BAB I
PENDAHULUAN

1.1. Latar Belakang

PT. Sekuriti Siber Indonesia (Nemo Security) adalah perusahaan konsultan yang fokus pada keamanan siber, khususnya layanan pengujian penetrasi, pemantauan *Security Operation Center* (SOC) dan kepatuhan terhadap standar keamanan informasi. Di era digital saat ini, aktivitas *online* telah menjadi bagian yang tak terpisahkan dari kehidupan sehari-hari, termasuk untuk kebutuhan sosial seperti penggalangan dana hingga transaksi pembelian barang dan jasa. Dalam konteks transaksi *online*, proses pengisian saldo merupakan langkah awal yang penting untuk mendukung berbagai aktivitas keuangan digital. Namun, proses ini seringkali menghadapi berbagai ancaman seperti pembobolan data dan penipuan transaksi. Untuk mengatasi masalah ini, Nemo Security memberikan solusi yang tidak hanya memperkuat keamanan tetapi juga memudahkan administrator untuk memantau dan mengelola aktivitas keuangan pengguna dengan cara yang lebih terstruktur dan efisien. Kami telah mengembangkan sistem top-up yang berbasis persetujuan admin.

Sistem top-up menggunakan persetujuan admin adalah salah satu prosedur keamanan pada transaksi digital yang diterapkan dalam website komersial. Sistem ini dibuat untuk memastikan validitas & akurasi setiap transaksi *top-up* yg dilakukan sang pengguna, sekaligus mencegah potensi penyalahgunaan atau transaksi nir sah. Pada prosedur ini, pengguna bisa mengajukan permintaan *top-up* melalui antarmuka pengguna (*user interface*) dalam *website*. Permintaan tadi meliputi jumlah saldo yang ingin ditambahkan dan bukti pembayaran yg sudah dilakukan, misalnya bukti *transfer* bank atau pembayaran digital lainnya. Setelah permohonan diajukan, sistem akan mencatat data transaksi pada basis data menggunakan status "menunggu persetujuan admin."

Top ten OWASP ASVS (*Open Web Application Security Project Application Security Verification Standard*) dipilih sebagai dasar pengujian keamanan sistem top-up karena sistem memuat berbagai komponen yang rentan terhadap ancaman keamanan aplikasi. Proses *top-up* yang melibatkan memasukkan data pengguna, memverifikasi bukti pembayaran, dan persetujuan admin atas transaksi dapat dieksploitasi jika kerentanan tidak diidentifikasi dan diatasi dengan benar. OWASP *Top Ten* memungkinkan fokus pengujian pada ancaman yang paling relevan, termasuk: Injeksi (yang dapat terjadi jika data masukan tidak divalidasi dengan benar), atau Kebocoran Data Sensitif (yang dapat membahayakan keamanan pembayaran dan informasi identitas pengguna). Selain itu, OWASP memberikan pendekatan berbasis risiko yang memungkinkan pengembang untuk memprioritaskan ancaman yang memiliki dampak terbesar pada sistem mereka, termasuk: Kegagalan otentikasi dan kesalahan konfigurasi keamanan dapat membuka lubang yang dapat dimanipulasi oleh penyerang untuk melakukan transaksi atau mengakses dasbor administratif. Dengan demikian, *Top Ten* OWASP memberikan kerangka kerja komprehensif untuk memastikan sistem top-up yang disetujui admin dikembangkan dan diuji dengan aman sesuai dengan standar industri. Dengan memahami dan mengatasi kerentanan ini, sistem top-up dapat dirancang untuk memberikan perlindungan yang lebih kuat terhadap ancaman keamanan siber.

Berdasarkan latar belakang diatas, laporan ini akan berfokus pada Perancangan dan Implementasi Web Aplikasi dengan Fitur *Top-Up* Saldo Berbasis Persetujuan Admin Menggunakan OWASP ASVS untuk Pengujian Keamanan mendalam mengenai langkah-langkah yang harus diambil dalam mengelola kerentanan teknis, serta dampak dari implementasi ini terhadap kesiapan *website* komersial. Dengan terpenuhinya standar OWASP ASVS, maka keamanan sistem *top-up* di web aplikasi akan lebih terjamin.

1.2. Deskripsi Pekerjaan

Selama menjalani program magang, saya berfokus pada berbagai tugas yang berkaitan dengan keamanan siber, mencakup pemantauan, pelaporan, serta pengujian kerentanan pada aplikasi web. Lingkup pekerjaan yang saya lakukan adalah sebagai berikut:

1. Monitoring Aktivitas Log di SIEM Wazuh

   Melakukan pemantauan aktivitas log client secara berkala melalui platform SIEM(*Security Information and Event Management*) Wazuh untuk mengidentifikasi anomali atau potensi ancaman keamanan. Tugas ini melibatkan analisis log, penilaian pola akses, serta deteksi aktivitas yang tidak wajar untuk mendukung upaya pencegahan dini terhadap ancaman siber.

2. Pembuatan Laporan Log Mencurigakan

   Menyusun laporan terperinci jika ditemukan alert yang mencurigakan pada log SIEM Wazuh. Proses ini mencakup analisis penyebab *alert*, dampak potensial, serta rekomendasi tindakan mitigasi. Laporan ini menjadi referensi penting bagi tim keamanan untuk mengambil langkah proaktif.

3. Pembelajaran dan Praktik *Penetration Testing*

   Mendalami teori dan teknik penetration testing untuk mengidentifikasi kerentanan keamanan pada aplikasi web. Aktivitas ini meliputi eksplorasi alat-alat pengujian, seperti OWASP ZAP dan *Burp Suite*, serta pemahaman kerangka kerja pengujian seperti OWASP ASVS untuk memastikan pengujian dilakukan secara terstandar.

4. Pelaksanaan Penetration Testing pada Aplikasi Web

   Mengaplikasikan metode penetration testing pada aplikasi web untuk mengidentifikasi potensi kerentanan, seperti injeksi SQL, XSS, atau kelemahan autentikasi. Proses ini mencakup tahap perencanaan, eksploitasi kerentanan, hingga dokumentasi hasil

pengujian dan rekomendasi perbaikan yang mendetail untuk pengembang aplikasi.

Dalam lingkup magang ini mencerminkan kompleksitas yang menuntut ketelitian, kemampuan analisis, serta pemahaman mendalam terkait keamanan siber. Setiap tugas dilakukan secara kolaboratif dengan tim untuk memastikan sistem yang dikelola tetap aman dan sesuai dengan standar keamanan yang berlaku.

1.3. Tujuan

Tujuan dari implementasi yang di hasilkan bisa mendukung proses transaksi keuangan secara aman, terstruktur, & sinkron kebutuhan pengguna. Sistem ini didesain buat memastikan bahwa setiap transaksi yg dilakukan melalui pelaksanaan bisa dikontrol & diverifikasi sang admin, sebagai akibatnya meminimalkan risiko kesalahan atau penyalahgunaan yg bisa terjadi selama proses *top-up*.

1.4. Manfaat

Pengimplementasian dan pengujian keamanan berstandar OWASP ASVS pada sistem *top-up* berbasis persetujuan admin memberikan manfaat yang signifikan dalam mendukung keberhasilan operasional web aplikasi sekaligus melindungi kepentingan pengguna dan bisnis, sistem yang dirancang ini meningkatkan keandalan transaksi dan memastikan keamanan data, yang pada akhirnya memberikan nilai tambahan baik bagi pengguna maupun pengelola aplikasi.

.