BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi telah mengalami kemajuan yang signifikan seiring dengan peningkatan penggunaannya. Di era internet saat ini, akses informasi menjadi lebih mudah dan cepat. Namun, hal ini juga menyebabkan informasi menjadi aset yang sangat berharga dan rentan untuk disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, keamanan informasi menjadi sangat penting. Dalam konteks ini, keamanan informasi melibatkan aspek keamanan teknologi komputer dan jaringan yang digunakan untuk menyimpan, mengirim, dan memproses informasi secara online. (Nurul dkk., 2022).

Pemanfaatan sistem informasi untuk aktivitas organisasi pendidikan seperti perguruan tinggi dapat menjadi faktor penunjang kesuksesan dan kemajuan dari perguruan tinggi seperti mengatur perkuliahan, dosen, dan nilai mahasiswa. Perlu disadari bahwa penggunaan sistem informasi berbasis *web application* memiliki kelemahan–kelemahan keamanan yang dapat dieksploitasi oleh pihak luar melalui jaringan internet. Apabila hal ini terjadi, maka organisasi dapat mengalami berbagai macam kerugian. Eksploitasi yang dimaksud adalah penyalahgunaan wewenang dalam mengakses informasi, seperti merubah informasi yang ada atau bahkan menghapus informasi-informasi penting yang ada di dalam *web application*.

Sebagai salah satu perguruan tinggi di Indonesia, Institusi XYZ yang menerapkan sistem informasi memiliki *website* Akademik Penunjang Pengajaran yang digunakan untuk mengupload bukti pembayaran mahasiswa yang ingin mengambil sertifikat yang telah di ikuti dari Lab ERP. Namun hingga saat ini *Website* Akademik Penunjang Pengajaran yang digunakan Institusi XYZ belum pernah dilakukan uji keamanannya. Pada proses pembuatan *website* di institusi XYZ, pihak terkait tidak melakukan proses *security testing* sehingga ketika *website* tersebut telah terpublikasi akan banyak celah keamanan yang masuk ke dalam *website* tersebut. Ini menimbulkan kekhawatiran akan terjadinya eksploitasi pada celah yang ada pada *website* Akademik Penunjang Pengajaran.

Berdasarkan informasi di atas, diperlukan solusi untuk mencegah serangan cyber terhadap *website* untuk menjaga data dan sistem yang berjalan didalamnya. Salah satu *website* yang memiliki fungsionalitas untuk memverifikasi data adalah *website* verifikasi pembayaran sertifikat praktikum. *Website* tersebut berfungsi untuk memvalidasi data pembayaran mahasiswa dalam mengikuti praktikum, dikarenakan data pembayaran praktikum akan berpengaruh pada penilaian akhir semester. Maka dari itu, *website* harus dilindungi agar validasi data di dalammya dapat berjalan dengan baik, oleh sebab itu perlu dilakukan pengujian eksploitasi untuk mendapatkan hasil kerentanan pada *Website* Akademik Penunjang Pengajaran pada Institusi XYZ untuk mencari celah kerentanannya. Kerentanan yang ditemukan akan dianalisis dan dilakukan mitigasi menggunakan metode PTES. Pada penelitian in menggunakan lima *tools* yang akan membantu simulasi eksploitasi celah keamanan pada *website* target, yaitu SQLMap, Bupsuite, jSQL Injection, dan Havij. Setelah dilakukan pengujian eksploitasi dan penetration testing pada *website* tersebut, diharapkan akan meminimalisir serangan cyber yang dapat merugikan pengguna *website*.

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah di sebutkan diatas, rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana hasil analisis dari pengujian kemanan pada *web* akademik penunjang pengajaran Institusi XYZ menggunakan SQL *Injection*?
b. Bagaimana rekomendasi yang akan di berikan pada *web* akademik penunjang pengajaran Institusi XYZ dari hasil pengujian celah keamanan yang telah dilakukan?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah di sebutkan diatas, penelitian ini bertujuan untuk:

a. Hasil analisis dari pengujian kemanan pada *web* akademik penunjang pengajaran Institusi XYZ menggunakan metode SQL *Injection*.

b. Rekomendasi yang akan di berikan pada *web* akademik penunjang pengajaran Institusi XYZ dari hasil pengujian celah keamanan yang telah dilakukan.

I.4 Batasan Penelitian

Agar penelitian ini tidak keluar dari ruang lingkupnya, pada proses penelitian ini diberikan beberapa batasan diantaranya terbatas pada hal-hal berikut:

1. Pada penelitian ini, tahap eksploitasi hanya dilakukan menggunakan SQL *Injection*.
2. Hasil dari tahap eksploitasi berupa celah keamanan atau kerentanan pada *Website* Akademik Penunjang Pengajaran.
3. Penelitian ini terbatas pada eksploitasi, dan dilanjutkan tahap *reporting*.

I.5 Manfaat Penelitian

Adapun Manfaat penelitian ini adalah sebagai berikut:

1. Penelitian ini bermanfaat bagi *developer web* institusi XYZ, mengetahui kerentanan yang terdapat pada *Website* Akademik Penunjang Pengajaran yang dapat digunakan untuk melakukan peningkatan keamanan pada *Website* Akademik Penunjang Pengajaran agar dapat ditangani dan meminimalisir ancaman keamanan yang dapat terjadi.
2. Bagi peneliti lain yang bergerak dalam bidang sistem informasi, penelitian ini bermanfaat sebagai referensi dalam melakukan sebuah analisis *Penetration Testing* pada *Website* dan juga memberikan referensi penggunaan *tools* yang digunakan pada penelitian ini
3. Penelitian ini memiliki manfaat bagi pengguna *Website* Akademik Penunjang Pengajaran Institusi XYZ. Dengan penelitian ini, pengguna *website* akan merasa lebih aman dan nyaman ketika mengakses *website* tersebut.