BAB I PENDAHULUAN

I.1 Latar Belakang

Pada era saat ini perkembangan teknologi semakin pesat, terutama dalam sektor pendidikan. Berbagai institusi pendidikan sudah menerapkan media pembelajaran melalui aplikasi *website.* Tentunya hal tersebut perlu memperhatikan sebuah keamanan informasi yang dapat meminimalisir resiko, melindungi data, dan informasi dari ancaman atau serangan yang ada. Salah satu contohnya, serangan *SQL Injection* yang mengarah ke *server database* dengan menyisipkan pernyataan SQL berbahaya kemudian *database* mengeksekusi *query* tersebut. Serangan ini masih sering dilakukan dikarenakan kurangnya kesadaran keamanan para developer, kode yang rentan, hingga sistem yang tidak diperbarui. Karena hal tersebut, *SQL Injection* termasuk kategori *Top 3 (A03:2021 – Injection)* pada *OWASP Top 10 Web Application Security Risk.* Dengan adanya serangan tersebut penyerang dapat mencuri data, memanipulasi atau memodifikasi data guna menipu pengguna atau melakukan kejahatan lainnya.

Kondisi ini perlu menjadi perhatian salah satunya Institusi XYZ yang memiliki aplikasi penentuan peminatan berbasis aplikasi *website*. *Website* ini menyimpan banyak data sensitif, seperti informasi mahasiswa maupun civitas akademik. Hingga saat ini, *website* belum dilakukan *security testing* dan langsung memasuki tahapan *Go-Live*, sehingga kemungkinan masih terdapat celah keamanan, seperti kebocoran data pada *website* ataupun adanya perubahan data yang diperlukan. Jika informasi ini jatuh ke tangan yang salah dapat berdampak pada penyalahgunaan data/infomasi mahasiswa maupun civitas akademik, hingga merusak nama baik Institusi XYZ. Maka dari hal tersebut, diperlukan adanya pengujian terhadap *website* akademik penentuan peminatan. Penelitian ini menerapkan metode atau kerangka kerja keamanan PTES dengan tujuan mengetahui kemungkinan eksploitasi yang terjadi dalam sebuah sistem. Dalam simulasi penyerangannya akan disesuaikan juga dengan kebutuhan penelitian ini.

I.2 Perumusan Masalah

Adapun rumusan masalah yang mendasari dari penelitian yang akan dilakukan diantaranya sebagai berikut:

1. Bagaimana cara mengetahui kondisi celah keamanan terhadap serangan *SQL Injection* pada *website* akademik penentuan peminatan?
2. Bagaimana hasil serangan *SQL Injection* dapat digunakan untuk mengelola kondisi celah keamanan yang ada pada *website* akademik penentuan peminatan?

I.3 Tujuan Penelitian

Adapun tujuan dari penelitian yang akan dilakukan diantaranya sebagai berikut:

1. Hasil dari pengujian serangan *SQL Injection* terhadap *website* akademik penentuan peminatan.
2. Menggunakan kerangka kerja keamanan PTES untuk menghasilkan *security mitigation* berdasarkan hasil pengujian celah keamanan pada *website* akademik penentuan peminatan.

I.4 Batasan Penelitian

Adapun batasan dari penelitian yang akan dilakukan diantarannya sebagai berikut:

1. Parameter yang diukur dalam penelitian ini adalah tingkat kerentanan dan solusi berdasarkan hasil data keluaran dari *tools Exploitation* yang dilakukan.
2. Tahapan *Exploitation* yang dilakukan hanya berupa *SQL Injection* yang masuk ke dalam kategori *Top 3 (A03:2021 – Injection)* pada OWASP *Top 10 Web Application Security Risk.*
3. Penelitian ini terbatas hanya sampai tahap *Exploitation* dan dilanjutkan dengan tahap *Reporting.*
4. Hasil *penetration testing* berupa rekomendasi yang dapat dijadikan sebagai bahan pertimbangan perbaikan *website* akademik penentuan peminatan.

I.5 Manfaat Penelitian

Adapun manfaat dari penelitian yang akan dilakukan diantarannya sebagai berikut:

1. Pengguna *Website*

   Data/informasi pengguna *website* aman dan terhindar dari penyalahgunaan data, *website* dapat berjalan sesuai operasional tanpa adanya gangguan teknis, serta mampu meningkatkan kepercayaan dan kepuasan pengguna dalam penggunaan layanan *website*.

2. Pengembangan *Website*/Developer

   Hasil penelitian dapat membantu mengetahui berbagai informasi celah keamanan yang ada, melakukan perbaikan, dan bahan pertimbangan guna meminimalisir potensi ancaman dan serangan yang akan terjadi kedepannya, sehingga dapat melakukan langkah mitigasi yang tepat bagi sistem *website* dalam peningkatan keamanan informasi pada aplikasi *website* tersebut, baik secara teknis maupun non-teknis.

3. Institusi XYZ

   Nama baik Institusi XYZ dapat terjaga dengan baik dan terhindar dari penyalahgunaan data maupun informasi lainnya terkait website, serta mampu meningkatkan kepercayaan pengguna terhadap Institusi tersebut.

4. Peneliti

   Bagi peneliti dapat belajar pentingnya keamanan suatu sistem/aplikasi dan dapat memahami lebih dalam sistem/aplikasi yang sedang diuji. Selain itu, peneliti secara tidak langsung dapat mengembangkan dan meningkatkan keahlian dalam *cyber security*, serta berkontribusi terhadap keamanan *website* Intitusi XYZ.