BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi bermanfaat dalam berbagai aspek kehidupan baik dalam bidang hukum, politik, sosial budaya, ekonomi maupun pendidikan. Banyaknya manfaat efisiensi dan efektivitas yang diperoleh dari perkembangan teknologi membawa kemudahan dalam kehidupan manusia. Perpustakaan digital dalam lingkup perguruan tinggi merupakan salah satu contoh pemanfaatan teknologi informasi dibidang akademik. Perpustakaan digital menyediakan data atau informasi yang dapat dijangkau melalui *search engine* (mesin pencarian), tidak dibatasi oleh ruang dan kesediaan akses maupun multiakses dalam titik balik informasi (Mukhtarullah, 2021). Biasanya perpustakaan digital dibuat dalam bentuk *website* atau aplikasi *website*. Sama halnya dengan perpustakaan konvensional, perpustakaan digital juga berfungsi untuk mengelola hasil karya baik dalam bentuk tulis, cetak, maupun karya rekam secara ahli untuk memenuhi kebutuhan pendidikan baik akademik maupun non akademik, penelitian, pelestarian informasi, hiburan para pemustaka seperti yang tercatut dalam pasal 43 tahun 2007 Undang-Undang Republik Indonesia tentang perpustakaan.

Repository Unjaya merupakan perpustakaan digital perguruan tinggi berbasis *website* dengan fungsi publikasi, milik Universitas Jenderal Achmad Yani Yogyakarta beralamat *domain repository.unjaya.ac.id*. *Website* ini merupakan *website* khusus yang dibuat untuk menyimpan, mengelola, dan menyebarkan berbagai jenis informasi dan materi akademik dari Universitas Jenderal Achmad Yani Yogyakarta mencakup tugas akhir, jurnal penelitian, riset mahasiswa, publikasi ilmiah dan berbagai bentuk data yang relevan dengan lingkungan akdemik. Penggunaan website sebagai perpustakaan digital disertai dengan resiko munculnya permasalahan baru terkait dengan *cybercrime* atau istilah yang digunakan untuk kejahatan yang dilakukan melalui komputer dan teknologi sebagai

pendukung seperti pengiriman pesan yang melecehkan, penyusupan ke dalam sistem komputer secara tidak sah dan tindak kriminal lain (Bossler & Berenblum, 2019). Bentuk *cybercrime* yang berpotensi mengancam *website Repository* Unjaya dapat berupa plagialisme online, pencurian karya tulis, pembajakan konten, penipuan akademik, dan serangan terhadap platform penulisan. Variabel pengelolaan karya tulis digital *Privacy*, *Accuracy*, *Property* dan *Accessibility* (PAPA) dipertimbangkan dalam melakukan upaya pengamanan perpustakaan digital, berikut adalah 4 variabelnya (Mukhtarullah, 2021) yaitu ;

1. *Privacy* (Privasi)

   Perpustakaan digital wajib menjunjung tinggi kerahasiaan informasi penulis.
2. *Accuracy* (Akurasi)

   Kepercayaan terhadap koleksi perpustakaan digital bergantung pada kesesuaian konten yang disediakan dengan sumber aslinya.
3. *Property* (Kepemilikan)

   Karya yang tersedia di perpustakaan digital adalah milik penulis, sehingga penting untuk selalu mencantumkan nama penulis dan menjaga integritas karya tersebut.
4. *Accessibility* (Keterjangkauan)

   Meskipun perpustakaan digital memungkinkan akses yang luas dan mudah, tetap ada batasan tertentu mengenai bagian mana yang bisa diakses atau diunduh, yang mana perlu diatur dalam ketentuan khusus.

Kerugian dalam ruang lingkup perguruan tinggi yang dapat timbul dari *cybercrime* tersebut adalah penurunan kredibilitas akademik, pelanggaran kebijakan institusi, pembatasan karier akademik, kerusakan hubungan interpersonal, dan biaya hukum dan finansial. Saat ini keamanan yang dimiliki oleh *website Repository* Unjaya masih terbatas, hal ini dapat dilihat dengan jelas dari munculnya bar notifikasi *“ Not Secure “* pada saat *website* ini diakses. Hal ini menandakan bahwa koneksi antara pengguna dan *website* tidak dienskripsi sehingga input dan *output* data melalui *website* beresiko terhadap perentasan,

penyadapan dan berbagai ancaman lainnya (Lahitani dkk., 2024). Berbagai cara dapat dilakukan untuk melindungi *website* dari kejahatan atau serangan pihak tidak bertanggung jawab.

Salah satu langkah yang dapat dilakukan untuk mencegah hal tersebut adalah dengan melakukan pengujian *website* dengan *penetration testing* (Spoto dkk., 2019). *Penetration testing* adalah percobaan yang dilakukan untuk menyerang *website* target dengan tujuan untuk mengetahui celah pada keamanan sistem dari *website* target (Ary dkk., 2020). *Penetration testing* harus dilakukan untuk mengetahui sebanyak apa celah keamanan yang ada pada sebuah aplikasi *website*, agar nantinya pihak pengelola *website* dapat melakukan evaluasi demi keamanan para pengguna. Maka dari itu penelitian ini perlu dilakukan untuk menjaga keutuhan dan menghindari potensi kerugian yang dapat ditimbulkan oleh *website Repository* Unjaya, dalam penelitian ini penulis melakukan "Analisis Kerentanan pada *Domain Repository*.Unjaya.Ac.Id Menggunakan Metode *Open Source Security Testing Methodology Manual* (OSSTM)" untuk menemukan kerentanan dan tingkat keamanan, serta mengkategorikan keamanan *website* berdasarkan *RAV Score*.

1.2 PERUMUSAN MASALAH

Dari latar belakang yang dikemukakan, dalam penelitian ini terkait analisis *website Repository* Unjaya untuk menemukan kerentanan yang ada didalam domain *repository.unjaya.ac.id* dengan menggunakan metode *Open Source Security Testing Methodology Manual (OSSTMM).*

1.3 PERTANYAAN PENELITIAN

1. Bagaimana cara menganalisis kerentanan sistem pada situs *web repository.unjaya.ac.id* menggunakan metode *Open Source Security Testing Methodology Manual* (OSSTMM)?
2. Dari RAV *Score* yang telah diperoleh apakah termasuk kedalam katergori *website* dengan kemanan sempurna, keamanan kurang atau keamanan berlebih?

1.4 TUJUAN PENELITIAN

Penelitian ini dilakukan untuk menganalisis tingkat keamanan *website repository.unjaya.ac.id* untuk menemukan kerentanan dan mengkategorikan keamanan sistem berdasarkan *RAV Score* yang diperoleh menggunakan metode *Open Source Security Testing Methodology Manual (OSSTMM)* versi 3.0.

1.5 MANFAAT HASIL PENELITIAN

1. Bagi penulis:

a. Memahami standard keamanan *website*

b. Menjadi acuan karier penulis kedepannya, terutama dalam bidang *vulnerability assessment* dan keamanan *cyber*

2. Bagi pihak pengembang:

a. Memberikan pemahaman mendalam tentang celah kerentanan yang ada pada *website Repository* Unjaya agar pihak pengembang bisa meningkatkan keamanan pada website tersebut.

b. Mempermudah perbaikan pada celah-celah kerentanan yang ditemukan

3. Bagi pembaca dan pengguna:

Sebagai literasi mengenai kerentanan *website*, meningkatkan kesadaran keamananan dan kewaspadaan terhadap data pribadi.