BAB I
PENDAHULUAN

1.1 Latar Belakang

PT Sekuriti Siber Indonesia (NemoSecurity) merupakan perusahaan konsultan yang bergerak di bidang keamanan siber, dengan spesialisasi pada layanan penetration testing, pemantauan Security Operations Center (SOC), serta kepatuhan terhadap standar keamanan informasi, khususnya ISO 27001. Dalam era digital yang semakin kompleks, ancaman terhadap keamanan informasi menjadi semakin nyata, baik bagi perusahaan swasta maupun instansi pemerintah. Untuk itu, kebutuhan akan layanan keamanan yang komprehensif dan sesuai dengan standar internasional seperti ISO 27001 menjadi sangat penting.

ISO 27001 adalah standar internasional yang menetapkan persyaratan untuk Sistem Manajemen Keamanan Informasi (SMKI). Standar ini dirancang untuk memastikan bahwa organisasi dapat mengelola keamanan aset informasi dengan cara yang sistematis dan terstruktur. Salah satu kontrol penting dalam ISO 27001 adalah Technical Vulnerability Management yang tercantum dalam kontrol A.12.6.1. Kontrol ini mengharuskan organisasi untuk mengidentifikasi, mengkaji, dan menangani kerentanan teknis secara tepat waktu untuk mengurangi risiko yang terkait dengan kerentanan tersebut.

Salah satu klien PT Sekuriti Siber Indonesia adalah instansi pemerintah XYZ yang sedang membutuhkan pendampingan dalam proses sertifikasi ISO 27001. Sebagai bagian dari proses ini, perlu dilakukan implementasi kontrol A.12.6.1, yang menekankan pentingnya manajemen kerentanan teknis untuk memastikan bahwa sistem informasi yang digunakan oleh instansi tersebut aman dari ancaman dan kerentanan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Untuk mendukung kesiapan Instansi XYZ dalam sertifikasi ISO 27001, penetration testing dilaksanakan mulai tanggal 18 Maret 2024 sampai 3 April 2024.

Selain itu, implementasi ISO 27001 di Instansi XYZ juga mendukung program Sistem Pemerintahan Berbasis Elektronik (SPBE) yang diamanatkan oleh Peraturan Presiden No. 95 Tahun 2018. Penerapan ISO 27001 sebagai Sistem Manajemen Keamanan Informasi dapat melengkapi pelaksanaan SPBE dalam rangka mendukung tata kelola pemerintahan yang baik (good governance) yang bersih, transparan, dan akuntabel. Dengan memenuhi standar ISO 27001, keamanan informasi akan lebih terjamin, sehingga dapat mendukung terciptanya lingkungan pemerintahan yang lebih efisien dan aman.

Berdasarkan latar belakang di atas, laporan ini akan berfokus pada implementasi kontrol A.12.6.1 (Technical Vulnerability Management) dalam kerangka sertifikasi ISO 27001 di Instansi XYZ. Penelitian ini bertujuan

untuk memberikan panduan praktis dan analisis mendalam mengenai langkah-langkah yang harus diambil dalam mengelola kerentanan teknis, serta dampak dari implementasi kontrol ini terhadap kesiapan instansi dalam meraih sertifikasi ISO 27001. Dengan terpenuhinya standar ISO 27001, maka keamanan sistem informasi di Instansi XYZ akan lebih terjamin, yang pada gilirannya mendukung pelaksanaan SPBE dan tata kelola pemerintahan yang lebih baik.

1.2 Rumusan Masalah

Penelitian ini akan difokuskan pada kegiatan *penetration testing* terhadap dua aplikasi *mobile* yang digunakan oleh Instansi XYZ, yaitu aplikasi XXDOC dan KELHEBAT.

1.3 Ruang Lingkup

Penelitian ini mencakup pengujian keamanan terhadap dua aplikasi *mobile* yang digunakan oleh Instansi XYZ, yaitu aplikasi XXDOC dan KELHEBAT, dengan rincian sebagai berikut:

1.3.1 Aplikasi XXDOC

Aplikasi ini digunakan untuk menyimpan dan mengelola dokumen, melihat rekaman CCTV seluruh kota, serta mengakses data karyawan instansi pemerintah. Pengujian keamanan difokuskan pada beberapa aspek, termasuk akses terhadap dokumen dan data karyawan, fitur CCTV untuk mencegah akses ilegal, serta identifikasi kerentanan berdasarkan OWASP Top 10 dan OWASP API Security Top 10.

1.3.2 Aplikasi KELHEBAT

Aplikasi ini digunakan di lingkungan kelurahan, mencakup pejabat RT, RW, hingga kelurahan, dengan fungsi utama untuk pengelolaan data penduduk. Pengujian keamanan mencakup akses data penduduk untuk melindungi informasi pribadi, integritas dan kerahasiaan data guna mencegah manipulasi atau akses tanpa izin, serta identifikasi kerentanan berdasarkan standar OWASP Top 10 dan OWASP API Security Top 10 untuk mengamankan aplikasi dari ancaman umum.

1.3.3 Batasan Penelitian

a. Penelitian ini terbatas pada dua aplikasi *mobile* yang disebutkan di atas dan tidak mencakup sistem atau aplikasi lain yang digunakan oleh Instansi XYZ.

b. Penelitian ini hanya mencakup kerentanan teknis yang relevan dengan standar OWASP *Top* 10 dan OWASP API *Security Top* 10, dan tidak mencakup aspek manajemen atau kebijakan keamanan informasi lainnya.

c. Penelitian ini tidak akan melibatkan pengujian fisik atau pengujian terhadap jaringan luar yang terhubung dengan aplikasi.

1.3.4 Metodologi Pengujian

a. Metode pengujian yang akan digunakan adalah *greybox testing*, dimana peneliti memiliki akses terbatas ke informasi internal aplikasi, namun tetap mempertahankan perspektif pengguna.

b. Pengujian akan dilakukan berdasarkan standar dan *framework* yang ditetapkan oleh OWASP *Top* 10 dan OWASP API *Security Top* 10.

c. Penelitian akan mencakup identifikasi kerentanan, eksploitasi potensi kelemahan, dan evaluasi risiko yang dihasilkan dari kelemahan yang ditemukan.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mencapai hasil sebagai berikut:

a. **Mengidentifikasi** kerentanan keamanan yang terdapat pada aplikasi mobile XXDOC dan KELHEBAT yang digunakan oleh instansi pemerintah XYZ, dengan menggunakan standar OWASP *Top* 10 dan OWASP API *Security Top* 10 sebagai acuan.

b. **Mengevaluasi** efektivitas dari proses *penetration testing* berbasis metode *greybox* dalam mendeteksi dan mengungkap kelemahan keamanan pada aplikasi XXDOC dan KELHEBAT.

c. **Menentukan** langkah-langkah mitigasi yang tepat berdasarkan temuan hasil *penetration testing* untuk mengurangi risiko yang diidentifikasi pada aplikasi *mobile* tersebut.

d. **Menyusun** rekomendasi implementasi kontrol *Technical Vulnerability Management* (A.12.6.1) pada Instansi XYZ, dengan fokus pada perbaikan keamanan aplikasi XXDOC dan KELHEBAT.

e. **Mengevaluasi** dampak dari penerapan langkah-langkah mitigasi terhadap kesiapan Instansi XYZ dalam meraih sertifikasi ISO 27001, khususnya terkait dengan pemenuhan kontrol A.12.6.1.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1.5.1 Manfaat Teoritis

a. Menambah literatur dan pemahaman dalam bidang keamanan siber, khususnya terkait dengan implementasi *penetration testing*

menggunakan standar OWASP *Top* 10 dan OWASP API *Security Top* 10.

b. Memberikan kontribusi akademis dalam pengembangan metodologi pengujian keamanan aplikasi *mobile* dengan metode *greybox*.

1.5.2 Manfaat Praktis

a. Bagi Instansi XYZ

i. Memberikan wawasan yang mendalam tentang tingkat keamanan aplikasi *mobile* XXDOC dan KELHEBAT, serta mengidentifikasi kerentanan yang dapat mengancam keamanan data dan informasi.

ii. Membantu instansi dalam mempersiapkan diri untuk meraih sertifikasi ISO 27001 melalui implementasi kontrol *Technical Vulnerability Management* (A.12.6.1) yang lebih efektif.

iii. Menyediakan rekomendasi langkah-langkah mitigasi yang dapat diimplementasikan untuk memperkuat keamanan aplikasi dan mencegah potensi ancaman siber.

b. Bagi PT Sekuriti Siber Indonesia (NemoSecurity)

i. Memperkuat portofolio layanan konsultasi keamanan siber dengan studi kasus nyata yang mendalam dan berbasis standar internasional.

ii. Meningkatkan kualitas layanan *penetration testing* dengan penerapan metode dan standar yang telah terbukti efektif dalam penelitian ini.

c. Bagi Masyarakat

i. Meningkatkan keamanan data dan informasi yang dikelola oleh Instansi XYZ, yang pada gilirannya akan melindungi data pribadi dan kepentingan masyarakat.

ii. Meningkatkan kepercayaan masyarakat terhadap penggunaan aplikasi *mobile* yang dikelola oleh instansi pemerintah, khususnya yang berkaitan dengan pelayanan publik dan pengelolaan data penduduk.