BAB II
PROFIL INSTANSI

Profil instansi dari perusahaan nemo security, di jelaskan dalam bentuk struktur organisasai 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. Siber sekuriti Indonesia pada tahun 2018, dengan susunan organisasi sebagai berikut:

Gambar 2. 1 Struktur Organisasi

Gambar 2.1 Struktur Organisasi menjelaskan bahwa dijalankan oleh komisaris yang memimpin dengan membawahi direktur yang bertanggung jawab terhadap beberepa divisi yang dimiliki yaitu: *VP Bussines, Security Manager SOC, Legal, Security Engginer 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. 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.”

2.2.1. 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. Siber sekuriti Indonesia mempunyai tugas untuk meningkatkan kemanan pada setiap teknologi informasi yang sesuai dengan standar nasional maupun internasional. Lingkup pekerjaan dalam proyek ini

melibatkan sistem *top-up* dengan persetujuan admin serta pengujian keamanan berdasarkan OWASP ASVS. Peran utama penulis dalam proyek ini mencakup:

2.3.1. Web Aplikasi NemoSal

Web Aplikasi ini digunakan untuk melakukan transaksi dan memiliki fitur *top-up* saldo dengan persetujuan admin, menyimpan dan mengelola keuangan , serta mengakses data karyawan PT. Siber Sekuriti Indonesia. Pengujian keamanan difokuskan pada aspek *top-up* saldo dengan persetujuan admin. Fitur ini mencegah terjadinya penyalahgunaan saldo ilegal, serta identifikasi kerentanan berdasarkan OWASP ASVS.

2.3.2. Batasan Penelitian

1. Penelitian ini terbatas pada web aplikasi NemoSal yang disebutkan diatas dan tidak mencakup sistem atau aplikasi lain yang digunakan oleh PT. Siber Sekuriti Indonesia.
2. Penelitian ini berfokus pada analisis kerentanan teknis yang sesuai dengan standar OWASP ASVS, tanpa memasukkan aspek manajemen dan kebijakan keamanan informasi.
3. Penelitian ini tidak akan melibatkan pengujian fisik, pengujian jaringan, atau integrasi dengan sistem luar.

2.3.3. Metodologi Pengujian

1. Metode *Greybox Testing* digunakan untuk mengidentifikasi kerentanan aplikasi dari perspektif pengguna, dengan memanfaatkan informasi internal terbatas.
2. Pengujian keamanan aplikasi dilakukan berdasarkan standar OWASP ASVS untuk memastikan keamanan terhadap standar industri.
3. Penelitian ini terdiri dari tiga tahap: identifikasi kerentanan keamanan, analisis eksploitasi kelemahan dan evaluasi risiko potensial yang

dihasilkan.

2.3. Deskripsi pekerjaan

Dalam pengerjaan penelitian ini, ada sebuah penjelasan mengenai apa saja yang akan dan harus dikerjakan agar tidak terjadi kesalahan dalam pengerjaan, yang mana akan dijelaskan sebagai berikut:

2.4.1 Analisis dan Dokumentasi

a. Tugas: Mungumpulkan dan menganalisis kebutuhan keamanan pengguna dan bisnis untuk sistem *top-up* saldo. Menyusun dokumen spesifik yang mendetail.

b. Tanggung jawab: Melakukan koordinasi efektif dengan pemangku kepentingan untuk memastikan desain sistem memenuhi standar kebutuhan.

2.4.2 Implementasi

a. Tugas: Mengimplementasikan Fitur *top-up* saldo berbasis persetujuan admin dengan melakukan pegujian keamanan berstandar OWASP ASVS .

b. Tanggung jawab: Melakukan pengujian keamanan, serta menyelesaikan sesuai dengan tenggat waktu.

2.4.3 Pengujian dan Validasi

a. Tugas: Melakukan pengujian menyeluruh untuk memastikan bahwa fitur *top-up* berbasis persetujuan admin berfungsi dengan baik dan aman sesuai standar OWASP ASVS. Mengidentifikasi dan perbaikan bug

b. Tanggung jawab: Mengelola proses ujicoba dan mengevaluasi hasil pengujian untuk peningkatan keamanan fitur.

2.4.4 Mitigasi dan Pelaporan

a. Tugas: Melakukan pencegahan dan menyusun pelaporan terstruktur yang relevan dengan celah keamanan yang ditemukan.

b. Tanggung jawab: Membuat dan menyusun langkah langkah pencegahan dan tindak lanjut jika terjadi hal serupa serta melaporkan hasil penelitian.