BAB 1 PENDAHULUAN

1.1 Latar Belakang

Pada Era Digital 4.0 penggunaan teknologi sudah biasa digunakan untuk keberlangsungan perusahaan salah satunya *website*. *website* merupakan media internet yang menghubungkan dokumen secara local atau jarak jauh. Dokumen yang terdapat *website* dan *link* pada *website* dapat digunakan oleh user atau pengguna untuk berpindah dari satu halaman website ke halaman lain (*hypertext*) baik antar halaman yang dihosting di *server* seluruh dunia. (Anendya, 2024)

PTPN XI atau biasa dikenal PT Perkebunan Nusatara merupakan perusahaan perkebuanan yang dimiliki oleh Negara atau sering kita sebut BUMN. Didalam Perusahaan ini memiliki banyak sekali PG (pabrik gula dan jenis usaha lainya) untuk menyatukan pajak dari semua jenis usaha tersebut PTPN XI menggunakan *website* untuk mengontrol dan menyatukan pajak untuk dikelola. Dalam *website* pajak PTPN XI mengandung beberapa data *critical* seperti pajak keluaran dan masukan yang biasanya berisi tentang pembelian bahan baku, bibit, pupuk hingga data vendor yang melakukan transaksi dengan PTPN XI oleh karena itu analisis Keamanan sistem informasi merupakan cara untuk mencegah pencurian data, akses tidak sah, dan kerusakan terhadap sistem informasi suatu perusahaan. Ada pun sistem keamanan yang digunakan untuk melindungi jaringan informasi dan data dalam komputer.

Penelitian ini menggunakan *framework* OWASP dalam pengujian analisys sistem keamanan telah banyak dilakukan, beberapa pengujian pentest atau penetration testing disebutkan bahwa metode dan alat sangat berpengaruh terhadap hasil dari sistem keamanan wesbite. (Team B. , 2023). OWASP sendiri memiliki metode yang dinamai dengan nama OWASP TOP 10 memiliki 10 kerentanan yang bertujuan untuk sebagai uji peneterasi terhadap keamanan website yang paling sering digunakan. Penelitian ini dalam melakukan *Peneration Testing* yang bertujuan untuk meningkatkan kesadaran dan meningkatakan keamanan pada aplikasi *website* dengan cara melakukan *Testing* pada *website* dengan tingkatan resiko yang berturutan dan untuk mendukung metode tersebut.

Penelitian ini menggunakan metode Grey*Box* karena peneliti melakukan penetration testing dari luar dan dibantu dari pihak internal. Dari penelitian ini dapat meningkatkan keamanan sistem informasi yang ada di perusahaan terutama pada *website* pajak PTPN XI yang memiliki data yang sensitive seperti data vendor, data pembelian bibit yang sangat dirahasiakan oleh perusahaan dan oleh karena itu keamanan sistem infromasi pada *website* dapat diperhatikan dan diprioritaskan. (Rahmalia, glints, 2024)

1.2 Perumusan Masalah

Dari latar belakang diatas dapat disimpulakan rumusan masalah :

1. Bagaimana tingkat keamanan aplikasi *website* pajak PTPN XI menurut *framework* OWASP TOP 10 2021
2. Apa resiko keamanan *website* Pajak PTPN XIn
3. Apa saja langkah yang dapat dilakukan untuk meningkatkan kemanan *website* pajak PTPN XI dengan menggunakan *framework* OWASP TOP 10

1.3 Tujuan dan Manfaat Penelitian

Ada pun tujuan dari penelitan ini:

1. Mengetahui tingkat keamanan pada *website* pajak PTPN XI dengan *framework OWASP TOP 10*
2. Mengetahui resiko keamanan *website* pajak PTPN XI dengan *framework OWASP TOP 10*
3. Meningkatkan keamanan pada *website* pajak PTPN XI dengan memberikan rekomendasi kepada PTPN XI.

Ada pun manfaat dari penelitian ini dari sisi peneliti dan perusahaan

Dari sisi perusahaan :

1. .Meningkatkan kepercayaan pengguna *website*.
2. .Mengurangi dan mencegah serangan *Cyber*.
3. .Pemantauan dan perbaikan keamanan secara terus menerus.

Dari sisi peneliti :

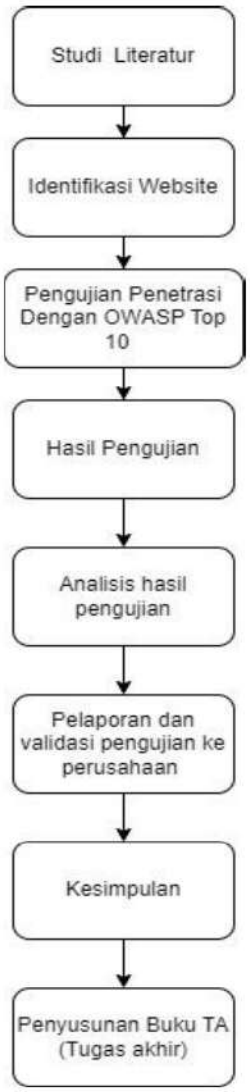
1. Pengembangan bidang keahlian yang dilakukanya peneliti terkait.
2. Pengalamaan praktis yang didapat dengan penelitian ini akan meningkatkan berpikir kritis.

1.4 Batasan Penelitian

Adapun batasan masalah dalam penelitian ini

1. Penelitian ini sebatas hanya menguji keamanan *website* pajak PTPN XI
2. Penelitian ini menggunakan metode *Greybox*
3. Pada penelitian ini mengikuti petujuk dari OWASP TOP 10
4. Penelitian ini dilakukan diluar jaringan PTPN 11
5. Penelitian ini hanya menganalisis *website* dengan melakukan uji penetrasi dengan ZAP, BuprSuite,Wappanalyzer dan pendukungnya

1.5 Prosedur Penelitian



Gambar I. 1 Struktur Pengerjaan

1.5.1 Studi Literatur

Tahap ini bertujuan untuk menjelaskan kajian pustaka dari teori-teori penunjang yang mendukung konstruksi fokus penelitian. Kegiatan ini dilakukan dengan membaca buku, jurnal, artikel laporan penelitian, dan situs-situs di internet.

1.5.2 Identifikasi *Website*

Website pajak PTPN XI adalah sebuah aplikasi *website* yang didalamnya terdapat data penting berupa pajak perusahaan yang menjadi jantung perputaran pajak untuk PTPN XI dan anak perusahaan namun beberapa waktu lalu terjadi kebocoran data yang menyebabkan hilangnya data pajak dengan ini perlu untuk

dilakukanya *Test* keamanan sistem informasi untuk menjaga dan meningkatkan keamanan *website* perusahaan.

1.5.3 Metode OWASP *TOP* 10 2021

OWASP merupakan organisasi non-profit amal di Amerika Serikat yang didirikan pada tanggal 21 April 2004 yang berdedikasi untuk membuat *framework* pengujian keamanan yang bebas digunakan oleh siapa saja. Pengujian kerentanan sistem informasi pada *website* pajak PTPN XI. OWASP Top 10 2021 adalah daftar sepuluh risiko keamanan aplikasi web paling kritis yang diidentifikasi oleh Open Web Application Security Project (OWASP). Daftar ini merupakan panduan penting bagi pengembang, penguji keamanan, dan organisasi untuk fokus pada perbaikan keamanan aplikasi web.

1.5.4 Daftar Kerentanan pada Metode OWASP *TOP* 10 2021

Pengujian Akan dilakukan dengan menggunakan metode OWASP TOP 10 yang dimana terdapat 10 kerentanan *website,* yaitu sebagai berikut :

1. A01 Broke Access Control
2. A02 Cryptographic Failures
3. A03 Injection
4. A04 Insecure Design
5. A05 Security Misconfiguration
6. A06 Vulnerable and Outdated Components
7. A07 Identification and Authetication Failures
8. A08 Software and Data Integrity Failures
9. A09 Security Logging and Monitoring Failures
10. A10 Server side Request Forgery (SSRF)

1.5.5 Hasil Pengujian Penetrasi

Setelah dilakukanya pengujian dengan menggunakan metode OWASP TOP 10 maka akan menghasilkan uji kerentana pada *website* PTPN XI.

1.5.6 Analisis Hasil Pengujian

Kegiatan ini bertujuan untuk menganalisi berdasarkan hasil pengujian menggunakan metode OWASP TOP 10 untuk menentukan keamanan PTPN XI.

1.5.7 Pelaporan dan Validasi Pengujian

Kegiatan ini bertujuan untuk melaporakan dan mevalidasi hasil dari pengujian penetrasi ke perusahaan dengan tujuan agar perusahaan mengetahui hasil pengujian dan menyetujui dari hasil yang didapat.

1.5.8 Kesimpulan

Kesimpulan berisi uraian hasil pengujian dan analisis *website* pajak PTPN XI.

1.5.9 Penyusunan Buku TA

Dalam proses ini mahasiswa yang sudah melalui tahapan-tahapan dalam melakukan penelitian akan menyusun tugas akhir.