BAB I
PENDAHULUAN

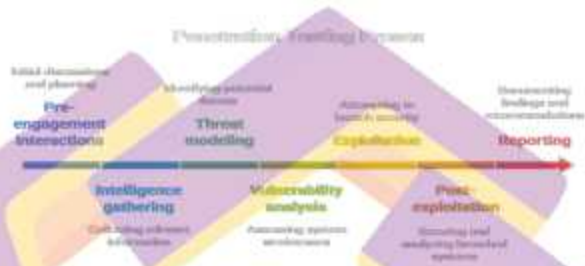
1.1. Latar Belakang

Transformasi digital di sektor pendidikan Indonesia mengalami percepatan signifikan dalam beberapa tahun terakhir, terutama sebagai dampak dari pandemi COVID-19 yang mendorong penerapan pembelajaran daring secara masif. Kondisi ini memicu pertumbuhan berbagai platform teknologi pendidikan (*edutech*) yang menawarkan akses pembelajaran yang lebih fleksibel, inklusif, dan terjangkau [1]. Salah satu kelompok pengguna utama layanan edutech adalah anak-anak, yang secara hukum dan teknis dikategorikan sebagai kelompok rentan dalam konteks perlindungan data pribadi dan privasi digital. Oleh karena itu, aspek keamanan informasi menjadi elemen krusial yang harus diperhatikan dalam setiap tahapan pengembangan dan pengoperasian sistem edutech [6].

Dalam konteks tersebut, PT ANAK HEBAT NUSANTARA sebagai pengembang platform edutech Skill Upkids, yang menyediakan layanan pembelajaran daring berbasis web untuk anak-anak, dihadapkan pada tantangan serius dalam aspek keamanan digital. Platform ini dirancang dengan arsitektur sistem yang kompleks, mencakup integrasi layanan cloud computing, penggunaan Application Programming Interface (API) pihak ketiga, serta sistem manajemen konten yang bersifat dinamis dan real-time. Kompleksitas arsitektur tersebut memperluas permukaan serangan (attack surface) dan meningkatkan potensi munculnya celah keamanan yang dapat dimanfaatkan oleh pihak tidak berwenang [2], [10].

Berdasarkan penelusuran yang dilakukan peneliti terhadap dokumentasi publik dan informasi yang tersedia pada platform Skill Upkids, belum ditemukan informasi terbuka mengenai pelaksanaan audit keamanan sistem yang mengacu pada standar internasional, khususnya Penetration Testing Execution Standard (PTES). Ketidakhadiran audit keamanan yang sistematis berpotensi menyebabkan kerentanan tersembunyi tidak terdeteksi secara proaktif [3], [5]. Oleh karena itu, penelitian ini mengusulkan penerapan metode Vulnerability Assessment dan

Penetration Testing (VA/PT) berbasis PTES, yang menyediakan kerangka kerja pengujian keamanan melalui tujuh tahapan utama, sebagaimana ditunjukkan pada Gambar 1.2. Pendekatan PTES bersifat terstandarisasi dan terdokumentasi dengan baik, serta terbukti efektif dalam mendeteksi kerentanan kritis pada sistem berbasis web dan platform pendidikan daring [7], [8].



Gambar 1. 1 Proses Pentesting

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana proses identifikasi kerentanan keamanan pada platform Skill Upkids melalui penerapan metode *Vulnerability Assessment and Penetration Testing* (VA/PT) yang mengacu pada framework *Penetration Testing Execution Standard* (PTES)?
2. Bagaimana rekomendasi mitigasi keamanan berdasarkan tingkat keparahan kerentanan yang diklasifikasikan menggunakan metode CVSS dari hasil pengujian penetrasi pada platform Skill Upkids?

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan fokus, maka batasan masalah dalam penelitian ini ditetapkan sebagai berikut:

1. Platform edutech Skill Upkids yang dikembangkan oleh PT ANAK HEBAT NUSANTARA
2. Pengujian keamanan *Vulnerability Assessment* (VA) dan *Penetration Testing* (PT).
3. Framework *Penetration Testing Execution Standard* (PTES).
4. Pengujian difokuskan pada kerentanan keamanan sistem berbasis web, meliputi konfigurasi server, layanan aplikasi, serta integrasi *Application Programming Interface* (API)
5. Variabel utama dalam penelitian ini adalah jenis dan tingkat kerentanan keamanan sistem yang teridentifikasi melalui tahapan VA/PT berbasis PTES.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Melakukan evaluasi keamanan sistem pada platform Skill Upkids menggunakan metode *Vulnerability Assessment* (VA) dan *Penetration Testing* (PT) yang mengacu pada framework *Penetration Testing Execution Standard* (PTES).
2. Mengidentifikasi dan menganalisis kerentanan keamanan yang terdapat pada sistem Skill Upkids berdasarkan hasil pengujian penetrasi yang dilakukan.
3. Menyusun rekomendasi strategi mitigasi keamanan yang tepat dan efektif berdasarkan temuan teknis dari proses *Vulnerability Assessment* dan *Penetration Testing*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat secara teoretis dan praktis. Secara teoretis, hasil penelitian dapat berkontribusi pada pengembangan literatur keamanan siber, khususnya terkait penerapan *Penetration Testing Execution Standard* (PTES) pada sistem teknologi pendidikan (*edutech*) di Indonesia. Secara praktis, penelitian ini diharapkan menjadi panduan teknis yang sistematis bagi pengembang platform edutech, khususnya **Skill Upkids**, dalam mengidentifikasi dan memitigasi kerentanan keamanan guna memperkuat perlindungan data pribadi anak-anak. Selain itu, temuan penelitian ini diharapkan dapat mendukung penguatan ketahanan keamanan siber sektor pendidikan serta menjadi referensi bagi penelitian selanjutnya pada platform pendidikan digital sejenis.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran umum mengenai alur pembahasan dan keterkaitan antar bab yang disajikan secara sistematis sebagai berikut:

Bab I Pendahuluan

Bab ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan yang menjadi dasar dan arah pelaksanaan penelitian.

Bab II Tinjauan Pustaka dan Landasan Teori

Bab ini membahas studi literatur dan dasar teori yang relevan dengan penelitian, meliputi konsep keamanan informasi, *Vulnerability Assessment*, *Penetration Testing*, *Penetration Testing Execution Standard* (PTES), serta penelitian terdahulu yang digunakan sebagai landasan teoritis dan pembanding penelitian.

Bab III Metode Penelitian

Bab ini menjelaskan metodologi penelitian yang digunakan, meliputi objek penelitian, alur penelitian, serta alat dan bahan yang digunakan dalam pelaksanaan *Vulnerability Assessment and Penetration Testing* pada platform Skill Upkids berdasarkan framework PTES.

Bab IV Hasil dan Pembahasan

Bab ini menyajikan hasil pelaksanaan pengujian keamanan sistem yang meliputi

tahapan *Information Gathering*, *Threat Modelling*, *Vulnerability Analysis*, *Exploitation*, dan *Reporting*. Selain itu, bab ini juga membahas analisis temuan kerentanan, tingkat risiko, serta rekomendasi mitigasi keamanan yang dihasilkan dari proses pengujian.

Bab V Penutup

Bab ini berisi kesimpulan yang diperoleh dari hasil penelitian serta saran yang ditujukan bagi pengelola sistem dan peneliti selanjutnya sebagai bahan evaluasi dan pengembangan keamanan system di masa mendatang.