BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, perpustakaan digital telah menjadi sarana penting dalam mengelola dan menyediakan akses terhadap informasi [1]. Perpustakaan digital memungkinkan pengguna untuk mengakses berbagai jenis literatur, jurnal, dan buku elektronik dengan mudah melalui platform *online*. Keuntungan ini tidak hanya mempermudah akses informasi, tetapi juga meningkatkan efisiensi dan kenyamanan bagi pengguna. Namun, keamanan aplikasi perpustakaan digital merupakan aspek penting yang perlu diperhatikan agar data pengguna tetap aman [2].

Dalam konteks Desa Damai, perpustakaan digital merupakan salah satu infrastruktur penting yang mendukung peningkatan akses terhadap informasi bagi warga. Dengan adanya perpustakaan digital, warga dapat mengakses berbagai materi bacaan tanpa harus datang ke perpustakaan fisik. Namun, keamanan aplikasi perpustakaan digital di Desa Damai belum pernah secara formal diuji, sehingga kerentanan pada sisi autentikasi belum diketahui dengan pasti. Oleh karena itu, perlu dilakukan pengujian keamanan yang komprehensif untuk memastikan bahwa aplikasi perpustakaan digital ini aman dari serangan dan ancaman yang mungkin terjadi [3].

Salah satu aspek keamanan yang penting dalam aplikasi perpustakaan digital adalah autentikasi [4]. Autentikasi digunakan untuk memverifikasi identitas pengguna yang ingin mengakses sistem perpustakaan digital. Dari beberapa observasi yang telah dilakukan ditemukan beberapa kekurangan dari form login aplikasi pepustakaan digital, Pertama, tidak ada indikator password kuat pada form registrasi, meningkatkan risiko pengguna membuat password lemah. Kedua, kurangnya sanitasi karakter khusus pada form login membuka

celah serangan SQL injection. Terakhir, ketiadaan CAPTCHA meningkatkan risiko serangan brute force oleh bot.

Dari beberapa celah keamanan autentikasi pada aplikasi perpustakaan digital desa damai, serangan seperti *SQL Injection, Session Hijacking,* dan *Brute Force* dapat menjadi ancaman serius terhadap keamanan autentikasi. *SQL Injection* melibatkan penyisipan kode *SQL* yang berbahaya ke dalam *input* pengguna [5], lalu serangan *session hijacking* adalah serangan yang dilakukan oleh penyerang dengan tujuan mengambil alih sesi atau *session* yang sedang berjalan antara pengguna (*client*) dan server. Pada umumnya, saat pengguna berhasil melakukan otentikasi (*login*) ke suatu aplikasi atau situs web, sebuah sesi (*session*) akan dibuat dan diidentifikasi oleh *server*. Informasi session ini digunakan oleh *server* untuk mengenali pengguna yang telah terotentikasi dan memberikan akses yang sesuai [6], sedangkan *Brute Force* mencoba semua kemungkinan kombinasi kata sandi untuk mendapatkan akses yang tidak sah. Oleh karena itu, penting untuk menguji keamanan aplikasi perpustakaan digital di Desa Damai terhadap serangan-serangan ini [7].

Penelitian sebelumnya telah menunjukkan bahwa serangan *SQL Injection, Session Hijacking, dan Brute Force* masih menjadi ancaman yang signifikan bagi aplikasi web di berbagai sektor [8]. Pada aplikasi perpustakaan digital, serangan-serangan ini dapat mengakibatkan kerentanan pada sistem autentikasi, mengakibatkan kebocoran data pengguna dan potensi penyalahgunaan [9]. Oleh karena itu, pengujian keamanan aplikasi perpustakaan digital di Desa Damai perlu dilakukan untuk mengidentifikasi dan mengatasi kerentanan yang mungkin ada.

Pengujian keamanan aplikasi perpustakaan digital di Desa Damai tidak hanya penting untuk melindungi data pengguna, tetapi juga untuk menjaga reputasi dan kepercayaan pengguna terhadap aplikasi tersebut. Keamanan yang lemah dapat mengakibatkan hilangnya kepercayaan masyarakat terhadap aplikasi perpustakaan digital dan mengurangi adopsi serta penggunaan aplikasi tersebut. Oleh karena itu, pengujian keamanan menjadi langkah penting dalam memastikan keberlanjutan dan keandalan perpustakaan digital di Desa Damai [4].

Dalam pengujian keamanan, perlu diperhatikan standar keamanan yang diakui secara internasional. Salah satu standar keamanan yang dikenal luas adalah yang dikeluarkan oleh *Open Web Application Security Project (*OWASP*)* [10] . OWASP memberikan pedoman dan praktik terbaik dalam mengamankan aplikasi web, termasuk aplikasi perpustakaan digital. Sehingga teknik pengujian yang diusulkan dalam penelitian akan dibandingkan dengan hasil pengujian menggunakan setandar keamanan OWASP. Dengan demikian membandingkan hasil pengujian keamanan dengan hasil pengujian menggunakan standar yang ditetapkan oleh OWASP, dapat dievaluasi sejauh mana validitas hasil pengujian menggunakan teknik yang diusulkan pada penelitian ini [10].

OWASP terdapat beberapa fitur fitur yang memungkinkan melakukan pengujian beberapa serangan seperti *SQL injection, session hijacking, dan brute force.* Sehingga OWASP bisa menjadi perbandingan yang sangat pas dengan serangan yang diajukan penulis dalam penelitian ini [10].

Melalui pengujian keamanan aplikasi perpustakaan digital di Desa Damai, diharapkan bahwa kerentanan yang mungkin ada pada sisi autentikasi dapat diidentifikasi dan diperbaiki secara efektif. Dengan meningkatkan keamanan aplikasi perpustakaan digital, warga Desa Damai akan dapat menggunakan layanan perpustakaan digital dengan percaya diri dan merasa aman terhadap privasi dan data pribadi mereka. Selain itu, pengujian keamanan ini juga dapat memberikan manfaat yang lebih luas dengan memberikan panduan dan rekomendasi umum bagi pengembang aplikasi perpustakaan digital di berbagai daerah.

1.2 Permasalahan

Dalam konteks ini, permasalahan yang dihadapi adalah keamanan *form login* dalam aplikasi web perpustakaan digital. *Form login* ini merupakan titik masuk utama bagi pengguna untuk mengakses aplikasi, dan kerentanan pada *form login* dapat mengakibatkan ancaman serius terhadap keamanan aplikasi secara keseluruhan. Oleh karena itu, diperlukan pengujian keamanan untuk mengetahui

sejauh mana aplikasi web perpustakaan digital mampu melindungi diri dari serangan *SQL injection*, *Session Hijacking,* dan *brute force.*

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

1. Menguji keamanan aplikasi web perpustakaan digital pada sisi autentikasi terhadap serangan *SQL injection, Serangan Session Hijacking,* dan *serangan brute force.*
2. Melakukan perbandingan tentang hasil pengujian manual menggunakan serangan *SQL Injection, Session Hijacking,* dan *Bruteforce* dengan hasil pengujian menggunakan setandar keamanan *OWASP.*
3. Menyusun rekomendasi perbaikan dan penguatan keamanan untuk aplikasi web perpustakaan digital.

1.4 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Mengetahui tingkat keamanan *form login* dalam aplikasi web perpustakaan digital dan melindungi informasi sensitif pengguna.
2. Menyediakan wawasan tentang kerentanan aplikasi web perpustakaan digital terhadap serangan *SQL injection, Session Hijacking,* dan *brute force.*
3. Memberikan informasi perbandingan tentang pengujian manual menggunakan serangan *SQL Injection, Session Hijacking,* dan *Bruteforce* dengan *OWASP*.
4. Memberikan rekomendasi perbaikan dan penguatan keamanan yang dapat diimplementasikan pada aplikasi web perpustakaan digital.
5. Meningkatkan kesadaran akan pentingnya pengujian keamanan secara teratur dalam pengembangan aplikasi web perpustakaan digital.