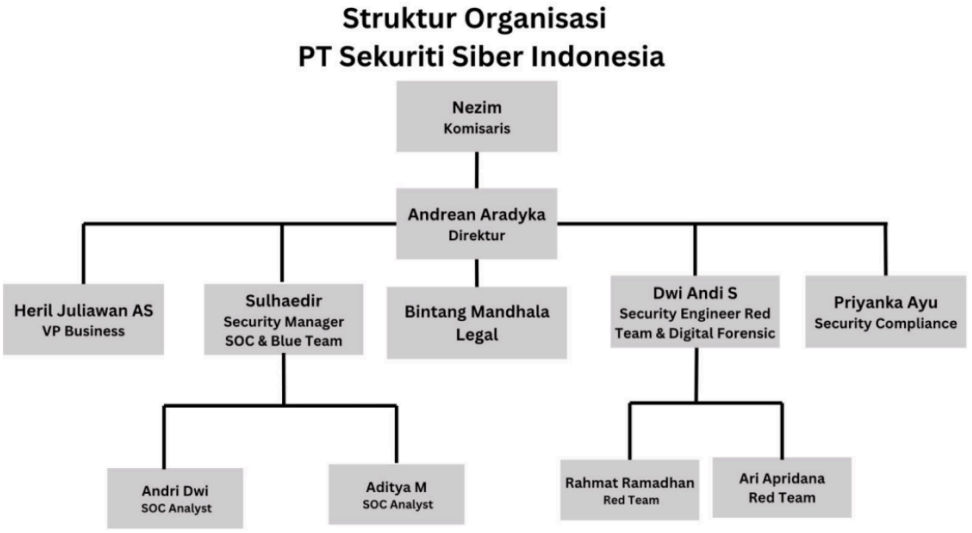
BAB II
PT. SEKURITI SIBER INDONESIA

PT Sekuriti Siber Indonesia (Nemo Security) merupakan perusahaan konsultan keamanan siber yang berdiri sejak tahun 2018. Perusahaan ini menyediakan layanan di bidang keamanan digital, termasuk pengujian penetrasi, penilaian kerentanan, pemantauan keamanan SIEM (Security Information and Event Management), respon insiden, forensik digital, serta pelatihan keamanan. Selain itu, perusahaan juga membantu klien dalam memenuhi standar keamanan internasional seperti ISO 27001(Information Security Management System) dan PCI DSS (Payment Card Industry Data Security Standard), serta memperhatikan aspek privasi data. Fokus utama perusahaan adalah melindungi aplikasi yang digunakan secara luas dari berbagai potensi kerentanan siber.

2.1. Struktur Organisasi

Setelah dibentuk oleh Nemo Security pada tahun 2018, struktur organisasi di bawah ini disahkan secara resmi menjadi PT. Sekuriti Siber Indonesia pada tahun 2018, dengan susunan organisasi sebagai berikut:



Gambar 2. 1 Struktur Organisasi

Direktur bertanggung jawab atas keseluruhan operasional dan strategi perusahaan. Semua divisi melapor kepada direktur, dan tiap divisi memiliki fungsi dan tanggung jawab spesifik untuk mendukung tujuan perusahaan. termasuk divisi Security Engineering Red Team/Pentester. Manajer Red Team/Pentester melapor langsung kepada direktur. Manajer ini bertanggung jawab atas semua aktivitas yang dilakukan oleh tim security engineering red team/pentester. Tim ini terdiri dari profesional yang memiliki keahlian dalam melakukan pengujian penetrasi (penetration testing) dan simulasi serangan (red teaming) Mereka memastikan bahwa tim bekerja sesuai dengan standar keamanan yang ditetapkan oleh perusahaan dan industri.

2.2. Visi dan Misi

Visi & misi yang dipegang teguh oleh PT. Siber Sekuriti Indonesia yang merupakan landasan untuk menjalankan organisasi secara menyeluruh dan terstruktur serta memiliki tujuan yang jelas, disebutkan sebagai berikut:

2.2.1 Visi

“menjadi perusahaan keamanan siber yang diakui secara global, meningkatkan standar keamanan siber di Indonesia, dan membina generasi baru yang terampil dan berintegritas.”

2.2.2 Misi

1. Keamanan siber berkualitas tinggi: memberikan solusi inovatif untuk melindungi dari ancaman siber.
2. Meningkatkan kesadaran: memberikan edukasi dan lokakarya gratis untuk meningkatkan pengetahuan tentang keamanan siber.
3. Mengembangkan bakat: menawarkan peluang karir melalui magang dan bimbingan.
4. Kemitraan strategis: bekerja sama dengan pemerintah dan organisasi untuk memperkuat keamanan siber.
5. Etika dan integritas: menjaga transparansi, etika, dan kepatuhan dalam semua operasi.

2.3. Lingkup Pekerjaan

PT. Sekuriti Siber Indonesia merupakan perusahaan yang bergerak di bidang keamanan siber, dengan layanan pengujian penetrasi, operasional Security Operation Center (SOC), serta edukasi keamanan informasi. Dalam proyek tugas akhir ini, penulis melakukan pengujian keamanan pada aplikasi web *G-Entry* sebagai media pembelajaran, dengan fokus pada identifikasi kerentanan *SQL Injection* dan *Cross-Site Scripting* (XSS) yang termasuk dalam kategori OWASP Top 10.

2.3.1. Web Aplikasi G-Entry

Aplikasi *G-Entry* yaitu sistem buku tamu berbasis web yang digunakan untuk mendukung proses pencatatan interaksi tamu atau pengguna secara daring. Aplikasi ini menyediakan fitur registrasi, login, pengisian form buku tamu, serta pengelolaan data pesan yang dapat diakses oleh pengguna dan admin sesuai hak aksesnya. Pengujian keamanan dalam penelitian ini difokuskan pada input form yang langsung terhubung dengan basis data tanpa mekanisme validasi input yang memadai. Hal ini bertujuan untuk mengidentifikasi potensi kerentanan, khususnya terhadap serangan *SQL Injection* dan *Cross-Site Scripting* (XSS) berdasarkan kategori OWASP Top 10.

2.3.2 Batasan Penelitian

Penelitian ini hanya terbatas pada web aplikasi *G-Entry*, tidak mencakup sistem atau aplikasi PT. Siber Sekuriti Indonesia. Fokus penelitian ini adalah pada pengujian dua jenis kerentanan utama, yaitu *SQL Injection* (SQLi), *Cross-Site Scripting* (XSS). Penelitian ini tidak melibatkan eksploitasi lanjutan seperti privilege escalation atau post-exploitation, serta tidak mencakup proses perbaikan terhadap aplikasi web yang diuji.

2.3.3 Metodologi Pengujian

Pengujian dilakukan menggunakan pendekatan greybox testing, di mana penulis memiliki akun pengguna aplikasi tetapi tidak memiliki akses penuh ke kode sumber. Proses pengujian mengacu pada standar OWASP Top 10,

menggunakan alat bantu seperti Burp Suite untuk memonitor dan memodifikasi request HTTP, serta SQLMap untuk membuktikan eksploitasi SQL Injection.

Tahapan pengujian meliputi identifikasi titik input rentan, penyusunan payload, eksekusi eksploitasi, serta pendokumentasian hasil dan rekomendasi mitigasi.

2.3.5 Analisis dan Dokumentasi Awal

Pada tahap awal, penulis mempelajari struktur aplikasi secara menyeluruh dan mengidentifikasi fitur-fitur penting seperti login, pendaftaran akun, serta formulir pengisian pesan. Informasi yang diperoleh kemudian dijadikan acuan untuk menyusun dokumen awal serta merancang skenario pengujian yang akan dilakukan.

2.3.6 Perencanaan dan Implementasi Pengujian

Tahapan ini berfokus pada pelaksanaan skenario pengujian menggunakan payload khusus dan tools seperti Burp Suite untuk intercept request. Parameter input diuji dengan memodifikasi data agar dapat memicu respon anomali, error basis data, atau eksekusi skrip di sisi klien.

2.3.7 Pengujian dan Validasi Hasil

Setelah eksploitasi dijalankan, hasil pengujian di validasi dengan memastikan bahwa payload benar-benar memicu celah keamanan, dibuktikan dengan error database, bypass login, dump data user, atau munculnya pop-up XSS. Semua bukti dikumpulkan sebagai dasar evaluasi.

2.3.8 Penyusunan Rekomendasi dan Pelaporan

Sebagai tahap akhir, penulis menyusun laporan hasil temuan secara sistematis, lengkap dengan dokumentasi tangkapan layar. Rekomendasi teknis disusun untuk mendukung penguatan sistem keamanan agar celah yang sama dapat diminimalkan pada pengembangan selanjutnya.