BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini semua *Website* institusi dalam pendidikan dan edukasi memiliki situs *Web*, setiap situs *Web* tersebut memiliki tingkat keamanan yang beragam, tetapi seiring dengan berjalannya waktu dapat menimbulkan berbagai ancaman ke situs *Web* tersebut yang memiliki informasi dan juga data yang sangat rentan terkena serangan. Ketika terhubung ke dunia luar atau internet setiap situs *Web* rentan terhadap serangan disebabkan situs *Web* yang tidak update dari sisi keamanan situs *Web*. Namun setiap serangan yang ditujukan pada setiap situs *Web* yang memiliki tingkatan yang berbeda seperti edukasi dan pendidikan akan jatuhnya reputasi dikarenakan memiliki data dan informasi yang sensitif atau yang sangat privasi tidak untuk dipublikasikan, maka informasi dan data yang dimiliki akan jatuh ke pihak yang menyalahgunakan. Contoh dari serangan tersebut ialah seperti *SQL Injection*. Terjadinya *SQL Injection* dikarenakan *security* atau keamanan pada situs *Web* masih kurang.

Berdasarkan permasalahan diatas ialah,salah satu yang difokuskan disini mengenai keamanan dan melakukan penilaian risiko terhadap sistem informasi dan data dari sebuah situs *Web* institusi dalam pendidikan dan edukasi. Pada semua situs *Web* yang sudah terhubung ke internet seperti situs *Web* ac.id, sch.id dan *website* yang termasuk institusi pendidikan, tidak semua memiliki keamanan yang 100% aman dalam *SQL Injection*[1][2], semua situs *Web* memiliki celah untuk dimanfaatkan isi dari situs *Web* dan hasil isinya tersebut terdapat informasi dan data. Menurut hasil penelitian yang dilakukan oleh Pinzon (2010)[3] tentang *SQL Injection* diperoleh akurasi kerentan situs *Web* hampir sebesar 90% yang memiliki tingkat keamanan situs *Web* yang sangat rentan untuk diserang[2][4][3].

Proyek akhir ini akan menggunakan metode *clustering K-Means*, *scan* situs *Web Vulnerable*, *Risk Rank, OWASP (The Open Web Application Security Project) Top 10 2013* [5][6] sebagai pembanding dalam pembobotan risiko, dan menggunakan parameter *Directory Information, Educational Information &*

Personally Identifiable (Ferpa, 2020) dalam membantu menyelesaikan masalah. Untuk teknik ini ialah untuk melakukan pengecekkan situs *Web* yang memiliki risiko dengan menggunakan pemindai situs *Web Vulnerable*, ketika situs *Web* tersebut sangat rentan dan memiliki informasi dan data lalu akan dilakukan menggunakan metode *clustering Simple K-Means*, metode *clustering Simple K-Means* ini ialah mengelompokkan data-data dan informasi, dengan menggunakan teknik *SQL Injection* dari sebuah situs *Web* institusi guna untuk mengetahui data dan informasi yang sensitive atau valid, dan melakukan analisis dengan melakukan pengelompokkan data dan informasi dengan menggunakan *Simple K-Means*. Dan hasil dari pengumpulan data dan informasi tersebut maka akan dinilai berdasarkan tingkatan bahaya atau dilakukan skor dengan menggunakan *Risk Rank*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah diuraikan oleh penulis diatas, rumusan masalah yang diperoleh dari proyek akhir ini adalah,mengetahui *tools Acunetix* untuk memberikan informasi mengenai situs *Web* yang memiliki kelemahan / *Vulnerable*, teknik *SQL Injection* untuk mendapatkan informasi dan data dengan menggunakan *tools havij*, lalu data yang sudah didapatkan maka dikelompokkan dengan menggunakan metode *clustering Simple K-Means* dan untuk mengetahui tingkatan risiko *Website* yaitu menggunakan *Risk Ranking Low Medium* dan *High*.

1.3 Tujuan

Tujuan penyusunan Proyek Akhir ini ialah :

a) Membuat Sistem *Risk Rank* untuk mengetahui tingkat risiko institusi dengan melakukan penetrasi, pengelompokkan data dan analisis risiko.
b) Parameter yang diukur yaitu Risk Rank / Tingkatan Risiko data & *Website*.

1.4 Batasan Masalah

Batasan masalah meliputi:

a) Proyek akhir ini menggunakan *tools Acunetix* untuk analisis celah dari situs *Web* institusi.
b) Melakukan penetrasi *SQL Injection* dengan menggunakan *Havij* pada setiap situs *Web* untuk mengetahui data informasi Institusi yang tereskpos ,

c) Melakukan teknik *clustering Simple K-Means* / atau pengelompokkan data pada situs *Web* apabila data nya memiliki tingkat kerentanan yang rendah ,

d) Melakukan identifikasi hasil akhir pada Situs *Web* yang memiliki risiko tinggi atau memiliki celah untuk *SQL Injection* dengan menggunakan metode *Risk*