

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Website telah menjadi salah satu elemen krusial dalam berbagai aspek kehidupan modern, mulai dari bisnis, pendidikan, hingga layanan publik. Keberadaan website memungkinkan pengguna untuk mengakses informasi dan layanan secara cepat dan efisien. Namun, seiring dengan meningkatnya ketergantungan pada website, ancaman keamanan juga semakin kompleks. Serangan seperti *SQL Injection*, *Cross-Site Scripting (XSS)*, dan *Distributed Denial of Service (DDoS)* menjadi tantangan serius yang dapat mengganggu operasional website dan membahayakan data pengguna.

Keamanan website menjadi aspek penting yang harus diperhatikan dalam pengembangan sistem berbasis web. Pengujian keamanan secara berkala, termasuk *vulnerability assessment (VA)*, menjadi langkah preventif untuk mendeteksi dan memperbaiki celah keamanan sebelum dimanfaatkan oleh pihak tidak bertanggung jawab. Secara standar, proses pengujian VA mencakup beberapa tahapan penting, seperti *Preparation*, *Scanning* dan *Reporting* (Shawheen, 2025).

Contoh alat bantu seperti *OpenVAS*, *Acunetix*, dan *SnIper*, meskipun sangat berguna, masih memiliki keterbatasan. Banyak alat yang kompleks dan memerlukan keahlian teknis tinggi untuk mengoperasikannya. Selain itu, kebanyakan tools ini belum terintegrasi ke dalam aplikasi mobile yang mudah diakses pengguna awam.

Rekomendasi dari kalangan komunitas keamanan siber untuk melakukan VA diantara alat bantu diatas adalah *SnIper*. *SnIper* dipilih selain sumber terbuka alasan lain karena merupakan framework *pentest* yang mengotomatisasi banyak aspek VA, termasuk *preperation*, *scanning*, hingga eksploitasi ringan. Keunggulan *SnIper* terletak pada kemampuannya untuk mengintegrasikan berbagai tools seperti *Nmap*, *Nikto*, dan *WPScan* dalam satu platform, sehingga mampu memberikan hasil *scanning* yang lebih menyeluruh dengan sekali eksekusi.

Di sisi lain, pesatnya perkembangan teknologi digital telah memberikan dampak yang signifikan terhadap keamanan siber, terutama dalam ekosistem perangkat mobile. Peningkatan penggunaan perangkat mobile untuk mengakses berbagai layanan digital turut memperbesar potensi risiko keamanan yang dapat mengancam integritas data dan privasi pengguna. Kondisi ini mendorong perlunya pengembangan alat bantu yang mampu melakukan *vulnerability assessment* untuk mendeteksi serta mengatasi potensi kerentanan keamanan secara lebih efektif.

Namun, tantangan masih ditemukan dalam implementasi alat bantu *vulnerability assessment* yang ada saat ini. Sebagian besar perangkat lunak yang tersedia masih mengandalkan antarmuka baris perintah (*command line interface* — *CLI*), yang memerlukan pemahaman teknis yang mendalam dan berpotensi menjadi hambatan bagi pengguna non-teknis dalam mengoperasikannya. Keterbatasan ini membuat alat bantu tersebut kurang inklusif dan sulit diadopsi oleh organisasi atau individu yang tidak memiliki keahlian khusus di bidang keamanan siber. Selain itu, banyak alat dirancang untuk berjalan secara optimal hanya pada sistem operasi Linux, dengan dukungan terbatas atau bahkan tidak ada sama sekali untuk platform lain seperti Android, atau iOS, yang menjadi perangkat utama pengguna saat ini.

Hasil pencarian dengan kata kunci *tools vulnerability assessment* di Google Play Store juga mengungkap bahwa hanya sedikit aplikasi yang benar-benar memenuhi standar sebagai alat *vulnerability assessment* yang andal dan komprehensif. Sebagian besar aplikasi yang ditemukan menawarkan fitur terbatas atau tidak ada yang benar-benar memakai *tools Snlper*, lebih berfokus pada pemindaian sederhana, tanpa laporan terperinci yang dibutuhkan untuk memahami kerentanan secara menyeluruh. Hal ini menunjukkan adanya kesenjangan antara kebutuhan pengguna akan alat yang mudah digunakan tetapi tetap memiliki kapabilitas tinggi, dengan solusi yang tersedia di pasaran.

Penelitian sebelumnya menunjukkan bahwa terdapat kekurangan dalam efisiensi dan aksesibilitas alat bantu *vulnerability assessment website*. Contohnya, penelitian oleh (Hariyadi dkk., 2020) mengembangkan aplikasi berbasis GUI menggunakan *Electron Framework*, namun aplikasi tersebut masih memerlukan perangkat komputer dengan spesifikasi tinggi dan belum mendukung platform

mobile secara penuh. Penelitian lain mengenai implementasi protokol *MQTT* dalam sistem *Smart Home* (Sari dkk., 2023) membuktikan bahwa penggunaan *MQTT* mampu meningkatkan keamanan dan efisiensi pengiriman data, namun aplikasi tersebut tidak mengintegrasikan pengembangan lintas platform. Sebagai respons terhadap kebutuhan untuk pengembangan yang lebih adaptif, penelitian oleh (Satrio & Wahab, 2024) menunjukkan bahwa penggunaan metode *Agile* dalam pembangunan aplikasi mobile khususnya sistem kehadiran karyawan berbasis GIS dapat mempercepat proses pengembangan, meningkatkan fleksibilitas, dan menghasilkan aplikasi yang responsif sesuai kebutuhan pengguna.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan aplikasi *mobile* yang dapat melakukan *vulnerability assessment* menggunakan Flutter dan *MQTT*. Dengan pendekatan ini, diharapkan aplikasi yang dihasilkan tidak hanya lebih mudah digunakan, tetapi juga dapat diakses di berbagai platform, sehingga meningkatkan kemudahan dalam identifikasi celah keamanan.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, permasalahan utama adalah minimnya aplikasi *vulnerability assessment* pada perangkat *mobile*. Hasil pencarian di Google Play Store menunjukkan bahwa hanya sedikit, atau bahkan tidak ada, aplikasi yang memanfaatkan *SnIper* sebagai *tools* utama.

1.3 Pertanyaan Penelitian

Penelitian ini berupaya menjawab beberapa pertanyaan utama yang menjadi dasar pengembangan solusi:

1. Bagaimana merancang dan mengembangkan aplikasi *mobile* yang mampu melakukan *vulnerability assessment* dengan target *website* yang telah di input *user*?
2. Bagaimana mengintegrasikan *SnIper* sebagai *tools* utama dalam aplikasi *mobile* untuk memperkuat proses deteksi kerentanan?
3. Bagaimana kinerja aplikasi berjalan di perangkat Android dan iOS?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk membangun sebuah aplikasi mobile lintas platform yang dapat melakukan *vulnerability assessment* dengan target *website*, menggunakan teknologi Flutter dan protokol *MQTT*. Aplikasi ini dirancang untuk memudahkan pengguna dalam mendeteksi celah keamanan tanpa perlu keahlian teknis yang mendalam, serta mengintegrasikan *SnIper* untuk meningkatkan kemudahan proses analisis keamanan.

1.5 Manfaat Hasil Penelitian

Penelitian ini diharapkan memberikan beberapa manfaat nyata bagi pengguna dan pengembang sistem keamanan website, di antaranya:

1. Memberikan solusi praktis bagi pengguna non-teknis untuk melakukan *vulnerability assessment* melalui aplikasi mobile.
2. Menghadirkan alat bantu yang mendukung berbagai *platform mobile*, sehingga pengguna tidak terbatas pada perangkat tertentu seperti Linux.
3. Mengintegrasikan *tools* seperti *SnIper* dalam aplikasi mobile, sehingga proses identifikasi kerentanan menjadi lebih mendalam dan komprehensif.

1.6 Batasan Penelitian

Agar penelitian ini terfokus dan terukur, maka ditetapkan beberapa batasan sebagai berikut:

1. Penelitian ini hanya mencakup deteksi kerentanan umum yang sesuai dengan tools yang digunakan yaitu *SnIper*.
2. Pengujian aplikasi difokuskan pada keberhasilan aplikasi dalam memproses target yang telah diinput *user* dan hasil *report* dari integrasi *SnIper*.
3. Penelitian ini terbatas hanya mencakup platform Android dan iOS.