# BAB II
# PROFIL INSTANSI TEMPAT MAGANG

Profil instansi dari perusahaan Nemo Security, di jelaskan dalam bentuk struktur organisasi seperti di bawah ini:

## 2.1 Struktur Organisasi

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


**Gambar 2.1 Struktur Organisasi**

Struktur organisasi di atas di jalankan oleh komisaris yang memimpin dengan membawahi direktur yang bertanggung jawab terhadap beberapa divisi yang dimiliki yaitu : *VP Business, Security Manager SOC, Legal, Security Engineer Red Team & Digital Forensic, dan Security Compliance.* Dimana setiap divisi memiliki tugas dan tanggung jawabnya masing-masing untuk menjalankan organisasi.

## 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 :

### 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 mempunyai tugas untuk meningkatkan keamanan pada setiap teknologi informasi yang sesuai dengan standar nasional maupun internasional. Lingkup pekerjaan dalam proyek ini melibatkan sistem web aplikasi manajemen persediaan serta pengujian keamanan berdasarkan *OWASP ASVS*. Peran utama penulis dalam proyek ini mencakup:

### 2.3.1 Web Aplikasi *Inventory Management*

Web Aplikasi ini digunakan untuk melakukan *update* dan memantau pemasukan dan pengeluaran barang secara *real-time*, serta sistem ini mempermudah proses pencatatan transaksi logistik seperti barang masuk, barang keluar, dan stok akhir yang tersedia di gudang. Aplikasi inventory ini bersifat berbasis web, sehingga dapat diakses oleh pengguna dari perangkat manapun yang memiliki koneksi internet dan hak akses yang sesuai.

Karena aplikasi ini mempunyai informasi sensitif dan hal-hal penting sebuah perusahaan, maka sangat penting untuk memastikan bahwa sistem tidak memiliki celah keamanan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Oleh karena itu, web aplikasi ini dijadikan sebagai objek dalam penelitian eksplorasi *penetration testing* terhadap fitur *upload* gambar pada aplikasi web berbasis PHP.

### 2.3.2 Batasan Penelitian

a. Penelitian ini hanya terbatas pada web yang diuji yaitu *Inventory Management* yang dijelaskan diatas dan tidak mencakup aplikasi lain ataupun sistem lain yang digunakan oleh PT. Sekuriti Siber Indonesia.
b. Penelitian ini akan berfokus pada analisis kerentanan teknis yang sesuai dengan standar *OWASP ASVS*, tanpa memasukkan aspek manajemen dan kebijakan keamanan informasi.
c. Penelitian ini tidak akan melibatkan pengujian fisik, pengujian jaringan, atau integrasi dengan sistem luar.

### 2.3.3 Metodologi Pengujian

a. Metode yang digunakan yaitu *Greybox Testing.*
b. Penelitian ini terdiri dari tiga tahap: identifikasi kerentanan, eksploitasi, dan evaluasi potensi resiko yang dihasilkan.

## 2.4 Deskripsi Pengujian

Dalam pengujian penelitian ini, ada beberapa penjelasan mengenai hal apa saja yang harus diuji agar tidak terjadi kesalahan dalam pengujian sebagai berikut:

### 2.4.1 Analisis dan Dokumentasi

a. Tugas: Menganalisis dan mengumpulkan kebutuhan keamanan pengguna dan bisnis untuk sistem manajemen persediaan. Menyusun dokumen secara mendetail.
b. Tanggung jawab: Melakukan koordinasi secara efektif dengan pemilik kepentingan untuk memastikan sistem telah memenuhi standar kebutuhan.

### 2.4.2 Implementasi

a. Tugas: Mengimplementasikan Fitur yang ada pada manajemen persediaan dengan melakukan pengujian keamanan dengan standar *OWASP ASVS*.
b. Tanggung jawab: Melakukan pengujian keamanan dengan jangka waktu yang sudah ditentukan.

### 2.4.3 Pengujian dan Validasi

a. Tugas: Melakukan pengujian secara menyeluruh dan memastikan semua fitur dapat digunakan serta berfungsi dengan baik dan aman sesuai dengan standar *OWASP ASVS*.
b. Tanggung jawab: Mengelola proses uji coba keamanan.

### 2.4.4 Membuat *Report*

a. Tugas: Melakukan *report* secara terstruktur yang relevan dengan celah keamanan yang diuji.
b. Tanggung jawab: Membuat rekomendasi langkah pencegahan serta melaporkan hasil pengujian dan penelitian