BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan sistem informasi berbasis web merupakan salah satu isu utama dalam era digital saat ini, khususnya dalam mendukung efisiensi dan keandalan operasional di berbagai sektor, termasuk agribisnis. Sistem informasi digital telah menjadi sarana utama untuk proses pencatatan, pelaporan, dan distribusi hasil pertanian, seperti kelapa sawit. Namun, seiring dengan meningkatnya adopsi sistem digital, potensi ancaman serangan siber terhadap sistem-sistem tersebut juga semakin besar.

Berbagai jenis serangan seperti *SQL Injection, Cross-Site Scripting (XSS),* dan *Broken Authentication* masih menjadi ancaman serius bagi sistem informasi yang tidak dilindungi secara memadai. Menurut OWASP (*Open Web Application Security Project),* sebagian besar celah keamanan pada aplikasi web berasal dari validasi input yang lemah, konfigurasi sistem yang tidak aman, serta kegagalan dalam menerapkan autentikasi dan kontrol akses secara tepat [1].

Fakta tersebut diperkuat oleh data dari Badan Siber dan Sandi Negara (BSSN) yang mencatat ratusan juta anomali trafik yang terindikasi sebagai serangan siber dalam satu tahun, termasuk terhadap sistem berbasis web [2]. Selain itu, kasus kebocoran 91 juta data pengguna Tokopedia pada tahun 2020 [3] menunjukkan bahwa bahkan sistem berskala besar dan banyak digunakan oleh masyarakat tetap rentan terhadap serangan siber apabila tidak dilindungi dengan mekanisme keamanan yang memadai.

Di tingkat lokal, Sistem Informasi Pencatatan Panen Sawit dimanfaatkan untuk mencatat dan mendistribusikan hasil panen secara digital di Kecamatan Bengkalis, Kabupaten Bengkalis, Provinsi Riau. Sistem ini memiliki peran strategis dalam meningkatkan efisiensi operasional petani dan pengelola sawit, karena memfasilitasi pencatatan volume panen, penjadwalan pengiriman, serta pengelolaan data pengguna dan transaksi distribusi. Sistem Informasi Pencatatan

Panen Sawit yang menjadi objek penelitian ini selanjutnya disebut sebagai *SawitGoDigi*.

Saat ini, sistem telah beroperasi dan digunakan secara aktif oleh beberapa pihak. Berdasarkan pemeriksaan awal dan uji pemindaian menggunakan beberapa alat bantu keamanan (mis. *Nmap dan OWASP ZAP*), terdapat indikasi konfigurasi yang belum optimal — antara lain adanya port yang terbuka dan kebijakan header keamanan yang belum lengkap — serta potensi kelemahan validasi input pada beberapa endpoint. Kondisi tersebut menunjukkan bahwa sistem masih berpotensi dieksploitasi oleh pihak yang tidak bertanggung jawab, yang dapat berujung pada kebocoran data, manipulasi informasi, serta kerugian ekonomi dan reputasi bagi pemangku kepentingan.

Untuk mengidentifikasi dan memperbaiki potensi kerentanan tersebut, penelitian ini menggunakan metode *penetration testing* berbasis *OWASP Testing Guide (OTG)* dengan acuan pada kategori kerentanan OWASP Top 10. Pendekatan ini menyediakan kerangka kerja yang sistematis: dimulai dari *information gathering*, dilanjutkan *vulnerability scanning* dan manual *testing/exploitation* pada temuan kritis, serta diakhiri dengan *reporting* yang memuat rekomendasi perbaikan. Hasil pengujian akan disusun menjadi rekomendasi teknis yang terprioritisasi berdasarkan penilaian *risiko (likelihood × impact)* dan kriteria penutupan *(closure criteria*) untuk memastikan bahwa perbaikan yang disarankan efektif.

Pemilihan OWASP Top 10 sebagai standar pengujian dalam penelitian ini didasarkan pada pertimbangan komparatif dengan kerangka kerja lain yang tersedia. *Penetration Testing Execution Standard* (PTES) bersifat generik dan mencakup domain yang luas — mulai dari infrastruktur jaringan, pengujian fisik, hingga rekayasa sosial — sehingga kurang spesifik untuk konteks pengujian aplikasi web seperti SawitGoDigi, yang kerentanannya berpusat pada lapisan aplikasi. Sebaliknya, OWASP *Web Security Testing Guide* dirancang khusus untuk mengevaluasi keamanan aplikasi web, menjadikannya lebih relevan dan terukur sebagai acuan dalam penelitian ini [17]. Adapun kombinasi pendekatan *grey-box* dan *white-box* dipilih karena keduanya saling melengkapi: *grey-box testing* mensimulasikan skenario serangan realistis dari perspektif pengguna dengan akses

terbatas, sementara *white-box testing* memungkinkan analisis akar permasalahan *(root cause)* secara mendalam sehingga proses remediation dapat dilakukan secara tuntas dan terverifikasi [11].

Pendekatan gabungan ini diterapkan agar proses pengujian dapat menggambarkan kondisi riil yang dihadapi oleh pengembang sistem dalam mengevaluasi serta memperbaiki keamanan aplikasi secara menyeluruh. Penelitian ini tidak hanya berhenti pada tahap identifikasi celah, tetapi juga mencakup proses *retesting* untuk memastikan efektivitas perbaikan yang dilakukan, sebelum akhirnya memberikan rekomendasi peningkatan keamanan sistem.

Dengan demikian, penelitian ini diharapkan dapat memberikan dampak nyata, baik dalam bentuk solusi teknis maupun peningkatan kesadaran akan pentingnya keamanan informasi, khususnya di lingkungan lokal seperti Kecamatan Bengkalis. Penerapan *penetration testing* dalam penelitian ini diharapkan dapat memperkuat sistem informasi digital sektor perkebunan serta mendukung tata kelola data yang aman, andal, dan berkelanjutan.

1.2 Rumusan masalah

Sistem Informasi Pencatatan Hasil Panen Sawit (SawitGoDigi) merupakan sistem berbasis web yang digunakan secara aktif dalam proses operasional pencatatan dan distribusi hasil panen di Kecamatan Bengkalis. Sebagai sistem yang mengelola data sensitif seperti identitas pengguna, volume panen, dan transaksi distribusi, aspek keamanan sistem menjadi hal yang sangat krusial. Namun berdasarkan pemeriksaan awal, sistem ini belum pernah menjalani pengujian keamanan secara menyeluruh, sehingga potensi kerentanan yang dapat mengancam kerahasiaan, integritas, dan ketersediaan data belum dapat dipastikan kondisinya.

Penelitian-penelitian sebelumnya menunjukkan bahwa metode penetration testing berbasis OWASP Top 10 efektif dalam mengidentifikasi kerentanan aplikasi web, namun sebagian besar hanya berfokus pada tahap identifikasi tanpa mengintegrasikan proses perbaikan dan pengujian ulang dalam satu siklus yang utuh. Kondisi ini menjadi celah metodologis yang perlu diisi, khususnya pada sistem informasi di sektor agribisnis lokal yang selama ini luput dari evaluasi keamanan sistematis.

Berdasarkan hal tersebut, penelitian ini difokuskan untuk menjawab pertanyaan berikut:

1. Bagaimana tingkat keamanan Sistem Informasi Pencatatan Hasil Panen Sawit (SawitGoDigi) terhadap potensi serangan siber berdasarkan standar OWASP Top 10?
2. Apa saja kerentanan keamanan yang teridentifikasi pada sistem dan bagaimana tingkat risikonya berdasarkan parameter likelihood dan impact?
3. Bagaimana metode *penetration testing* dapat diterapkan secara efektif untuk mengidentifikasi, memperbaiki, dan memverifikasi keamanan sistem dalam satu siklus pengujian yang terintegrasi?

1.3 Batasan Masalah

Penelitian ini dibatasi pada analisis dan perbaikan keamanan Sistem Informasi Pencatatan Hasil Panen Sawit (SawitGoDigi) berbasis web yang digunakan di wilayah Kecamatan Bengkalis, Kabupaten Bengkalis, Provinsi Riau. Pengujian keamanan difokuskan pada aspek *web application security* dengan menggunakan metode *penetration testing* yang mengacu pada standar OWASP Top 10, meliputi proses identifikasi kerentanan, eksploitasi terkendali, penilaian risiko, perbaikan *(remediation),* serta pengujian ulang *(retesting).* Pendekatan pengujian dilakukan menggunakan *grey-box testing* pada tahap awal dan *white-box testing* pada tahap perbaikan, dengan ruang lingkup mencakup modul autentikasi, manajemen sesi, validasi input, kontrol akses, dan konfigurasi keamanan aplikasi. Penelitian ini tidak membahas aspek keamanan infrastruktur jaringan, perangkat keras server, sistem operasi secara mendalam, maupun serangan fisik, serta tidak menilai performa atau kualitas fungsional sistem di luar konteks keamanan.

1.4 Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Menganalisis tingkat keamanan Sistem Informasi Pencatatan Hasil Panen Sawit (SawitGoDigi) terhadap potensi serangan siber berdasarkan standar OWASP Top 10 melalui metode *penetration testing.*

2. Mengidentifikasi kerentanan keamanan yang terdapat pada sistem dan mengevaluasi tingkat risikonya berdasarkan parameter *likelihood* dan *impact* menggunakan OWASP *Risk Rating Methodology.*

3. Melakukan perbaikan *(remediation)* terhadap kerentanan yang teridentifikasi serta memverifikasi efektivitasnya melalui pengujian ulang *(retesting)* dalam satu siklus pengujian yang terintegrasi.

1.5 Manfaat

Adapun manfaat yang diperoleh dari penelitian ini adalah sebagai berikut:

1. Secara teoretis, penelitian ini memberikan gambaran penerapan metode penetration testing berbasis OWASP Top 10 yang mengintegrasikan tahapan identifikasi kerentanan, analisis risiko, perbaikan *(remediation),* dan pengujian ulang *(retesting)* dalam satu siklus pengujian yang utuh — berbeda dengan penelitian sebelumnya yang umumnya hanya berfokus pada tahap identifikasi.
2. Secara teoretis, penelitian ini dapat digunakan sebagai referensi metodologis bagi penelitian sejenis yang berfokus pada evaluasi dan perbaikan keamanan aplikasi web, khususnya pada sistem informasi berbasis web di sektor agribisnis lokal.
3. Secara praktis, penelitian ini meningkatkan tingkat keamanan Sistem Informasi Pencatatan Hasil Panen Sawit (SawitGoDigi) melalui penutupan kerentanan yang telah diverifikasi melalui retesting dan dinyatakan tidak dapat dieksploitasi kembali.
4. Secara praktis, penelitian ini menghasilkan dokumentasi teknis pengujian keamanan dan langkah perbaikan yang dapat digunakan oleh pengembang dan pengelola sistem sebagai acuan dalam pengelolaan keamanan aplikasi web secara sistematis dan terukur.