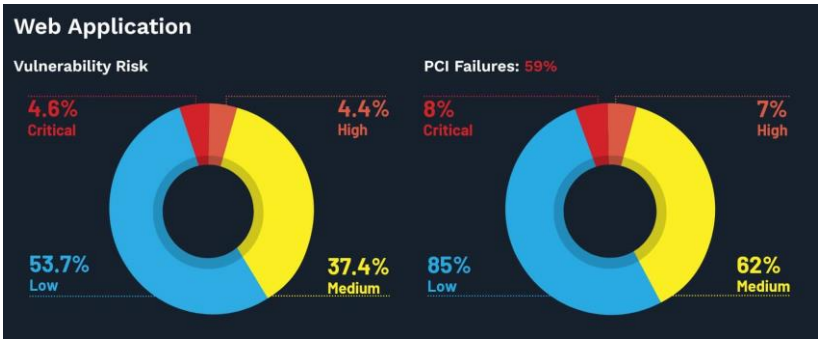
BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, kita berada di era yang penuh dengan teknologi komunikasi dan informasi. Kemajuan teknologi telah menyediakan sumber daya informasi dan komunikasi yang sangat luas dari apa yang telah dimiliki manusia. Meskipun Peran informasi mendapat sedikit perhatian dalam beberapa dekade terakhir, tetapi itu nyata, kebutuhan akan informasi dan komunikasi juga tidak kalah pentingnya dari kebutuhan manusia akan sandang dan pangan.

Era digital merupakan bentuk modernisasi atau pembaharuan teknologi yang sering dikaitkan dengan kemunculan internet dan komputer. Saat ini kita hidup di dunia digital yang serba cepat dan pintar, saling terhubung menjadi hal yang tidak bisa dihindarkan. Dalam keseharian kita saat ini tidak bisa terlepas dari ketergantungan akan penggunaan gawai seperti komputer tablet ataupun telepon pintar. Dalam dunia digital, informasi menjadi aset yang sangat berharga dimana pertukaran informasi dan data menjadi sangat cepat dan mudah. Dengan kemudahan yang didapat karena kemajuan teknologi, tentu memunculkan pula ancaman terhadap keamanan informasi. Terdapat pihak- pihak yang memiliki integritas buruk dan tidak bertanggung jawab melakukan tindakan illegal demi mendapatkan informasi yang diinginkan. Hal ini menjadikan individu, organisasi, maupun negara menjadi sangat rentan akan serangan terhadap sistem informasi seperti hacking, cybercrime, skimming dan lain-lain. Jika informasi yang dicuri kemudian disalahgunakan akan berdampak kerugian, kekacauan, dan menjadi sangat berisiko jika informasi tersebut termasuk kategori informasi bersifat sangat rahasia.

Laporan Statistik Kerentanan Edgescan 2022 menganalisis tingkat keparahan kerentanan aplikasi web. Ditemukan bahwa hampir satu dari sepuluh kerentanan dalam aplikasi yang terhubung ke internet dianggap berisiko tinggi atau kritis. Ini naik menjadi 15 persen jika target biasanya memproses pembayaran online.



Gambar 1. 1 Statistik Risiko Kerentanan Aplikasi Web Tahun 2022

Universitas Islam Ahmad Dahlan Sinjai (UIAD) merupakan salah satu perguruan tinggi yang menyediakan Portal Akademik yang biasa disebut SIAKAD, yaitu sistem informasi yang berfungsi sebagai integrator informasi akademik yang terdapat di berbagai unit akademik (program studi/fakultas) sekaligus sebagai sarana komunikasi antar civitas akademika kampus.

Berangkat dari hal tersebut, tentunya sistem ini tidak terlepas dari kemungkinan terjadinya serangan dan rentan terhadap kerusakan dan pencurian data. Meskipun pada system SIAKAD sebelumnya belum pernah terjadi, namun masih terdapat beberapa kelemahan-kelemahan pada system ini, yang bisa saja dimanfaatkan oleh orang-orang yang tidak bertanggung jawab, oleh karena itu tujuan dari penelitian ini adalah untuk menghindari kemungkinan terjadinya hal-hal yang tidak diinginkan tadi. Adapun metode yang akan penulis gunakan yaitu Risk rating dari Open Web Application Security Project (OWASP). Penelitian ini menghasilkan 2 faktor untuk memperkirakan Likelihood dan Impact. Dari masing-masing faktor terdapat 3 resiko yang ditemukan yaitu risk severity High, risk severity Medium dan risk severity Low. Hasil penilaian resiko ini dapat dijadikan acuan untuk menyadari resiko yang mungkin terjadi sehingga dapat mengambil tindakan untuk mencegah dan mengatasi resiko tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka didapatkan rumusan masalah sebagai berikut :

1. Apa saja celah keamanan yang didapatkan pada sistem Informasi Akademik Universitas Islam Ahmad Dahlan Sinjai.
2. Bagaimana menghitung dan menganalisis risiko terkait system dengan menggunakan metode Risk Rating dari Open Web Application Security Project (OWASP) .
3. Apa saja solusi yang bisa diberikan terkait dari celah keamanan yang didapatkan.

1.3 Ruang Lingkup

Adapun ruang lingkup pada penilitian ini, antara lain :

1. Analisis dilakukan pada Sistem Informasi Akademik (SIAKAD) Universitas Islam Ahmad Dahlan Sinjai.
2. Penelitian dilakukan dengan acuan Metode Risk Rating dari Open web Application Security Project (OWASP).
3. Vulnerability Testing menggunakan tools OwaspZap
4. Melakukan evaluasi untuk menentukan priotitas dan memberikan solusi dari celah keamanan yang ditemukan

1.4 Tujuan Penelitian

Berdasarkan uraian latar belakang masalah, tujuan dari penelitian ini yaitu :

1. Menemukan celah keamanan pada sistem informasi akademik.
2. Menghitung dan mengukur tingkat risiko keamanan pada sistem informasi akademik
3. Menentukan prirotas dan memberikan solusi dari celah keamanan yang ditemukan

1.5 Manfaat Penelitian

Tidak hanya meningkatkan pengetahuan penulis terkait dengan keamanan informasi, tapi penelitian ini juga diharapkan dapat membantu meningkatkan awareness keamanan informasi pada sistem informasi akademik perguruan tinggi terkait.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyusunan laporan akhir ini terbagi menjadi 5 pokok bab pembahasan yang terstruktur, dengan kajian yang saling terkait dan berhubungan sehingga dapat dijadikan sebagai acuan dalam menyelesaikan penilitian ini, berikut sistematika penulisannya :

1. **Bab 1 : Pendahuluan**

   Pada tahapan ini terdapat beberapa sub pembahasan yang mendasari dimulainya penelitian ini, yang memuat latar belakang, rumusan masalah, tujuan serta maanfaat penelitian,

2. **Bab 2 : Tinjauan Pustaka dan Dasar Teori**

   Berisi gambaran umum dan materi pendukung yang relevan dengan penilitian yang dilakukan.

3. **Bab 3 : Metode Penelitian**

   Pada tahapan ini membahas mengenai metode dan tahapan-tahapan yang digunakan dalam penelitian

4. **Bab 4 : Implementasi dan Pembahasan**

   Tahapan dimana menjelaskan proses dan hasil yang didapatkan berdasarkan metode yang digunakan.

5. **Bab 5 : Penutup**

   Berisi kesimpulan dari seluruh hasil penelitian yang dilakukan juga berisi saran sebagai acuan penelitian selanjutnya.