BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan mengenai implementasi Vulnerability Assessment dan Penetration Testing (VA/PT) berbasis Penetration Testing Execution Standard (PTES) pada platform web Skill Upkids milik PT ANAK HEBAT NUSANTARA, maka dapat ditarik kesimpulan sebagai berikut:

1. Penerapan metode Vulnerability Assessment dan Penetration Testing (VA/PT) berbasis Penetration Testing Execution Standard (PTES) terbukti mampu mengidentifikasi dan menganalisis kerentanan keamanan secara sistematis dan komprehensif pada platform web Skill Upkids. Proses pengujian dilaksanakan dengan pendekatan *black box testing* melalui tahapan PTES yang meliputi *pre-engagement interactions, intelligence gathering, threat modelling, vulnerability analysis, exploitation, post-exploitation,* dan *reporting*. Pada tahap *intelligence gathering*, diperoleh informasi teknis terkait arsitektur sistem, infrastruktur jaringan, layanan backend, serta teknologi yang digunakan oleh aplikasi web. Informasi tersebut digunakan untuk memetakan permukaan serangan (*attack surface*) secara menyeluruh. Selanjutnya, pada tahap *threat modelling* dan *vulnerability analysis*, dilakukan analisis terhadap potensi ancaman dan kelemahan sistem menggunakan kombinasi pemindaian otomatis dan pengujian manual. Hasil pengujian menunjukkan adanya beberapa kerentanan dengan tingkat risiko tinggi hingga kritis, antara lain lemahnya manajemen sesi yang berpotensi menyebabkan *session hijacking*, mekanisme reset kata sandi tanpa verifikasi identitas yang memadai, ketiadaan token Cross-Site Request Forgery (CSRF) pada formulir input, penggunaan cookie sesi tanpa atribut keamanan, serta terbukanya layanan backend yang masih menggunakan protokol HTTP tanpa enkripsi. Kerentanan-kerentanan tersebut berpotensi berdampak signifikan terhadap aspek kerahasiaan

(*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data pengguna, khususnya data pribadi anak-anak sebagai kelompok pengguna rentan.

2. Berdasarkan hasil pengujian penetrasi yang mengidentifikasi 5 kerentanan dengan tingkat keparahan tinggi hingga kritis, rekomendasi mitigasi disusun secara spesifik sesuai karakteristik masing-masing temuan. Kerentanan session hijacking akibat manajemen sesi yang lemah direkomendasikan untuk diperbaiki melalui regenerasi session ID setelah autentikasi dan pembatasan masa aktif sesi. Kerentanan pada mekanisme reset kata sandi tanpa verifikasi identitas direkomendasikan untuk ditingkatkan dengan penerapan verifikasi berbasis One-Time Password (OTP) atau multi-factor authentication. Ketiadaan token CSRF pada formulir input direkomendasikan untuk diperbaiki melalui implementasi CSRF token yang tervalidasi di sisi server. Cookie sesi tanpa atribut keamanan diperbaiki dengan konfigurasi atribut Secure, HttpOnly, dan SameSite untuk mencegah pencurian sesi melalui serangan XSS maupun man-in-the-middle. Selain itu, temuan terbukanya port backend yang masih menggunakan protokol HTTP tanpa enkripsi direkomendasikan untuk ditutup atau diamankan menggunakan protokol HTTPS dengan sertifikat TLS yang valid. Rekomendasi tersebut dirumuskan berdasarkan tingkat risiko kerentanan dan hasil validasi eksploitasi yang dilakukan pada penelitian ini, sehingga secara langsung menargetkan kelemahan yang teridentifikasi pada sistem.

5.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang telah diperoleh dari penerapan Vulnerability Assessment dan Penetration Testing (VA/PT) berbasis Penetration Testing Execution Standard (PTES) pada platform web Skill Upkids milik PT ANAK HEBAT NUSANTARA, maka saran yang dapat diberikan adalah sebagai berikut:

1. Bagi Pengelola dan Pengembang Platform Skill Upkids Pengelola dan tim pengembang platform Skill Upkids disarankan untuk segera menindaklanjuti seluruh temuan kerentanan keamanan yang telah diidentifikasi dalam penelitian ini sesuai dengan tingkat risiko masing-masing. Prioritas perbaikan perlu difokuskan pada kerentanan dengan tingkat risiko tinggi hingga kritis, khususnya yang berkaitan dengan manajemen sesi, mekanisme reset kata sandi, serta keamanan komunikasi data. Selain itu, disarankan untuk menerapkan standar pengembangan aplikasi yang aman (*secure coding practices*), melakukan pembaruan dan konfigurasi sistem secara berkala, serta memastikan seluruh layanan backend dan endpoint aplikasi web telah menggunakan protokol HTTPS untuk mencegah potensi serangan *man-in-the-middle*. Penerapan pengujian keamanan secara rutin sebelum dan sesudah proses pengembangan (*secure software development lifecycle*) juga sangat dianjurkan guna menjaga keamanan sistem secara berkelanjutan.
2. Bagi Pihak Manajemen dan Pemangku Kepentingan Pihak manajemen PT Anak Hebat Nusantara disarankan untuk menjadikan hasil penelitian ini sebagai dasar dalam penyusunan kebijakan keamanan informasi dan pengambilan keputusan strategis terkait pengelolaan risiko keamanan sistem informasi. Penyusunan kebijakan keamanan yang terstruktur, termasuk pengaturan hak akses, pengelolaan insiden keamanan, serta mekanisme audit keamanan secara berkala, diharapkan dapat meningkatkan kesadaran dan kesiapan organisasi dalam menghadapi potensi ancaman siber. Selain itu, pelatihan dan peningkatan kompetensi

sumber daya manusia di bidang keamanan informasi perlu dilakukan secara berkelanjutan untuk meminimalkan risiko kesalahan manusia (*human error*) yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.

3. Bagi Penelitian selanjutnya disarankan untuk mengembangkan cakupan pengujian keamanan dengan mengombinasikan framework PTES dengan metode pengujian teknis lain seperti OWASP Web Security Testing Guide (WSTG), serta mengintegrasikannya dengan standar manajemen keamanan informasi seperti ISO/IEC 27001 guna mengevaluasi kesesuaian kontrol keamanan sistem secara lebih menyeluruh. ISO/IEC 27001 merupakan standar internasional yang mengatur penerapan Sistem Manajemen Keamanan Informasi (Information Security Management System/ISMS), sehingga dapat digunakan sebagai acuan dalam menilai kebijakan, prosedur, dan kontrol keamanan organisasi secara strategis. Selain itu, pengujian dapat diperluas pada aspek keamanan lain seperti keamanan aplikasi mobile, keamanan Application Programming Interface (API), serta pengujian terhadap skenario serangan lanjutan. Penggunaan metrik penilaian risiko seperti Common Vulnerability Scoring System (CVSS) versi terbaru juga disarankan agar tingkat keparahan kerentanan dapat diukur secara lebih objektif dan terstandarisas