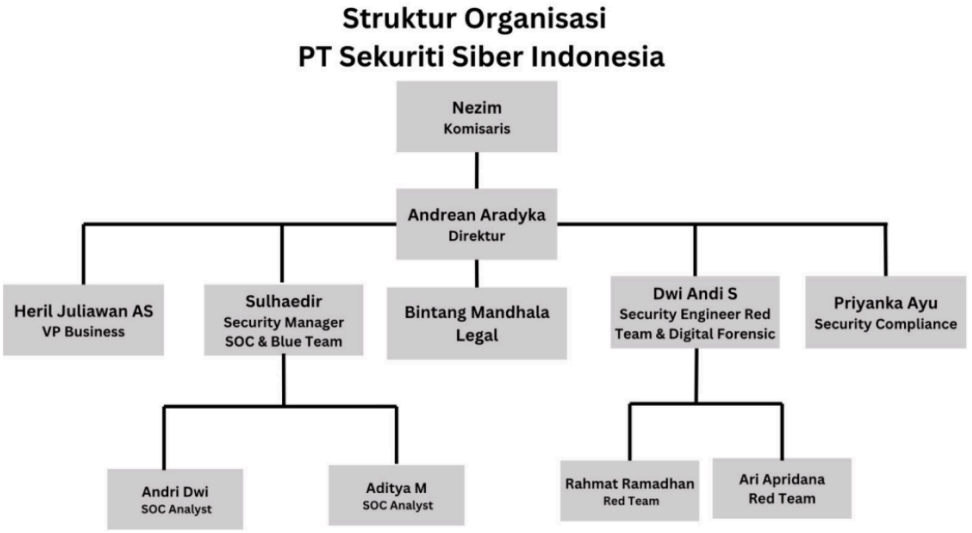
BAB II

PT. SEKURITI SIBER INDONESIA

PT Sekuriti Siber Indonesia adalah perusahaan yang bergerak di bidang keamanan siber dan teknologi informasi, yang berfokus pada layanan pengujian keamanan sistem, pelatihan keamanan digital, serta pengembangan solusi keamanan berbasis teknologi. Perusahaan ini memiliki visi untuk meningkatkan kesadaran dan ketahanan keamanan siber di Indonesia melalui pendekatan edukatif dan teknis yang terstruktur.

2.1 Struktur Organisasi

Struktur organisasi pada gambar 2.1 ini dibentuk oleh Nemo Security pada tahun 2017, dan disahkan secara aklimasi 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 Misi

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

Visi

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

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 berfokus pada pengujian keamanan siber berbasis standar nasional maupun internasional. Dalam proyek tugas akhir ini, penulis melakukan pengujian keamanan pada aplikasi web To-Do List sebagai studi pembelajaran, dengan fokus terhadap

dua jenis kerentanan yang termasuk dalam dalam OWASP Top 10 2021, yaitu SQL Injection dan Cross Site Scripting (XSS).

2.3.1 Batasan Penelitian

a. Penelitian ini hanya dilakukan pada satu aplikasi, yaitu To-Do List, dan tidak mencakup sistem atau aplikasi lain milik PT. Sekuriti Siber Indonesia
b. Fokus penelitian ini terbatas pada identifikasi kerentanan teknis berupa SQL Injection dan XSS, tanpa mencakup aspek kebijakan manajemen keamanan informasi.
c. Pengujian tidak melibatkan eksploitasi lanjutan seperti privilege escalation, pengujian jaringan, atau pengujian terhadap sistem server lainnya.
d. Penelitian dilakukan dalam lingkungan lokal/developments, bukan pada sistem produksi aktif.

2.3.2 Metodologi Pengujian

a. Pengujian ini dilakukan menggunakan pendekatan greybox testing, dimana penulis memiliki akses sebagai pengguna aplikasi namun tidak memiliki informasi kode sumber penuh.
b. Proses pengujian mengacu pada OWASP Top 10, dengan memanfaatkan tools seperti Burp Suite untuk intercept dan memodifikasi HTTP.
c. Penelitian dilakukan dalam tiga tahap utama yaitu identifikasi titik input, eksploitasi menggunakan payload, dokumentasi dan penyusunan rekomendasi mitigasi.

2.4 Deskripsi Pengujian

Dalam Pelaksanaan penelitian ini, penulis memiliki tanggung jawab utama untuk merancang dan melaksanakan proses pengujian keamanan terhadap aplikasi web To-Do List. Fokus utama pekerjaan adalah mengidentifikasi dan mengevaluasi kerentanan keamanan berdasarkan kategori SQL Injection dan Cross Site Scripting (XSS) dari OWASP Top 10 2021. Rincian pekerjaan dijelaskan sebagai berikut.

2.4.1 Analisis dan Dokumentasi Awal

Tahap awal ini dilakukan untuk memahami struktur aplikasi dan mengidentifikasi fitur-fitur yang akan diuji. Informasi yang dikumpulkan digunakan sebagai dasar penyusunan dokumentasi awal dan perencanaan pengujian.

2.4.2 Perencanaan dan Implementasi Pengujian

Tahapan ini berfokus pada pelaksanaan skenario pengujian keamanan dengan menyiapkan payload teknik eksploitasi, dan alat bantu seperti Burp Suite yang digunakan untuk menguji input dengan respon sistem.

2.4.3 Pengujian dan Validasi Hasil

Setelah pengujian dilakukan, hasilnya validasi untuk memastikan bahwa temuan benar-benar merupakan celah keamanan. Bukti eksploitasi dikumpulkan sebagai bahan evaluasi dan pelaporan.

2.4.4 Penyusunan Rekomendasi dan Pelaporan

Setelah semua tahapan pengujian selesai, dilakukan penyusunan laporan hasil pengujian dalam format yang sistematis serta pemberian saran mitigasi berdasarkan temuan yang diperoleh.