BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan digitalisasi yang sangat pesat telah membawa berbagai manfaat dan perubahan positif dalam berbagai aspek kehidupan, terutama dalam bidang komunikasi dan akses terhadap informasi [1]. Salah satu sektor yang turut mengalami dampak signifikan dari transformasi ini adalah bidang teknologi informasi, khususnya dalam pengembangan website. Website kini menjadi media utama bagi berbagai organisasi, termasuk perpustakaan, untuk menyediakan informasi kepada masyarakat luas serta mempermudah akses terhadap layanan yang disediakan [2]. Namun, seiring kemudahan yang diberikan, perkembangan teknologi web ini juga menuntut perhatian serius terhadap aspek keamanannya. Keamanan sistem informasi, khususnya *website*, sangat penting untuk melindungi data pengguna, menjaga kerahasiaan, dan memastikan integritas informasi yang dikelola oleh organisasi.

Perpustakaan berfungsi sebagai tempat penyimpanan dan pengelolaan berbagai koleksi pustaka yang diatur secara sistematis sehingga dapat ditemukan dengan cepat dan mudah ketika dibutuhkan [3]. Seiring dengan kemajuan teknologi, banyak perpustakaan telah beralih menjadi perpustakaan digital, yakni perpustakaan yang menyediakan layanan berbasis web untuk memfasilitasi akses informasi secara daring. Salah satu inovasi penting dalam pengelolaan perpustakaan digital adalah *Online Public Access Catalog (OPAC),* yaitu sistem katalog terpasang yang dapat diakses oleh publik untuk menelusuri data koleksi seperti judul buku, pengarang, lokasi penyimpanan, serta status ketersediaan bahan pustaka. Implementasi OPAC terbukti meningkatkan efisiensi, efektivitas, dan kualitas layanan perpustakaan, serta memperluas akses informasi bagi pengguna. [4].

Universitas Maritim Raja Ali Haji (UMRAH) sebagai salah satu perguruan tinggi negeri di Kepulauan Riau, turut mengimplementasikan sistem OPAC untuk mendukung layanan akademik di Perpustakaan UMRAH. Sistem OPAC UMRAH yang diakses melalui http://opac.umrah.ac.id ini menyediakan layanan pencarian koleksi buku, jurnal, dan karya ilmiah lainnya secara daring. Keberadaan OPAC

menjadi vital dalam menunjang kegiatan pembelajaran, penelitian, dan pengembangan akademik di lingkungan universitas.

Namun demikian, penggunaan sistem berbasis web seperti OPAC juga menimbulkan tantangan baru, terutama terkait aspek keamanan informasi. Aspek ini kerap kali kurang mendapatkan perhatian dibandingkan dengan tampilan visual atau desain antarmuka sistem. Padahal, keamanan *website* merupakan fondasi utama dalam menjaga kepercayaan pengguna, melindungi data pribadi, serta memastikan kerahasiaan dan integritas informasi yang dikelola organisasi. Pengabaian terhadap aspek keamanan dapat menimbulkan risiko seperti pencurian data, manipulasi informasi, hingga perusakan tampilan situs yang berpotensi menurunkan reputasi lembaga. Oleh karena itu, pemahaman dan penerapan keamanan *website* seharusnya menjadi prioritas utama sejak tahap awal pengembangan sistem [5].

Pengujian keamanan secara berkala sangat penting untuk mengidentifikasi serta menutup celah kerentanan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab. Sejumlah penelitian menunjukkan bahwa kerentanan seperti *SQL Injection* dan *Cross-Site Scripting* (XSS) masih sering ditemukan dan berpotensi dimanfaatkan untuk mencuri data sensitif atau merusak sistem [6].

penelitian yang dilakukan oleh Mu'min et al. [7] menemukan bahwa Sistem Informasi Akademik (SIA) STIKES Guna Bangsa Yogyakarta memiliki 12 kerentanan keamanan, termasuk empat kerentanan tingkat *medium* seperti *Absence of Anti-CSRF Tokens dan Cross-Domain Misconfiguration, Missing Anti Clickjacking Header, dan vulnerability JS Library* yang dapat dieksploitasi melalui serangan berbasis input pengguna. Penelitian lain yang dilakukan oleh G.A. Saputra et al. [8] juga menunjukkan bahwa sistem informasi akademik berbasis web juga rawan terhadap serangan *SQL Injection* dan XSS akibat lemahnya pengamanan pada *form input* data. Ini menjadi perhatian serius mengingat data yang dikelola oleh sistem informasi akademik dan OPAC sangat sensitif dan harus dilindungi dari penyalahgunaan.

Salah satu metode yang efektif untuk mengidentifikasi dan mengevaluasi potensi kerentanan tersebut adalah *penetration testing*. Metode ini merupakan simulasi serangan terhadap sistem dengan tujuan menemukan celah keamanan

sebelum dimanfaatkan oleh pihak yang tidak berwenang.. Menurut penelitian yang dilakukan oleh Umar et al. [9] *penetration testing* pada aplikasi web mampu mengungkapkan berbagai kerentanan yang sering kali tidak terdeteksi melalui pengujian fungsional biasa.

Dalam pelaksanaan *penetration testing*, beberapa *tools* yang umum digunakan di antaranya adalah OWASP ZAP (*Zed Attack Proxy*) untuk mendeteksi kerentanan XSS dan CSRF, Burp Suite untuk melakukan analisis interaktif terhadap lalu lintas HTTP/HTTPS dan mengidentifikasi parameter rentan, serta SQLMap untuk mendeteksi dan mengeksploitasi kerentanan *SQL Injection.* Dan dalam penelitian lain juga melakukan kombinasi penggunaan *tools* OWAPS ZAP, Burp Suite, dan SQLMap dalam penelitiannya untuk menemukan kerentanan dalam aplikasi web [10].

Berdasarkan pentingnya peran OPAC dalam mendukung kegiatan akademik di UMRAH serta adanya potensi ancaman terhadap keamanan aplikasi web, maka diperlukan penelitian untuk menguji tingkat keamanan *website* Perpustakaan UMRAH dengan menggunakan metode *penetration testing*. Penelitian ini bertujuan untuk mengidentifikasi kerentanan yang terdapat pada sistem serta memberikan rekomendasi teknis guna memperkuat dan meningkatkan keamanan *website* OPAC UMRAH di masa mendatang.

B. Perumusan Masalah

Berdasarkan latar belakang penelitian yang telah diuraikan diatas, maka rumusan penelitian ini adalah "Bagaimana tingkat keamanan sistem website perpustakaan Universitas Maritim Raja Ali Haji menggunakan metode *Penetration Testing*?".

C. Batasan Penelitian

Batasan maslah dalam penelitian ini adalah sebagai berikut :

1. Penelitian ini dilakukan pada *website* perpustakaan Universitas Maritim Raja Ali Haji yang diakses pada URL http://opac.umrah.ac.id.
2. Pengujian Keamanan dilakukan menggunakan pendekatan *black-box testing*, tanpa akses terhadap kode sumber konfigurasi server, maupun *database internal*.

3. *Tools* yang digunakan terbatas pada OWASP ZAP dan Pentest-Tools, dengan fokus pada identifikasi kerentanan dasar.
4. Ruang lingkup pengujian bersifat *non destruktif,* sehingga *eksploitasi* hanya dilakukan sebatas pembuktian celah tanpa merusak atau memanipulasi data.
5. Penelitian risiko kerentanan dilakukan menggunakan standar *CVSS,* dan penelitian hanya memberikan saran rekomendasi.

D. Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah tujuan penelitian adalah untuk menguji tingkat keamanan OPAC pada *website* perpustakaan Universitas Maritim Raja Ali Haji menggunakan metode *penetration testing*.

E. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan beberapa manfaat terutama pada :

1. Pengelola Perpustakaan UMRAH

   Memberikan informasi detail mengenai celah keamanan yang terdapat pada sistem OPAC, serta merekomendasikan Langkah-langkah mitigasi yang dapat dilakukan untuk meningkatkan keamanan data dan layanan perpustakaan.
2. Pengembangan *Website* Perpustakaan UMRAH

   Memberikan gambaran nyata tentang jenis-jenis kerentanan umum yang sering muncul pada aplikasi web, sehingga dapat dijadikan acuan dalam merancang sistem yang lebih aman di masa depan.
3. Akademisi dan Peneliti selanjutnya:

   Sebagai referensi dan dasar pengembangan penelitian lebih lanjut dalam bidan keamanan siber, khususnya terkait penerapan *metode penetration testing* pada sistem informasi perpustakaan.