BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini telah berhasil mengidentifikasi dan menganalisis kerentanan keamanan pada aplikasi *mobile* XXDOC dan aplikasi web KELHEBAT melalui *penetration testing* yang dilakukan sesuai dengan standar OWASP *Top* 10 dan OWASP API *Security Top* 10. Implementasi pengujian ini dilakukan dengan menggunakan alat seperti *Burp Suite,* Frida, dan Apktool.

Dari hasil pengujian ini, ditemukan:

5.1.1 Pada Aplikasi *Mobile* XXDOC

a. **CCTV *Credential Exposed via Memory Dump and App Logs*:** Kredensial CCTV terekspos di memori dan log aplikasi, berpotensi diakses oleh penyerang.

b. ***Path Traversal Expose Internal Client Apps***: Penyerang dapat mengakses aplikasi internal klien melalui *path traversal*.

5.1.2 Pada Aplikasi Web KELHEBAT

a. ***Insecure Direct Object References* (IDOR) - Pengambilalihan Akun:** Penyerang dapat mengambil alih akun pengguna lain.

b. ***Cross Site Scripting* (XSS) - *Reflected:*** Penyerang dapat menginjeksi skrip berbahaya yang dieksekusi di *browser* pengguna.

c. ***Insecure Direct Object References* (IDOR) - Hapus Data:** Penyerang dapat menghapus data penting.

Kerentanan ini berdampak langsung pada keamanan informasi dan berkaitan dengan ISO 27001 Kontrol A.12.6.1, yang mengharuskan kerentanan teknis dikelola secara efektif. Setelah dilakukan perbaikan atau penerimaan risiko, laporan hasil pengujian ini dapat mendukung pemenuhan kontrol tersebut dan memperkuat keamanan serta kepatuhan organisasi terhadap standar ISO 27001.

5.2 Saran

Berdasarkan hasil temuan dan analisis dalam penelitian ini, beberapa saran yang dapat diberikan untuk meningkatkan keamanan aplikasi dan mendukung kepatuhan terhadap standar ISO 27001, adalah sebagai berikut:

a. **Perbaikan Kerentanan**

Segera lakukan perbaikan pada kerentanan yang ditemukan. Hal ini penting untuk mencegah potensi eksploitasi yang dapat berdampak pada keamanan dan privasi data.

b. **Peningkatan Proses *Technical Vulnerability Management***

Implementasikan proses *Technical Vulnerability Management* yang lebih ketat dan berkelanjutan sesuai dengan ISO 27001 Kontrol A.12.6.1. Ini termasuk melakukan pengujian keamanan secara rutin, pemantauan, serta respons cepat terhadap kerentanan baru yang mungkin muncul.

c. **Penerapan *Best Practices* dalam Pengembangan Aplikasi**

Terapkan *best practices* dalam pengembangan aplikasi, seperti penggunaan enkripsi yang kuat, sanitasi input yang ketat, dan validasi data yang diterima dari pengguna. Pastikan juga bahwa semua data sensitif disimpan dan ditransmisikan secara aman.

d. Pelatihan dan Peningkatan Kesadaran Keamanan

Berikan pelatihan dan peningkatan kesadaran keamanan kepada tim pengembang dan staf terkait mengenai praktik keamanan terbaik, potensi ancaman, dan cara-cara untuk mencegahnya. Ini penting untuk mengurangi risiko kesalahan manusia yang dapat menyebabkan kerentanan keamanan.

e. Pengujian Keamanan Secara Berkala

Lakukan pengujian keamanan secara berkala untuk mengidentifikasi potensi kerentanan baru. Pengujian seperti *penetration testing* harus menjadi bagian integral dari siklus pengembangan dan pemeliharaan aplikasi.

Dengan menerapkan saran-saran ini, organisasi dapat memperkuat keamanan aplikasi dan meningkatkan kepatuhan terhadap standar keamanan informasi, yang pada akhirnya akan melindungi data sensitif dan menjaga integritas sistem informasi.