1. PENDAHULUAN

1.1 Latar Belakang

Seiring berjalannya waktu dan jaman, sebagian besar aktivitas yang tadinya dilakukan secara luring telah bergeser menjadi daring. Ada berbagai media untuk menyampaikan informasi di mana audiens tidak perlu berada secara fisik untuk menerima informasi tersebut. Salah satu contoh dari media penyampaian informasi yang kerap digunakan khususnya untuk perusahaan atau bisnis adalah *Website. Website* merupakan sarana yang kerap dipakai untuk menyampaikan informasi mengenai produk atau bisnis yang dikerjakan dan juga merupakan sebuah *platform* dilakukannya aktivitas jual beli antar perusahaan dan konsumen. Semakin besar atau sukses suatu perusahaan, data yang dimiliki perusahaan tersebut menjadi semakin berharga. Karena data itu berharga, akan banyak kompetitor atau orang jahat yang akan menyerang sistem dari suatu perusahaan dan mencuri data-data penting untuk menjatuhkan perusahaan itu maupun menjual data penting untuk kepentingan pribadi. Banyak serangan siber yang dapat dilakukan untuk mendapatkan data, dan salah satunya adalah dengan mencuri *credentials* dari *user* yang telah tercatat pada *website* terkait. (AMT IT Solutions, 2023) menyatakan bahwa penyerangan dapat dilakukan melalui *website* dan informasi *user* dapat didapatkan dan jika hal ini terjadi, maka penyerang dapat mengakses banyak data serta informasi penting dan dapat menjualnya di *dark web.* Semakin luas *role user* yang dibobol oleh penyerang, semakin besar kerugian yang didapatkan perusahaan dikarenakan data yang diambil bisa lebih luas berdasarkan *role*. Maka dari itu, dibutuhkan suatu perlindungan dan antisipasi pada keamanan siber agar perusahaan dapat mencegah terjadinya kebocoran data.

Salah satu perusahaan di Indonesia yang menggunakan *website* sebagai penunjang proses bisnisnya adalah PT XYZ. PT XYZ merupakan perusahaan yang bergerak di bidang Otomotif. Perusahaan ini memiliki berbagai jenis bisnis seperti lelang mobil dan juga jual beli mobil. Kedua bisnis ini dapat dilakukan secara luring maupun daring, namun untuk langkah pertama seperti pendaftaran dan transaksi tetap dilakukan secara daring, yaitu melalui *website* perusahaan. Konsumen diharuskan membuat akun terlebih dahulu jika ingin melakukan transaksi, dan karena adanya proses transaksi, maka akan ada portal lain untuk mengecek data penjualan dari konsumen yang hanya dapat diakses oleh internal perusahaan. Lantas, hal ini membuat PT XYZ ini menyimpan banyak data penting untuk kelangsungan proses bisnisnya. Selain itu Seperti yang sudah dibahas sebelumnya, semakin besar suatu perusahaan, maka akan terdapat data-data penting yang diincar oleh kompetitor

maupun orang jahat yang tidak bertanggung jawab untuk merugikan perusahaan. Yang menjadi target utama adalah mereka yang memiliki akses atau dampak signifikan terhadap data penting, dan seringkali akses tersebut diperoleh melalui kredensial seorang pengguna. Jika kredensial itu sudah diketahui oleh pihak yang tidak bertanggung jawab, perusahaan itu akan mengalami kerugian besar. Selain perusahaan, konsumen yang telah memberikan data pribadi untuk proses transaksi juga dapat mendapat akibatnya karena data mereka telah dicuri dan dapat disalahgunakan. Hal ini dapat berefek juga pada citra dari perusahaan. Untuk melindungi data perusahaan, perlu dilakukan suatu aksi pencegahan yaitu dengan melakukan *Penetration Test* secara berkala. Hal ini dilakukan untuk mencari celah dari sistem yang berjalan dan melakukan penanganan agar penyerang tidak dapat menyerang pada celah tersebut.

Penetration Testing atau biasa disebut *PenTesting* adalah serangan yang dilakukan secara resmi pada suatu sistem untuk mengevaluasi dan mencari kerentanan dari keamanan sistem atau jaringan. Ada beberapa metode *PenTesting* seperti *Social Engineering, Wireless Testing, Web Application Testing,* dan *Network Penetration Testing.* Untuk melakukan *PenTesting,* metode yang digunakan disesuaikan dengan tujuan dan kebutuhan yang ada. Pada penelitian kali ini, akan dilakukan *PenTesting* menggunakan metode *Cross-Site Scripting* (XSS). Metode *Cross-Site Scripting* dipilih menjadi metode yang digunakan dalam penelitian ini karena *Website* XYZ merupakan sebuah sarana transaksi dimana dilakukannya jual beli dengan konsumen. Pada proses ini, akan membutuhkan data *user,* entah dari pihak konsumen maupun internal perusahaan sendiri untuk kelangsungan proses bisnis pada PT XYZ. Oleh karena itu, sebuah kredensial pada *Website* XYZ yang digunakan untuk menunjang proses bisnis PT XYZ ini merupakan suatu yang krusial sehingga harus dilakukan pengamanan dengan tingkat tinggi. Dengan menggunakan metode *Cross-Site Scripting,* diharapkan *output* yang didapatkan bisa meningkatkan keamanan pada *Website* XYZ dan meminimalisir kerentanan pada sistem.

Selain ada beberapa metode dalam *PenTesting,* ada juga beberapa tipe *PenTesting* yaitu *White Box Testing, Black Box Testing,* dan *Grey Box Testing.* Dalam penelitian ini, akan dilakukan *PenTesting* tipe *Black Box,* dimana selama pengujian, tidak semua informasi mengenai *Website* XYZ diketahui. Penyerangan dengan menggunakan metode *Cross-Site Scripting* akan dilakukan pada *server Website* XYZ dan *tools* yang akan digunakan adalah OWASP ZAP dan Burp Suite dan pada Kali Linux. OWASP ZAP adalah alat keamanan aplikasi

web gratis dan *open-source* yang efektif dalam menemukan kerentanan, memungkinkan pengguna untuk mencegat dan memodifikasi permintaan dan respons secara *real-time*, dan didukung oleh komunitas *open source* yang aktif (Muhammad Gibran Abraham Danialdo, Fariz Andri Bakhtiar, Mahendra Data, 2023). Setelah dilakukan *scanning* kerentanan, akan dilakukan penyerangan dan eksploitasi pada *website* menggunakan Burp Suite. Dengan demikian, hasil dari penelitian ini dapat diharapkan dapat mengurangi potensi kerentanan pada *Website* XYZ dan meningkatkan perlindungan secara keseluruhan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka rumusan masalahnya adalah:

1. Bagaimana mengidentifikasi dan mencegah kerentanan *Cross-Site Scripting* pada *Website* XYZ?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas maka tujuan dari penelitian ini adalah:

1. Menemukan dan melakukan eksploitasi kerentanan yang ada pada *Website* XYZ melalui proses *PenTesting* menggunakan metode *Cross-Site Scripting*.

1.4 Ruang Lingkup

Ruang lingkup dibatasi pada :

- Operation System yang digunakan adalah Kali Linux, yang akan dijalankan menggunakan VirtualBox.
- *Reconnaissance* dilakukan menggunakan *Tools* Netcraft.
- *Vulnerability Assessment* akan menggunakan *Tools* Nessus, XSpear, dan Acunetix.
- Tipe *PenTesting* yang dilakukan adalah *Black Box Penetration Testing*.
- Target yang diuji adalah *Website* XYZ.
- *Output* dari *PenTesting i*ni adalah laporan dan rekomendasi solusi yang dapat dilakukan oleh perusahaan guna mencegah terjadinya penyerangan terhadap sistem perusahaan.

Seluruh hasil secara keseluruhan dari PenTesting pada Website XYZ akan dibuat dalam bentuk laporan. Dalam laporan tersebut akan mencakup beberapa hal berikut :

Hasil Uji :

- Daftar temuan XSS yang ditemukan.
- Detail teknis dari setiap temuan, termasuk URL dan parameter yang terlibat.
- Tingkat keparahan setiap temuan (ringan/ sedang/ berat) berdasarkan hasil *Vulnerability Assessment*.

Bukti Pendukung :

- Tangkapan layar dari setiap langkah instalasi hingga penyerangan.
- Bukti kode skrip yang dieksploitasi.

Rekomendasi Perbaikan :

- Saran untuk mengatasi atau mengurangi risiko XSS.
- Rekomendasi tentang perubahan yang dapat dilakukan untuk mencegah risiko XSS.

Risiko dan Dampak :

- Penilaian risiko dan dampak dari temuan XSS.
- Potensi kerugian yang dapat disebabkan oleh penyalahgunaan celah XSS.

Ringkasan Eksekutif :

- Kesimpulan singkat tentang keamanan website yang diuji.
- Rekomendasi umum solusi untuk peningkatan keamanan.
- Setelah rekomendasi diberikan, perusahaan akan melakukan perbaikan sesuai rekomendasi. Lalu akan dilakukan serangan kembali untuk melihat apakah rekomendasi dapat berjalan atau tidak dan akan dimasukkan ke dalam laporan akhir.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat bermanfaat bagi :

1. Keamanan dari *Website* XYZ dapat ditingkatkan lebih lagi.
2. Pencegahan terjadinya serangan pada celah sistem *Website* XYZ.
3. Integritas perusahaan jadi lebih terjamin karena data perusahaan tidak gampang diretas.

1.6 Metodologi Penelitian

Langkah-langkah dalam pengerjaan skripsi :

1. Persiapan & *Planning*
2. Pengujian terhadap metode *Cross-Site Scripting*
3. Penemuan *Cross-Site Scripting Vulnerabilities*
   3.1 Kerentanan ditemukan
   3.2 Kerentanan tidak ditemukan
4. Membuat Laporan Akhir Kesimpulan Pengujian

1.7 Sistematika Penulisan

Penulisan pada skripsi ini dibagi menjadi beberapa bab, yaitu :

- Bab I : Pendahuluan
  Bab ini berisikan judul, latar belakang, perumusan masalah, ruang lingkup, tujuan penelitian, metodologi dan manfaat penelitian.
- Bab II : Teori Penunjang
  Bab ini berisikan teori yang mendasari metode dan implementasi pada penelitian ini.
- Bab III : Analisis dan Desain Sistem
  Bab ini akan membahas mengenai analisis dan desain dari sistem pengerjaan yang akan dilakukan.
- Bab IV : Implementasi Sistem
  Pada bab ini akan berisi mengenai implementasi sistem dari Desain Sistem.
- Bab V : Pengujian
  Bab ini akan berisi hasil uji dari *Penetration Testing* sesuai implementasi sistem.
- Bab VI : Kesimpulan dan Saran
  Bab ini berisikan kesimpulan dari segala hasil temuan dan saran bagi perusahaan.