BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong transformasi digital di berbagai layanan. Salah satu dari layanan tersebut yaitu aplikasi berbasis web kini menjadi komponen utama dalam penyediaan layanan digital, seperti sistem informasi, *e-commerce*, perbankan, hingga layanan publik (Sayan et al., 2024). Namun, peningkatan penggunaan aplikasi web juga diikuti dengan meningkatnya ancaman keamanan siber. Hal ini disebabkan oleh luasnya *attack surface* serta masih banyaknya praktik pengembangan aplikasi yang belum memperhatikan aspek keamanan secara optimal . Kerentanan *seperti SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF),* dan *Password Guessing Attack* masih sering ditemukan dan menjadi ancaman serius bagi keamanan aplikasi web (Bararia & Choudhary, 2023).

Seiring dengan meningkatnya ancaman tersebut, kebutuhan akan sumber daya manusia yang memiliki kompetensi dalam bidang keamanan aplikasi web juga semakin tinggi. Perguruan tinggi, khususnya pada Program Studi Pendidikan Teknik Informatika dan Komputer (PTIK), memiliki peran penting dalam mempersiapkan lulusan yang memahami dan menerapkan prinsip-prinsip keamanan. Oleh karena itu, pembelajaran keamanan aplikasi web tidak cukup hanya disampaikan secara teoritis, melainkan perlu didukung dengan kegiatan praktikum yang memungkinkan mahasiswa memperoleh pengalaman langsung melalui pendekatan *hands-on laboratory* (Chhetri, 2023). Dalam implementasinya, materi keamanan aplikasi web dan mitigasi ancaman memiliki keterkaitan erat dengan mata kuliah Keamanan Sistem Komputer. Pada mata kuliah tersebut, mahasiswa telah dibekali dengan konsep dasar keamanan pada perangkat komputer dan digital secara umum.

Namun, berdasarkan hasil observasi awal pada Program Studi Pendidikan Teknik Informatika dan Komputer (PTIK), pelaksanaan pembelajaran pada mata

kuliah Keamanan Sistem Komputer masih menghadapi beberapa kendala, khususnya dalam kegiatan praktikum. Praktikum masih dilakukan secara mandiri pada perangkat masing-masing mahasiswa dengan mengikuti modul tutorial yang diberikan dosen pengampu. Mahasiswa diminta membangun lingkungan praktik sendiri dan mengumpulkan hasil praktik dalam bentuk dokumentasi atau video. Namun, pelaksanaan praktikum tersebut belum didukung oleh lingkungan laboratorium yang aman dan terisolasi untuk simulasi keamanan siber secara optimal.

Berdasarkan hasil wawancara dengan dosen pengampu mata kuliah Keamanan Sistem Komputer, pembelajaran masih didominasi oleh teori dengan perbandingan sekitar 60% teori dan 40% praktik. Selain itu pada saat diberikan tugas praktikum, perbedaan spesifikasi perangkat mahasiswa menjadi salah satu kendala utama dalam pelaksanaan praktikum karena tidak seluruh perangkat mampu menjalankan kebutuhan simulasi server pada perangkat masng-masing. Serta, Narasumber juga menyampaikan bahwa saat ini belum tersedia media praktikum yang aman dan fleksibel untuk mendukung simulasi serangan secara terkontrol, narasumber juga menyampaikan materi praktikum yang sangat dibutuhkan pada praktikum langsung adalah *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS).

Oleh karena itu, diperlukan suatu solusi pembelajaran praktikum yang mampu menyediakan lingkungan praktik keamanan siber secara aman, fleksibel dan mudah digunakan tanpa bergantung pada spesifikasi perangkat mahasiswa, serta mendukung simulasi serangan dan pengujian keamanan secara terkontrol sehingga proses praktikum dapat dilakukan dengan aman dan terarah. Penelitian oleh Ferdiansyah et al. (2023) menjelaskan bahwa laboratorium berbasis virtualisasi mampu menyediakan lingkungan pengujian yang realistis, terkendali serta mendukung simulasi untuk kegiatan praktikum keamanan siber, juga virtualisasi dapat memudahkan pengelolaan dan replikasi lingkungan praktikum tanpa memerlukan banyak perangkat keras fisik. Berdasarkan penjelasan tersebut, teknologi virtualisasi dipilih sebagai solusi untuk menyediakan lingkungan praktikum keamanan siber yang aman, terisolasi, dan mudah direplikasi tanpa mempengaruhi sistem utama pada perangkat mahasiswa.

Selain itu, kebutuhan praktikum pada materi *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) memerlukan suatu sistem yang mampu melakukan pemantauan, pendeteksian, serta analisis aktivitas keamanan secara langsung selama proses praktikum berlangsung. Berdasarkan penelitian yang dilakukan oleh Mikyal et al. (2024) *Wazuh* yang merupakan *platform Security Information and Event Management* (SIEM) dapat dimanfaatkan sebagai solusi keamanan untuk mendukung proses *Monitoring* dan deteksi ancaman pada server melalui kemampuan pemantauan aktivitas jaringan, analisis log, serta pendeteksian aktivitas mencurigakan secara *real-time*. Penelitian tersebut juga menunjukkan bahwa *Wazuh* mampu mendeteksi berbagai aktivitas serangan seperti DDoS dan memberikan peringatan terhadap ancaman yang terjadi pada sistem, sehingga dapat mendukung fungsi IDS dan IPS dalam lingkungan praktikum keamanan siber. Oleh karena itu, penelitian ini mengintegrasikan *Wazuh* sebagai *platform Monitoring* keamanan untuk membantu proses praktikum melalui pengumpulan, analisis dan visualisasi log keamanan. Data log tersebut digunakan untuk menganalisis pola serangan, proses eksploitasi kerentanan, serta aktivitas mitigasi yang dilakukan mahasiswa sehingga proses pembelajaran dapat berlangsung secara lebih kontekstual, objektif dan terukur.

Agar pengembangan lingkungan praktikum tersebut dapat dilakukan secara sistematis dan terarah, diperlukan suatu model pengembangan yang terstruktur. Salah satu model yang banyak digunakan dalam pengembangan media dan sistem pembelajaran adalah model ADDIE (*Analysis, Design, Development, Implementation, Evaluation*). Model ADDIE menyediakan tahapan yang jelas mulai dari analisis kebutuhan pembelajaran, perancangan sistem, pengembangan media, implementasi dalam proses pembelajaran, hingga tahap evaluasi untuk mengukur kelayakan dan efektivitas media yang dikembangkan (S. Siregar et al., 2021). Namun, penelitian ini dibatasi sampai tahap *Development* karena fokus penelitian adalah menghasilkan dan memvalidasi produk *Virtual Hands-on Lab*. Pendekatan serupa juga diterapkan oleh Arianti et al. (2021), yang hanya mengkaji pengembangan produk sampai tahap *Development* tanpa melaksanakan tahap *Implementation* dan *Evaluation*.

Penelitian ini dilakukan dengan tujuan mengembangkan *Hands-on Lab* Praktikum Keamanan Aplikasi Web berbasis teknologi virtualisasi menggunakan model ADDIE hingga tahap *Development*, dimana Produk yang dikembangkan diharapkan dapat menjadi solusi alternatif dalam mengatasi keterbatasan infrastruktur praktikum di lingkungan pendidikan, sekaligus mendukung pelaksanaan simulasi keamanan siber secara aman, fleksibel, dan terkontrol. Selain itu, pengembangan *Virtual Hands-on Lab* ini diharapkan mampu meningkatkan pemahaman konseptual serta keterampilan praktis mahasiswa PTIK dalam melakukan identifikasi kerentanan, simulasi serangan, dan mitigasi keamanan.

Posisi kebaruan tersebut dapat diperjelas melalui perbandingan langsung dengan penelitian *Hands-on Lab* keamanan siber sebelumnya. Mustamin et al. (2025) mengembangkan modul *cyber drill* investigasi *dark web* pada *platform* eksternal *TryHackMe* tanpa integrasi sistem *Monitoring* terpadu; Kim et al. (2023) berfokus pada gamifikasi lab keamanan jaringan tanpa aspek analitik log; Wijayanto et al. (2026) menggunakan lingkungan VirtualBox yang bersifat standalone tanpa kemampuan *Monitoring* terpusat; Tapiawala dan Wang (2023) merancang laboratorium sederhana berbasis *virtual machine* dengan BeEF-XSS tanpa sistem SIEM; dan Pattanayak et al. (2022) mengembangkan sembilan modul *hands-on* melalui *platform* CYOTEE tanpa fitur analitik berbasis log. Berbeda dengan kelima penelitian tersebut, penelitian ini mengintegrasikan *Wazuh* sebagai SIEM di dalam infrastruktur *Proxmox VE* yang menghadirkan aplikasi web rentan *OWASP Juice Shop*, sehingga aktivitas praktikum mahasiswa mulai dari upaya eksploitasi hingga mitigasi dapat direkam, dianalisis, dan dievaluasi secara objektif berbasis data log.

Dengan demikian, penelitian ini tidak hanya berfokus pada pengembangan media pembelajaran, tetapi juga menghadirkan pendekatan evaluasi berbasis data yang lebih komprehensif dalam pembelajaran keamanan aplikasi web.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat diidentifikasi beberapa permasalahan sebagai berikut:

1. Pembelajaran pada mata kuliah Keamanan Sistem Komputer masih didominasi teori dibandingkan praktik.
2. Praktikum masih dilakukan secara mandiri pada perangkat masing-masing mahasiswa sehingga belum tersedia lingkungan praktikum yang aman dan terstandarisasi.
3. Materi praktikum yang dibutuhkan seperti *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) memerlukan dukungan lingkungan praktikum yang mampu melakukan simulasi, *Monitoring*, dan analisis keamanan.

1.3 Batasan Masalah

Agar penelitian lebih terarah dan tidak meluas, maka penelitian ini dibatasi pada:

1. Pengembangan *Virtual Lab* menggunakan *platform Proxmox VE* sebagai sistem virtualisasi.
2. *Virtual Hands-on Lab* difokuskan pada simulasi kerentanan dan serangan keamanan aplikasi web menggunakan *OWASP Juice Shop* serta integrasi *Wazuh* sebagai *Security Information and Event Management* (SIEM) untuk *Monitoring* dan analisis keamanan.
3. Penelitian menggunakan model pengembangan ADDIE yang dibatasi hingga tahap *Analysis, Design, dan Development* untuk menghasilkan produk *Virtual Hands-on Lab*.
4. Penelitian difokuskan pada aspek kelayakan dan tidak mengukur efektivitas pembelajaran. Pemanfaatan *Virtual Hands-on Lab* sebagai pendukung praktikum pada mata kuliah Keamanan Sistem Komputer.

1.4 Rumusan Masalah

Bagaimana hasil pengembangan *Virtual Hands-on Lab* Praktikum Keamanan Aplikasi Web Berbasis Teknologi Virtualisasi Menggunakan Model *ADDIE* ?

1.5 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengembangkan virtual lab untuk keamanan aplikasi web berbasis *Proxmox VE* menggunakan model ADDIE dengan integrasi aplikasi web *OWASP Juice Shop* dan *Wazuh* sebagai SIEM untuk mitigasi kerentanan. Penelitian ini juga bertujuan untuk melihat kelayakan virtual lab dalam mendukung pembelajaran pada mata kuliah Keamanan Sistem Komputer. Sehingga, Penelitian ini berfokus pada pengembangan dan kelayakan produk, bukan pada pengujian efektivitas terhadap peningkatan kompetensi mahasiswa.

1.6 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

1. Bagi Peneliti
   a. Memperluas pengetahuan dan pemahaman mengenai pengembangan *Virtual Hands-on Lab* berbasis teknologi virtualisasi untuk pembelajaran keamanan aplikasi web.
   b. Meningkatkan kemampuan praktis dalam merancang, mengimplementasikan, dan mengevaluasi lingkungan laboratorium virtual menggunakan *Proxmox VE*, *OWASP Juice Shop*, dan *Wazuh*.
   c. Memberikan pengalaman penelitian ilmiah yang bermanfaat sebagai dasar pengembangan lebih lanjut di bidang keamanan siber, virtualisasi, dan *learning analytics* berbasis SIEM.
2. Bagi Program Studi PTIK
   a. Menyediakan solusi alternatif terhadap keterbatasan infrastruktur laboratorium melalui lingkungan praktikum yang aman, terisolasi, dan fleksibel.
   b. Mendukung proses pembelajaran yang lebih praktis, interaktif, dan aplikatif, khususnya pada mata kuliah terkait keamanan sistem komputer dan aplikasi web.
   c. Membantu dosen dan laboran dalam menyediakan media pembelajaran berbasis praktik yang terstruktur dan relevan dengan kebutuhan industri keamanan siber.
3. Bagi Universitas Negeri Jakarta

a. Menambah referensi penelitian dalam bidang teknologi informasi, khususnya pada pengembangan *virtual lab* dan pembelajaran keamanan siber berbasis virtualisasi.
b. Mendorong mahasiswa lain untuk menghasilkan penelitian yang inovatif dan dapat diterapkan secara nyata dalam menyelesaikan permasalahan pembelajaran berbasis teknologi.
c. Menunjukkan kontribusi aktif universitas dalam mendukung transformasi digital dan pengembangan kompetensi mahasiswa di bidang keamanan siber.

4. Bagi Pembaca Umum / Peneliti Selanjutnya
   a. Menyajikan gambaran komprehensif mengenai penerapan *Virtual Hands-on Lab* sebagai media pembelajaran keamanan aplikasi *web*.
   b. Menjadi sumber referensi bagi peneliti atau institusi pendidikan yang ingin mengembangkan laboratorium virtual dengan konsep serupa.
   c. Memberikan acuan dalam pemanfaatan *Wazuh* sebagai SIEM dan *learning analytics* untuk analisis aktivitas pembelajaran berbasis log secara *real-time.*