan individu untuk menyampaikan aspirasinya, dan memfasilitasi promosi (Nisa, 2022).

Menurut APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) 2024 Jumlah penduduk yang terkoneksi internet pada tahun 2024 adalah 221.563.479 orang, dari 278.696.200 orang yang tinggal di Indonesia pada tahun 2023. Tingkat penetrasi internet di Indonesia pada tahun 2024 adalah 79.50%, sedangkan pada tahun 2023 adalah 78.19%. Karena pesatnya kemajuan teknologi, banyak oknum tidak bertanggung jawab yang sering disebut dengan *hacker* atau peretas mencuri data (Elanda & Buana, 2020).



Gambar 1. 1 Tingkat Penetrasi Internet Indonesia

Hacker mencari lubang di server web untuk berbagai alasan, termasuk untuk mendapatkan informasi tentang bisnis, kelompok, atau lembaga pemerintah, sehingga mereka dapat merugikan pihak lain (Hariyadi & Nastiti, 2021). Solusi pengamanan web dari gangguan atau serangan *hacker* dapat dilakukan dengan cara *selftest* yaitu pengujian yang dilakukan terhadap web server secara legal dengan aktifitas menyerupai hacker (Ghozali, 2019). Keamanan dianggap penting karena jika orang yang tidak bertanggung jawab mengakses informasi, keakuratan informasi dicurigai dan informasi menjadi tidak dapat stabil(Umar, 2019).

Keamanan informasi didefinisikan sebagai melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pengguna tidak berwenang untuk memastikan kerahasiaan, integritas, dan kemudahan penggunaan (Nurul, 2022). Keamanan informasi merupakan bagian terpenting dari sebuah instansi atau perusahaan (Tara, 2023).

Beberapa standar keamanan dapat digunakan sebagai dasar uji penetrasi, seperti ISO Standard, ISSAF, NIST CSF, dan OWASP (Tinambunan, 2024). OWASP (Open Web Application Security Project) merupakan organisasi non-profit amal yang didirikan di Amerika Serikat pada tanggal 21 April 2004. Organisasi ini memiliki misi mulia untuk meningkatkan keamanan aplikasi web dengan menyediakan berbagai sumber daya yang bermanfaat bagi individu dan organisasi di seluruh dunia. Salah satu kontribusi utama OWASP adalah pengembangan rangka kerja pengujian keamanan yang bebas digunakan oleh semua orang. Rangka kerja ini membantu para pengembang dan profesional keamanan IT untuk mengidentifikasi dan memperbaiki kelemahan keamanan dalam aplikasi web mereka, sehingga meminimalkan risiko serangan siber. Salah satu metode untuk menguji keamanan aplikasi berbasis web adalah *Open Web Application Security Project* (OWASP) (Yudiana, 2021). Analisis dan Kerangka Keamanan Siber untuk Perusahaan Teknologi Informasi, terdapat analisis terhadap kerangka kerja OWASP, ISO 27000/27001, dan NIST. Dalam analisis tersebut, OWASP terlihat unggul karena bersifat *open source* dan dapat diakses tanpa biaya besar, menjadi pilihan terbaik terutama bagi perusahaan dengan keterbatasan ekonomi (Burkan,2021).

Mengingat kompleksitas dan sensitivitas data yang dikelola dalam aplikasi e-training milik Badan Kependudukan dan Keluarga Berencana Kota Yogyakarta, potensi celah keamanan yang ada dapat menimbulkan berbagai konsekuensi serius, seperti kebocoran data pribadi pengguna, gangguan operasional layanan, dan kerusakan reputasi organisasi. Hal ini tentunya dapat menghambat efektivitas

pelaksanaan program-program e-training dan berpotensi merugikan masyarakat luas. Oleh karena itu, perlu dilakukan penelitian yang mendalam untuk menganalisis keamanan web aplikasi e-training tersebut secara menyeluruh. Penelitian ini diharapkan dapat mengidentifikasi celah-celah keamanan yang ada, menentukan tingkat keparahannya, dan merekomendasikan solusi yang tepat untuk memperbaikinya. Dengan demikian, keamanan web aplikasi e-training dapat terjamin dan pengguna dapat memanfaatkan layanan ini dengan aman dan nyaman. Metode yang digunakan adalah *Penetration Testing* dan *Vulnerability Assessment*, yang bertujuan untuk menemukan dan mengevaluasi celah keamanan pada aplikasi web. Kedua metode ini digunakan untuk memastikan sistem dan aplikasi web terlindungi dari serangan pihak yang tidak bertanggung jawab. Kombinasi dari *Penetration Testing* dan *Vulnerability Assessment* dapat memberikan gambaran yang komprehensif tentang keamanan aplikasi web dan membantu pengembang untuk memperbaiki celah keamanan yang ditemukan.

1.2 Identifikasi Masalah

Tahapan identifikasi masalah, mencari instansi yang akan diambil sebagai studi pembelajaran. Setelah menetapkan Badan Kependudukan dan Keluarga Berencana Nasional (BKKBN) kota yogyakarta sebagai studi pembelajaran dilakukan peninjauan masalah yaitu :

(a) Evaluasi keamanan belum dilakukan setelah pembaruan pihak litbang terhadap website E-Training BKKBN kota Yogyakarta yang dapat menimbulkan gangguan alur kerja dan keamanan website.

(b) Masih ditemukan celah keamanan (*vulnerability*) pada website E-Training setelah dilakukan analisis menggunakan OWASP ZAP.

(c) Perlunya kerangka strandarisasi keamanan informasi dalam melakukan analisis kerentanan sistem informasi pada aplikasi web.

1.3 Ruanglingkup

Berdasarkan latar belakang yang diuraikan, maka diberikan batasan masalah yaitu:

(a) Target melakukan analisis keamanan sistem informasi, yaitu etraining.latbangdjogja.web.id untuk memahami celah keamanan pada sistem informasi.

(b) Melakukan analisis celah keamanan dengan pemindai kerentanan menggunakan OWASP ZAP manual ataupun automasi.

1.4 Rumusan Masalah

Setelah masalah diidentifikasi dan dibatasi masalah diatas dapat dirumuskan masalah sebagai berikut :

(a) Bagaimana melakukan *vulnerability assessment* dan penetrasi testing dalam menemukan celah keamanan pada sistem informasi *etraining.latbangdjogja.web.id* sebagai langkah awal dalam melindungi tingkat keamanan website ?

(b) Bagaimana membuat mitigasi analisis menggunakan *Open Web Application Security Project* (OWASP) Top 10 tahun 2024 pada sistem informasi ?

1.5 Tujuan Penelitian

Tujuan dari penelitian sebagai berikut :

(a) Melakukan *vulnerability assessment* dan *penetrasi testing* terhadap sistem informasi menggunakan *Web Security Testing Guide* (WTSG).

(b) Membuat mitigasi terhadap setiap celah kerentanan menggunakan Open Web Application Security Project Top 10 tahun 2021.

1.6 Manfaat Penelitian

Manfaat penelitian sebagai berikut :

(a) Memberikan hasil celah keamanan dengan menggunakan *framework Open Web Application Security Project* (OWASP) sebagai acuan untuk menganalisis sistem informasi.

(b) Memberikan hasil mitigasi terhadap kerentanan keamanan dengan menggunakan *framework Open Web Application Security Project (OWASP)* sebagai evaluasi kerentanan sistem informasi.

(c) Memberikan kontribusi untuk mengoptimalkan kinerja, pemeliharaan, dan pengujian website dengan membantu meningkatkan keamanan dan penangan.