BAB I PENDAHULUAN

I.1 Latar Belakang

Seiring dengan perkembangannya, menerapkan sistem informasi sebagai cara untuk mempermudah pengelolaan suatu institusi harus menjadi hal yang diperhatikan, terutama dalam bidang pendidikan (Putu dkk., 2021). Salah satu contoh penerapan sistem informasi adalah sebuah *website*. Dengan segala kemudahannya, pemanfaatan sistem informasi ini sangat sensitif dikarenakan terdapat berbagai data penting yang rentan terhadap pencurian data. Kerentanan atau *Vulnerability* ini akan menjadi ancaman bagi pengguna jika ditemukan oleh *black hat* atau *hacker* jahat, dengan cara menyalahgunakan data-data pengguna untuk dijadikan peluang keuntungan bagi mereka, dan dengan adanya celah kerentanan ini pihak yang berkaitan harus menjamin keamanan pengguna untuk memberikan rasa aman dan nyaman.

Berbicara mengenai celah keamanan, menurut OWASP *Top* 10 *Most Critical Web Application Security Risks*, menempatkan *Cross Site Scripting* berada diposisi ketiga (Kurniawan, 2019). XSS merupakan jenis serangan dengan tipe injeksi, penyerang dapat menyisipkan *script* berbahaya ke halaman *website.* Serangan ini membuat seolah-olah hal berbahaya tersebut berasal dari *website* itu sendiri. Akibatnya penyerang dapat mengendalikan browser secara tidak sah, penyerang dapat mencuri data sensitif dari target melalui *cookie* atau *form* data yang telah dimodifikasi yang kemudian dikirim kepada penyerang, dan dapat menyisipkan file berbahaya ke halaman *website* (Yulianingsih, 2017).

Maka dari itu keamanan *website* adalah salah satu faktor penting yang harus diperhatikan dalam pengembangan sebuah *website*. Keamanan *website* dapat menjamin bahwa informasi yang disimpan dan dikirim melalui *website* terlindungi dari pihak yang tidak berwenang. Sangat penting untuk selalu memperhatikan dan meningkatkan keamanan *website* agar dapat melindungi privasi pengguna dan menjaga integritas data.

Institusi XYZ merupakan sebuah institusi pendidikan yang menggunakan bantuan sistem informasi untuk mengatur dan mengendalikan pengelolaan proses

bisnisnya. Salah satu produk dari bantuan itu adalah sebuah *Website* Akademik Penunjang Administrasi. *Website* tersebut digunakan untuk proses administrasi sehingga didalamnya terdapat banyak sekali data sensitif yang berharga seperti data diri dosen, mahasiswa, dan pegawai, juga terdapat data kelulusan mahasiswa, data topik tugas akhir, dan data mata kuliah. Pada proses pembuatan *website*, pihak terkait tidak melakukan proses *security testing*. Sehingga ketika *website* tersebut telah terpublikasi (*go live*) akan banyak celah keamanan yang masuk ke dalam *Website* tersebut. Perlu dilakukan *Security Testing* terhadap celah keamanan XSS dikarenakan celah ini memiliki potensi kerentanan yang tinggi dan berpotensi untuk pencurian data sensitif sehingga dapat dilakukan manipulasi data, jika hal tersebut terjadi dapat menghilangkan kredibilitas institusi terkait. Maka dari itu, pada penelitian ini melakukan sebuah project *Security Mitigation* terhadap *Website* Akademik Penunjang Administrasi di Institusi XYZ dengan menggunakan kerangka kerja PTES (*Penetration Testing Execution Standard)* dengan tujuan mengurangi risiko keamanan sistem atau data sehingga dapat terhindar dari ancaman yang ada.

I.2 Perumusan Masalah

Adapun perumusan masalah yang mendasari penelitian ini adalah sebagai berikut:

a. Bagaimana hasil analisis pengujian celah keamanan XSS yang dilakukan terhadap *Website* Akademik Penunjang Administrasi?
b. Bagaimana hasil mitigasi celah keamanan XSS yang dilakukan terhadap *Website* Akademik Penunjang Administrasi?

I.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini dilakukan adalah sebagai berikut:

a. Analisis dari pengujian celah keamanan XSS yang dilakukan terhadap *Website* Akademik Penunjang Administrasi.
b. Hasil dari mitigasi celah keamanan XSS yang dilakukan terhadap *Website* Akademik Penunjang Administrasi.

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. Proses Eksploitasi yang dilakukan terhadap *website* hanya menggunakan metode pengujian XSS.
2. Proses pengujian celah keamanan yang dilakukan menggunakan *tools* OWASP ZAP, Burp Suite, dan XSStrike.
3. Proses *Mitigation* dilakukan jika mendapat persetujuan dari pihak developer.
4. Proses *Mitigation* yang dilakukan terhadap celah XSS tidak mengubah atau menghapus *source code* yang sudah tersedia pada *website*.

I.5 Manfaat Penelitian

Adapun manfaat yang didapat dari penelitian ini adalah sebagai berikut:

1. Bagi institusi terkait, Penelitian ini berguna untuk mendeteksi celah kerentanan XSS pada *website* terkait dan mengetahui sejauh mana celah kerentanan ini dapat di eksploitasi. Juga memberikan mitigasi terhadap celah kerentanan ini untuk mengurangi celah-celah keamanan yang ada.
2. Bagi peneliti lain yang bergerak dalam bidang sistem informasi, penelitian ini bermanfaat sebagai referensi dalam melakukan sebuah analisis *Penetration Testing* pada *website* tertentu dan juga memberikan referensi penggunaan *tools* yang digunakan pada penelitian ini.
3. Bagi Pengguna *website*, Penelitian ini berguna untuk memberikan rasa aman ketika menggunakan *Website* Akademik Penunjang Administrasi.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

BAB I Pendahuluan

Bab ini berisikan mengenai latar belakang penulisan, perumusan masalah, tujuan penelitian, batasan penelitian, dan manfaat penelitian terhadap penelitian ini.

BAB II Tinjauan Pustaka

Bab ini berisikan mengenai penjelasan dasar dasar teori yang digunakan dalam penelitian ini dan literatur yang berkaitan dengan penelitian ini.

BAB III Metodologi Penelitian

Bab ini berfokus pada metode yang akan digunakan dalam penelitian ini. Penjelasan tentang langkah-langkah yang akan diambil, model konseptual yang digunakan untuk tahapan pengujian, analisis, dan pemberian solusi dari penelitian ini akan diuraikan. Selain itu, bab ini akan memberikan sistematika penyelesaian masalah yang akan diikuti dalam penelitian yang dilakukan.

BAB IV Perancangan dan Skenario Pengujian

Bab ini berisikan tentang rancangan pengujian dan skenaio pengujian yang di lakukan pada penelitian ini mencakup lingkup *Pre-engagement Interaction, Intelligence Gathering*, dan Skenario Pengujian XSS.

BAB V Hasil dan Analisis Pengujian

Bab ini menjelaskan hasil dan analisis pengujian terhadap celah XSS yang telah dilakukan dan memberikan *reporting* berupa rekomendasi solusi penambalan celah dan melakukan mitigasi untuk menambal celah keamanan XSS.

BAB VI Kesimpulan dan Saran

Bab ini berisikan intisari dari penelitian yang telah dilakukan yaitu *Security Mitigation* terhadap *Website* Akademik Penunjang Administrasi di Institusi XYZ Menggunakan Kerangka Kerja PTES dan menjelaskan saran yang diberikan untuk penelitian selanjutnya.