BAB I

PENDAHULUAN

1.1 Latar Belakang

Penggunaan aplikasi *web* telah mengalami transformasi secara signifikan di sejumlah industri, termasuk pendidikan. Aplikasi *web* ini membuat administrasi data dan interaksi pengguna lebih mudah diakses dan efisien, sebagai akibat dari kemajuan teknologi informasi yang cepat. Namun, kemajuan ini mendatangkan banyak risiko terhadap keamanan aplikasi web. Serangan *siber* yang menargetkan kelemahan aplikasi *web*. Serangan *siber* yang menargetkan kelemahan aplikasi *web* dapat menyebabkan kerugian moneter, pencurian data sensitif, serta merusak reputasi perusahaan atau instansi yang terkena dampaknya. (Tinambunan et al., 2024)

Penerapan transformasi digital di perguruan telah menjadikan aplikasi *web* sebagai elemen infrastruktur utama dalam pengelolaan data akademik. Universitas Siliwangi telah mengadopsi aplikasi SINTESYS sebagai pusat integrasi data mahasiswa dan dosen. Akan tetapi, semakin rumitnya arsitektur aplikasi *web* tersebut juga memicu lonjakan risiko ancaman keamanan siber. Aplikasi *web* tanpa perlindungan yang kuat kerap menjadi sasaran utama serangan siber yang mengancam kerahasiaan, integritas, serta ketersediaan (CIA Tiad) informasi akademik mahasiswa (Supriyatna et al., 2024)

Pentingnya penelitian ini semakin terbukti mengingat tingkat ancaman keamanan aplikasi *web* di Indonesia yang telah mencapai ambang batas mengkhawatirkan. Menurut data statistik keamanan siber global, Indonesia kerap

menjadi target serangan *credential stuffing* serta eksploitasi kerentanan aplikasi *web* dengan peringkat dalam insiden kebocoran data digital, hal ini mencerminkan ketimpangan antara perkembangan cepat fitur aplikasi dan penerapan standar keamanan yang layak *(security posture)*. Dalam sistem akademik perguruan tinggi, kerentanan semacam itu tidak hanya menyebabkan kebocoran data pribadi, melainkan juga merusak kredibilitas institusi akibat manipulasi integritas data. (Nur Aini, 2022)

Selama januari 2020 sampai januari 2024 ada sekitar 3,96 miliar akun digital yang mengalami kebocoran data. Angka tersebut merupakan estimasi berdasarkan riset surfshark terhadap kasus kebocoran data di 250 negara.

Gambar 1.1 Diagram 10 Negara dengan kebocoran data terbesar (Surfshark, 2024)

Kebocoran data atau *data breach* merupakan situasi di mana data suatu akun digital dapat diakses secara tidak sah oleh pihak lain. Data yang bocor itu umumnya berupa data pribadi, seperti nama lengkap, jenis kelamin, lokasi geografis, alamat *e-mail,* kata sandi akun, nomer telepon dll. Gambar di atas menjelaskan periode sepanjang januari 2020 – januari 2024 Indonesia menjadi negara dengan kebocoran data terbanyak ke-8 di dunia, dengan estimasi 94,22 juta akun bocor.

Kerangka kerja OWASP Top 10 digunakan sebagai acuan utama karena memuat kategori risiko keamanan aplikasi *web* yang paling kritis dan banyak dijadikan standar oleh praktisi keamanan aplikasi. Dalam penelitian ini, OWASP Top 10 digunakan untuk mengklasifikasikan temuan, sedangkan validasi manual digunakan untuk membedakan antara *alert* yang bersifat indikatif dengan kerentanan yang benar-benar terbukti. Dengan demikian, hasil penelitian diharapkan tidak hanya menghasilkan daftar celah, tetapi juga memberikan profil risiko keamanan aplikasi *web* yang lebih akurat.

Berdasarkan pengamatan awal terhadap aplikasi *web* SINTESYS, terdapat indikasi kelemahan pada aspek konfigurasi keamanan, khususnya pada pengelolaan *security headers* dan atribut *cookie* sesi. Temuan awal tersebut perlu diverifikasi secara sistematis karena berkaitan langsung dengan kemungkinan serangan seperti *Clickjacking* dan penyalahgunaan sesi. Di sisi lain, mekanisme filtrasi input pada aplikasi perlu diuji untuk mengetahui apakah aplikasi memiliki ketahanan terhadap skenario serangan seperti *Cross-Site Scripting* (XSS) dan *SQL Injection.*

Permasalahan yang muncul dalam penelitian ini bukan hanya apakah aplikasi memiliki celah keamanan, tetapi juga bagaimana karakteristik celah

tersebut, kategori risikonya menurut OWASP Top 10, dampaknya terhadap *confidentiality, integrity,* dan *availability,* serta rekomendasi teknis yang paling prioritas untuk diterapkan. Oleh karena itu, penelitian ini diarahkan untuk menghasilkan evaluasi keamanan yang bersifat aplikatif dan dapat menjadi masukan langsung bagi pengelola sistem SINTESYS.

Kebaruan penelitian ini terletak pada penyusunan profil risiko keamanan aplikasi akademik berbasis kombinasi pemindaian otomatis, validasi manual, pemetaan OWASP Top 10, analisis dampak CIA, dan prioritas remediasi teknis. Berbeda dari penelitian sebelumnya yang hanya menampilkan hasil *scanning,* penelitian ini menekankan pembuktian status temuan pemisahan *true positive* dan *negative finding,* serta penyusunan rekomendasi penguatan *security posture* aplikasi akademik secara lebih terarah.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang diuraikan, ada beberapa rumusan masalah yang akan di bahas dipenelitian ini yaitu :

1. Bagaimana hasil identifikasi kerentanan keamanan aplikasi *web* SINTESYS Universitas Siliwangi menggunakan metode *Web Application Penetration Testing* berbasis OWASP Top 10?
2. Bagaimana hasil validasi manual terhadap temuan pemindaian otomatis, khususnya pada skenario *Cross-Site Scripting, SQL Injection, Clickjacking, Session Management,* dan *Insecure Direct Object Reference?*

3. Bagaimana pemetaan temuan keamanan aplikasi *web* SINTESYS ke dalam kategori OWASP Top 10 serta dampaknya terhadap aspek *confidentiality, integrity,* dan *availability*?
4. Rekomendasi teknis (remediasi) apa saja yang perlu diterapkan untuk menambal celah keamanan yang teridentifikasi, sehingga memperkuat postur keamanan aplikasi *web* SINTESYS?

1.3 Tujuan Penelitian

Tujuan penelitian ini berdasarkan rumusan masalah yang telah dibuat sebagai berikut :

1. Mengidentifikasi kerentanan keamanan aplikasi *web* SINTESYS Universitas Siliwangi menggunakan metode *Web Application Penetration Testing* berdasarkan OWASP Top 10.
2. Melakukan validasi manual terhadap hasil pemindain otomatis untuk menentukan status temuan sebagai *true positive, false positive,* atau *negative finding*
3. Menganalisis tingkat risiko dan dampak temuan terhadap *confidentiality, integrity,* dan *availability* pada aplikasi *web* SINTESYS.
4. Menyusun rekomendasi perbaikan teknis *(remediation)* yang bersifat aplikatif guna menutup celah keamanan yang ditumukan dan meningkatkan *security posture* aplikasi SINTESYS secara keseluruhan.

1.4 Manfaat Penelitian

Manfaat penelitian ini dapat memberikan gambaran mengenai kondisi keamanan aplikasi *web* yang di analisis dan di lakukan pengujian berdasarkan dari temuan-temuan kerentanan yang ada, sehingga dapat digunakan sebagai dasar untuk memperbaiki dan meningkatkan keamanan *web* yang ada.

1.5 Batasan Masalah

Ada beberapa batasan masalah yang perlu diperhatikan dalam penelitian ini, yaitu :

1. Penelitian ini hanya berfokus pada analisis kerentanan keamanan *web* SINTESYS milik Universitas Siliwangi dan tidak mencakup *web* universitas secara keseluruhan atau *web* dari prodi lain.
2. Pengujian difokuskan pada kategori risiko yang relevan dengan OWASP Top 10, khusus nya *Broken Access Control, Injection, Security Misconfiguration, Identification and Authentication Failures,* dan aspek *Session Management*
3. Metode pengujian menggunakan pendekatan *Web Application Penetration Testing* dengan kombinasi pemindaian otomatis dan validasi manual terbatas.
4. Pengujian dilakukan secara non destruktif, tidak mengubah data, tidak melakukan penghapusan data, tidak melakukan *dump* basis data, dan tidak menyebarkan informasi sensitif

5. Data yang berpotensi sensitif, seperti token, *cookie*, identitas pengguna, atau endpoint internal, harus disamarkan dalam dokumen penelitian.

1.6 Keterbatasan Peneliti

Ada beberapa batasan masalah yang perlu diperhatikan dalam penelitian ini, yaitu :

1. Pengujian dilakukan melalui pendekatan *Black-box* dan *Grey-box non-*destrutif dari sudut pandang pengguna eksternal tanpa akses terhadap kode sumber *(source code review)* maupun file konfigurasi internal server *(server-side configuration).*
2. Pengujian penetrasi dibatasi pada *attack surface* aplikasi *web* yang terekspos secara publik dan tidak mencakup pengujian insfrastruktur fisik, pengujian *Denial of Service* (DoS/DDoS), serta simulasi *Social Engineering*
3. Pengujian validasi *Session Hijacking* dan IDOR dilakukan menggunakan akun uji mandiri dengan hak akses mahasiswa terbatas guna menjaga kerahasiaan dan integritas data pengguna asli di lingkungan produksi