BAB II
PROFIL INSTANSI PT. SEKURITI SIBER INDONESIA

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 memiliki tugas utama dalam meningkatkan keamanan teknologi informasi sesuai dengan standar nasional dan internasional. Dalam proyek ini, fokus pekerjaan diarahkan pada analisis serta pengujian keamanan terhadap aplikasi web TriUpasedanan, yang secara spesifik menyasar kerentanan pada fitur masukkan pengguna. Tujuan utama dari pengujian ini adalah untuk mendeteksi potensi serangan Cross-Site Scripting (XSS) yang dapat mengancam integritas dan kerahasiaan data. Lingkup pekerjaan penulis selama melaksanakan magang mencakup tiga aspek utama, yaitu:

2.3.1 Web Aplikasi TriUpasedanan

TriUpasedanan merupakan sebuah aplikasi web pemesanan hotel yang digunakan untuk mengelola layanan reservasi kamar, data pengguna, dan komunikasi melalui komentar. Aplikasi ini memiliki fitur login, register, dashboard user dan admin, serta pengelolaan data booking. Pengujian dilakukan pada fitur yang memungkinkan masukkan dari pengguna seperti edit profil dan komentar.

2.3.2 Batasan Penelitian

Penelitian ini hanya berfokus pada identifikasi dan eksploitasi kerentanan XSS (Cross-Site Scripting) tanpa mencakup jenis serangan lain seperti SQL Injection atau CSRF. Pengujian dilakukan dari sisi user biasa terhadap dua fitur utama, yakni edit profil dan komentar. Penyerang dalam skenario ini hanya dibatasi sebagai user terdaftar tanpa hak akses istimewa.

2.3.3 Metodologi Pengujian

Pengujian dilakukan melalui pendekatan simulasi dengan metode black-box testing, di mana penguji tidak memiliki akses ke kode sumber. Penyerangan XSS dilakukan dengan menyisipkan payload berbahaya ke dalam form masukkan pengguna, kemudian diamati apakah payload tersebut dieksekusi ketika ditampilkan kembali. Tools bantu yang digunakan termasuk Burp Suite dan layanan pelaporan seperti xss.report.

2.4 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

Penulis melakukan analisis terhadap seluruh masukkan form pada aplikasi untuk menemukan fitur yang berpotensi menerima masukkan pengguna tanpa proses validasi. Setelah identifikasi, dilakukan pencatatan dan dokumentasi detail fitur yang

menjadi target pengujian, termasuk halaman dan parameter masukkan yang tersedia.

2.4.2 Implementasi

Penulis menyisipkan payload XSS seperti `<script>alert('XSS')</script>` ke dalam kolom nama pengguna dan kolom komentar. Payload ini digunakan untuk menguji apakah sistem menampilkan kembali masukkan tanpa proses sanitasi. Selain itu, digunakan juga payload dari xss.report untuk melakukan simulasi pencurian cookie session milik admin.

2.4.3 Pengujian dan Validasi

Setelah payload disisipkan, pengujian dilakukan dengan memuat ulang halaman sebagai admin. Ketika halaman dibuka dan payload berhasil dijalankan, maka cookie session akan dikirim ke endpoint yang ditentukan. Validasi keberhasilan dilakukan dengan membuka halaman xss.report dan membandingkan nilai cookie admin yang dikirim. Jika cookie berhasil digunakan untuk login tanpa password, maka pengujian dinyatakan berhasil.

2.4.4 Perbaikan dan Pengujian Kembali

Setelah kerentanan XSS teridentifikasi dan dieksploitasi, dilakukan perbaikan pada sisi backend dengan menambahkan fungsi untuk menyaring karakter berbahaya seperti < dan >. Fungsi ini diterapkan pada data masukkan yang ditampilkan ulang, seperti pada nama pengguna dan isi komentar. Setelah proses perbaikan, dilakukan pengujian ulang untuk memastikan bahwa payload XSS tidak lagi dieksekusi, melainkan hanya ditampilkan sebagai teks biasa. Hasilnya, serangan XSS tidak berhasil dijalankan dan halaman tetap aman dari injeksi skrip. Hal ini membuktikan bahwa perbaikan berhasil diterapkan dan aplikasi sudah lebih aman terhadap serangan XSS.