BAB I
PENDAHULUAN

1.1 Latar Belakang

PT. Sekuriti Siber Indonesia (Nemo Security) merupakan perusahaan konsultan yang bergerak di bidang keamanan siber dengan spesialisasi pada layanan pengujian penetrasi (*penetration testing*), pemantauan *Security Operation Center* (SOC), dan kepatuhan terhadap standar keamanan informasi. Di era digital saat ini, platform digital seperti forum diskusi online menjadi bagian integral dalam aktivitas sosial dan profesional, memberikan ruang bagi pengguna untuk bertukar informasi, berdiskusi, serta menyampaikan opini secara terbuka.

Namun, keterbukaan akses pada forum diskusi juga meningkatkan potensi terhadap berbagai ancaman keamanan siber, termasuk penyusupan data, manipulasi konten, dan eksploitasi sistem melalui teknik serangan umum seperti *SQL Injection* dan *Cross-Site Scripting (XSS)*. Kedua teknik ini tergolong sebagai serangan siber yang umum digunakan dan memiliki dampak signifikan terhadap integritas dan kerahasiaan sistem informasi.

Dalam konteks tersebut, Nemo Security melakukan pengujian penetrasi terhadap sebuah aplikasi web forum diskusi untuk mengidentifikasi potensi kerentanan terhadap dua teknik serangan tersebut. Proses pengujian didasarkan pada kerangka kerja *OWASP Top Ten* dan *OWASP Application Security Verification Standard (ASVS)* yang digunakan sebagai acuan dalam mengidentifikasi celah keamanan kritis pada aplikasi web.

Pengujian menggunakan teknik *SQL Injection* dilakukan dengan mengevaluasi bagaimana sistem merespons masukan pengguna pada fitur-fitur tertentu seperti autentikasi login, pencarian data, serta interaksi lain yang melibatkan permintaan ke basis data. Jika sistem gagal dalam melakukan validasi input, perintah *SQL* berbahaya dapat disisipkan oleh penyerang untuk mengakses, memodifikasi, atau menghapus data dalam basis data.

Di sisi lain, pengujian *Cross-Site Scripting (XSS)* dilakukan untuk menguji sejauh mana sistem mengelola konten yang dimasukkan oleh pengguna, seperti pada kolom komentar dan postingan. Dalam kondisi tertentu, skrip berbahaya dapat disisipkan dan dijalankan di sisi pengguna lain apabila tidak terdapat mekanisme pemrosesan input yang aman, sehingga membuka peluang terhadap aksi pencurian sesi, manipulasi tampilan, dan penyalahgunaan fungsionalitas antarmuka.

Hasil dari pengujian menunjukkan adanya beberapa titik kerentanan dalam sistem forum diskusi yang dapat dieksploitasi melalui teknik *SQL Injection* dan *XSS*. Temuan ini memberikan gambaran mengenai potensi risiko yang dapat terjadi apabila aplikasi tidak dirancang dengan memperhatikan aspek keamanan dalam setiap tahap pengembangannya.

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 *Security Information and Event Management (SIEM)* 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 *SQL injection*, *Cross-Site Scripting*, atau kelemahan autentikasi. Proses ini mencakup tahap perencanaan, eksploitasi kerentanan, hingga dokumentasi hasil pengujian.

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 pengujian penetrasi ini adalah untuk mengevaluasi tingkat keamanan pada sistem forum diskusi terhadap ancaman siber yang umum terjadi, khususnya serangan *SQL Injection* dan *Cross-Site Scripting (XSS)*. Melalui pendekatan terstruktur yang mengacu pada standar *OWASP ASVS*, pengujian ini dilakukan guna mengidentifikasi potensi celah keamanan yang dapat dimanfaatkan oleh pihak tidak berwenang. Evaluasi ini bertujuan memberikan gambaran menyeluruh mengenai kondisi keamanan aplikasi web forum diskusi berdasarkan skenario serangan yang realistis.

1.4 Manfaat

Pengujian penetrasi yang dilakukan berdasarkan standar *OWASP ASVS* memberikan sejumlah manfaat penting dalam konteks identifikasi dan pemetaan risiko keamanan siber pada sistem forum diskusi. Beberapa manfaat yang diperoleh dari proses ini meliputi:

1. Mengidentifikasi titik-titik kerentanan pada sistem yang berpotensi dieksploitasi melalui teknik *SQL Injection* dan *Cross-Site Scripting (XSS)*.
2. Memberikan data teknis terkait respons sistem terhadap input berbahaya yang dikirim melalui berbagai fitur forum, seperti login, pencarian, dan kolom komentar.
3. Menyediakan informasi faktual mengenai kemungkinan akses tidak sah terhadap data pengguna melalui manipulasi input.
4. Memberikan dasar analisis mengenai seberapa besar dampak dari serangan tertentu terhadap aspek kerahasiaan, integritas, dan ketersediaan layanan forum.

Dengan hasil pengujian ini, dapat diperoleh pemahaman yang lebih dalam mengenai tingkat risiko yang dihadapi oleh sistem forum diskusi dalam konteks ancaman siber yang umum terjadi.