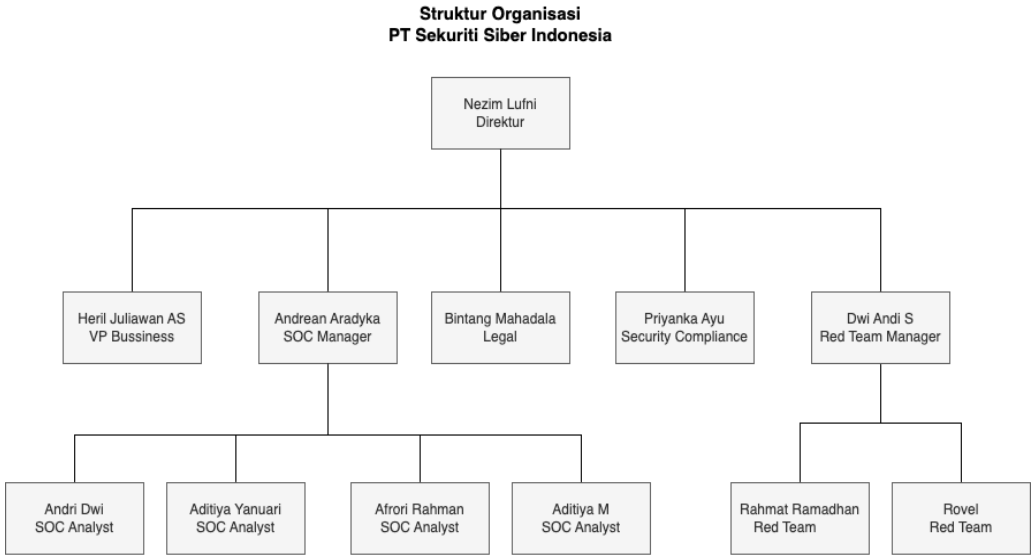
BAB II
PROFIL INSTANSI TEMPAT MAGANG

2.1 Struktur Organisasi

Struktur organisasi di bawah ini dibentuk oleh Nemo Security pada tahun 2017, dan disahkan secara aklamasi menjadi PT. Siber sekuriti Indonesia pada tahun 2018, dengan susunan organisasi sebagai berikut:



Gambar 2.1 Struktur organisasi PT SSI

Direktur bertanggung jawab atas keseluruhan operasional dan strategi perusahaan, dengan semua divisi melapor langsung kepadanya, termasuk Divisi *Security Engineering Red Team/Pentester*. Divisi ini dipimpin oleh seorang manajer yang mengawasi kegiatan pengujian penetrasi dan simulasi serangan, serta memastikan tim bekerja sesuai standar keamanan perusahaan dan industri.

PT. Siber Sekuriti Indonesia memiliki visi untuk menjadi perusahaan keamanan siber yang diakui secara global, meningkatkan standar keamanan siber di Indonesia, dan membina generasi baru yang terampil dan berintegritas. Misi

perusahaan meliputi pemberian solusi keamanan siber inovatif dan berkualitas tinggi, meningkatkan kesadaran melalui edukasi dan lokakarya, mengembangkan bakat melalui magang dan bimbingan, membangun kemitraan strategis dengan pemerintah dan organisasi, serta menjaga etika, transparansi, dan kepatuhan dalam seluruh kegiatan operasionalnya.

2.2 Lingkup Pekerjaan

PT. Sekuriti Siber Indonesia memiliki tanggung jawab untuk meningkatkan keamanan pada setiap teknologi informasi yang digunakan, dengan mengacu pada standar nasional maupun internasional. Dalam proyek ini, fokus utama adalah pada pengujian penetrasi terhadap sistem keamanan web forum diskusi, khususnya dalam mengidentifikasi dan mengevaluasi kerentanan terhadap *SQL Injection* dan *Cross-Site Scripting* (*XSS*).

Lingkup pekerjaan proyek ini mencakup pengujian keamanan terhadap antarmuka forum dan mekanisme input pengguna yang rawan terhadap eksploitasi, dengan mengacu pada standar *OWASP ASVS*.

2.2.1 Web Aplikasi Forum Diskusi

Web aplikasi ini merupakan platform diskusi daring yang digunakan oleh pengguna untuk membuat, membaca, dan membalas topik diskusi. Fitur utama melibatkan interaksi berbasis input pengguna, seperti form login, pencarian, pengiriman komentar, dan pengelolaan akun.

Pengujian keamanan difokuskan pada identifikasi potensi kerentanan *SQL Injection* dan *Cross-Site Scripting*, yang dapat terjadi apabila input pengguna tidak ditangani dengan benar. Tujuannya adalah untuk memastikan sistem aman dari eksploitasi yang dapat merusak integritas data atau membahayakan pengguna lain.

2.2.2 Batasan Penelitian

Penelitian ini terbatas hanya pada web aplikasi forum diskusi dan tidak mencakup aplikasi atau sistem lain yang digunakan oleh PT. Sekuriti Siber

Indonesia. Fokus penelitian adalah pada analisis kerentanan teknis, khususnya *SQL Injection* dan *Cross-Site Scripting*, tanpa mencakup aspek manajemen kebijakan atau prosedur keamanan informasi. Penelitian ini tidak mencakup pengujian fisik, jaringan, atau integrasi eksternal di luar ruang lingkup aplikasi forum diskusi.

2.3 Pengertian SQL Injection dan XSS

SQL Injection (SQLi) adalah teknik serangan yang memanfaatkan celah pada sistem basis data suatu aplikasi, di mana penyerang menyisipkan perintah SQL berbahaya melalui input pengguna. Tujuannya adalah untuk memanipulasi, mengambil, mengubah, atau menghapus data tanpa otorisasi yang sah. SQL Injection sering terjadi karena kurangnya validasi input dan penggunaan query yang tidak aman.

Cross-Site Scripting (XSS) adalah serangan yang memungkinkan penyerang menyisipkan skrip berbahaya, biasanya berupa *JavaScript*, ke dalam halaman web yang dilihat oleh pengguna lain. XSS dapat digunakan untuk mencuri data sensitif seperti *cookie, session*, atau mengarahkan pengguna ke situs berbahaya. Serangan ini umumnya disebabkan oleh tidak adanya proses sanitasi dan encoding pada input atau output aplikasi.

2.4 Burp Suite

Burp Suite adalah alat pengujian keamanan aplikasi web yang dikembangkan oleh PortSwigger Ltd, sebuah perusahaan keamanan siber yang berbasis di Inggris. Alat ini digunakan secara luas oleh profesional keamanan, *pentester*, dan *bug bounty hunter* untuk mengidentifikasi serta mengeksploitasi kerentanan pada aplikasi web.

Fungsi utama *Burp Suite* adalah untuk memfasilitasi proses pengujian keamanan dengan mengintersepsi, memodifikasi, dan menganalisis lalu lintas *HTTPS* antara browser dan server. *Burp Suite* memiliki berbagai fitur, di antaranya:

1. Proxy: Mengintersepsi dan memodifikasi *request/response* antara client dan server.
2. Repeater: Mengirim kembali permintaan *HTTP* dengan modifikasi untuk pengujian manual.
3. Intruder: Melakukan pengujian otomatis seperti *brute force* dan *fuzzing*.
4. Scanner (tersedia di versi profesional): Memindai kerentanan secara otomatis.
5. Sequencer: Menganalisis kekuatan entropi token atau *session ID*.
6. Decoder: *Meng-encode* atau *decode* data dalam berbagai format.
7. Comparer: Membandingkan dua data untuk melihat perbedaan.

Burp Suite tersedia dalam tiga versi:

1. *Community Edition* – versi gratis dengan fitur terbatas.
2. *Professional Edition* – versi berbayar dengan fitur lengkap, termasuk scanner otomatis.
3. *Enterprise Edition* – versi untuk otomatisasi pengujian skala besar.

Dengan kemampuannya yang fleksibel, Burp Suite menjadi salah satu alat utama dalam proses *penetration testing* aplikasi web.

2.5 Metodologi Pengujian

Metode *Greybox Testing* digunakan untuk mengidentifikasi kerentanan dari sudut pandang pengguna internal terbatas, dengan akses sebagian terhadap struktur sistem. Pengujian dilakukan berdasarkan kerangka kerja *OWASP ASVS* untuk memastikan bahwa aplikasi web memenuhi standar keamanan industri.