# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi informasi saat ini berlangsung sangat cepat, dimana teknologi informasi memiliki peran penting dalam kehidupan manusia. Untuk mendapatkan informasi yang akurat, efektif, dan efisien. Salah satu teknologi informasi yang sangat berkembang penggunaannya adalah *internet*. *Internet* (kependekan dari *interconnection-networking*) adalah seluruh jaringan komputer yang saling terhubung menggunakan standar sistem global *Transmision Control Protocol/Internet Protocol Suite (TCP/IP),* sebagai protokol pertukaran paket *(paket switching communication protocol)* untuk melayani miliaran pengguna di seluruh dunia (Lin Almeina Lubis dkk, 2018). Dengan perkembangan *internet* yang sangat cepat maka manusia harus menyesuaikan terhadap perubahan yang terjadi jika tidak dapat mengikuti perkembangannya maka manusia akan tertinggal dalam bidang teknologi informasi.

Manfaat *internet* bagi pemerintahan adalah bisa mengurangi *human error* dan meningkatkan efektifitas kerja, menyediakan informasi publik yang berguna untuk pengambilan keputusan, serta memudahkan masyarakat mendapatkan layanan publik tanpa harus mendatangi Kantor Pemerintahan (Putu Sugiartawan dkk, 2018). Pemerintah Kota Payakumbuh melalui Badan Keuangan Daerah memiliki visi yaitu Terwujudnya Pengelolaan Keuangan Daerah Secara Profesional Berbasis Teknologi Informasi. Untuk itu Badan Keuangan Daerah Kota Payakumbuh telah mengembangkan salah satu layanan publik berupa aplikasi pelaporan pajak daerah secara online.

Badan Keuangan Daerah Kota Payakumbuh memiliki salah satu tugas yaitu mengelola Pendapatan Asli Daerah (PAD). Salah satu sumber Pendapatan Asli Daerah adalah Pajak Daerah, yang menyumbang sekitar 12% untuk PAD. Berdasarkan Undang-Undang Nomor 28 Tahun 2009, Tentang Pajak Daerah dan Retribusi Daerah. Pajak Daerah adalah kontribusi wajib kepada daerah yang terutang oleh orang pribadi atau badan yang bersifat memaksa berdasarkan Undang-Undang, dengan tidak mendapatkan imbalan secara langsung dan digunakan untuk keperluan daerah bagi sebesar-besarnya kemakmuran rakyat.

Salah satu upaya yang dilakukan oleh Badan Keuangan Daerah dalam meningkatkan Pendapatan Asli Daerah dari Pajak Daerah adalah dengan memberikan kemudahan kepada wajib pajak untuk melaporkan dan melakukan pembayaran pajak daerah melalui fasilitas layanan publik, yang bisa diakses oleh wajib pajak tanpa harus mendatangi langsung Kantor Badan Keuangan Daerah. Aplikasi ini bisa diakses oleh publik setiap saat di alamat **http://sptpd.payakumbuhkota.go.id**. Dengan terbukanya aplikasi ini untuk diakses oleh pihak umum, maka tidak menutup kemungkinan aplikasi ini diakses juga oleh pihak-pihak yang tidak bertanggung jawab untuk menyalahgunakan informasi. Informasi Pajak Daerah ini bersifat rahasia karena menyangkut mengenai omzet penerimaan dari wajib pajak .

Cara kerja aplikasi ini dimulai dari wajib pajak melakukan login dengan *username* dan *password* yang telah diberikan oleh Badan Keuangan Daerah, lalu mengisi *form* dengan memasukkan hasil omzet penjualannya bulan yang lalu, output nya berupa Surat Pemberitahuan Pajak Daerah (SPTPD), yang berisi data wajib pajak, besaran pajak yang dibayar, dan kode pembayaran. Dokumen yang telah dilaporkan wajib pajak ini tersimpan di dalam *webserver* Badan Keuangan Daerah.

Badan Keuangan Daerah dalam mengembangkan aplikasi pelaporan pajak daerah ini telah memiliki server dan IP publik sendiri sehingga tidak di *hosting* di tempat lain. Aplikasi web memiliki banyak kesulitan yaitu web didistribusikan melalui *client/server* yang rentan bermasalah, web bersifat *heterogen* maksudnya bisa dikembangkan dengan berbagai macam bahasa pemograman yang berbeda misalnya, PHP, Ruby, Java di sisi server dan HTML, CSS, Javascipt di sisi client, dan terakhir web bersifat dinamis sehingga pengembangan yang dilakukan perlu diuji (Pamungkas & Rochimah, 2019).

Berdasarkan laporan *Gov-CSIRT* Tahun 2019 yang dikeluarkan oleh Badan Siber dan Sandi Negara, terdapat 229 (Dua ratus dua puluh sembilan) serangan cyber

terhadap situs pemerintah yang telah ditangani oleh *Gov-CSIRT* BSSN. *Government–Computer Security Incident Response Team* (*CSIRT*) Indonesia, disingkat *Gov-CSIRT* Indonesia merupakan *CSIRT* sektor Pemerintah Indonesia yang ditetapkan pertama kali oleh Kepala Badan Siber dan Sandi Negara dalam Keputusan Kepala Badan Siber dan Sandi Negara Nomor 570 Tahun 2018 tanggal 20 Desember 2018. Sedangkan pada tahun 2019, *Gov-CSIRT* Indonesia ditetapkan melalui Keputusan Kepala Badan Siber dan Sandi Negara Nomor 199 Tahun 2019 tanggal 21 Mei 2019. Konstituen dari *Gov-CSIRT* Indonesia meliputi seluruh Pemerintah Daerah dan Pemerintah Pusat. Untuk Wilayah 1 Pemerintah Daerah serangan yang sering terjadi adalah *web defacement* sebanyak 34%, *phising* sebanyak 9%, *malware* sebanyak 13%, lain-lain sebanyak 8%, dan kerentanan sebanyak 37%.

Berdasarkan data tersebut diketahui bahwa situs milik Pemerintah Daerah juga cukup banyak di serang oleh pihak yang tidak bertanggung jawab. Kurangnya sumber daya manusia yang dimiliki oleh Pemerintah Daerah dalam manajemen server menjadi salah satu penyebab banyaknya serangan yang terjadi. Pengujian kerentanan merupakan hal yang penting dilakukan terhadap suatu aplikasi maupun pada *webserver* tempat aplikasi tersebut dijalankan, karena jika hanya pada aplikasi sudah diamankan yakni pada penulisan kode programnya, namun dari sisi *webserver* tidak diamankan maka kemanan data dan informasi tidak akan terjamin.

*Webserver* bekerja menunggu permintaan *client* yang menggunakan browser seperti *mozilla, internet explorer*, dan program *browser* lainnya. Jika ada permintaan dari *browser* maka *webserver* akan memproses permintaan itu dan kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke browser. *Web server*, untuk berkomunikasi dengan client nya (*web browser*) mempunyai protokol sendiri, yaitu *HTTP (hypertext transfer protocol*). Dengan protokol ini, komunikasi antar *web server* dengan *client*-nya dapat saling dimengerti dan lebih mudah (Pratiwi & Nuraini, 2019). Banyaknya celah keamanan yang terdapat pada situs ataupun aplikasi layanan publik Pemerintah Daerah menuntut Pemerintah Daerah untuk melakukan pengujian kerentanan (*Vulnerability Assesment*) baik dari sisi aplikasi maupun dari sisi server.

Salah satu cara untuk melakukan pengujian kerentanan adalah dengan melakukan *"Penetration Testing Execution Standar"*. *Penetration Testing Execution Standar* adalah standar pengujian yang telah ditetapkan secara internasional.

*Penetration Testing*, atau *pentesting* merupakan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan. Penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, untuk menilai apa yang mungkin didapat oleh penyerang setelah eksploitasi sukses (Aziz & Fattah, 2019).

Penelitian terdahulu yang dilakukan oleh Aziz & Fattah (2019), melakukan analisis keamanan sistem kartu elektronik dengan *Penetration Testing*, menyimpulkan bahwa layanan keamanan yang ada pada kartu *magneticstripe* adalah *confidentiality* dan *availability*, layanan keamanan tersebut cukup aman dalam penggunaan transaksi dilokasi tersebut. Penelitian berikutnya yang dilakukan (Irwan Syarifuddin, 2019), yang melakukan analisa keamanan pada website paud dikmas dengan menggunakan metode *Penetration Testing*, terdapat celah keamanan seperti *Port FTP* yang terbuka, *web application information disclosure,* dan lemahnya keamanan untuk autentikasi *login* pada website. Penelitan lainnya yang dilakukan oleh Chu & Lisitsa, (2018), Dengan melakukan *Penetration Testing of IoT* didapatkan hasil kerentanan dari tiga lapisan *layer* yaitu *application layer, network layer dan perception layer*, terdapat kelemahan password yang tidak dienkripsi, kerentanan *sniffing* dan *spoofing*. Penelitian berikutnya dilakukan oleh Krasniqi & Bejtullahu, (2018), yang melakukan pengujian keamanan terhadap 3 buah aplikasi web dengan metode *Penetration Testing*. Hasil pengujian didapatkan kelamahan berupa *missing X-XSS header protection*, *insecure transportation security protocol (TLS 1.0), sourcode disclousure* dan beberapa file *jquery* yang sudah kadaluarsa. Penelitan berikutnya dilakukan oleh Khera dkk, (2019), melakukan pengujian menggunakan metode *Penetration Testing* terhadap IP server 192.168.197.130. Hasil pengujian terdapat beberapa kelemahan yaitu terbukanya *port FTP* dan *SSH* yang bisa dilakukan *exploitasi* kedalamnya.

Berdasarkan hasil-hasil dari penelitian terdahulu yang melakukan pengujian kerentanan dengan metode *Penetration Testing*, celah-celah keamanan pada suatu aplikasi maupun server dapat diketahui secara detail. dipahami. Berdasarkan uraian yang telah dijelaskan, banyak serangan yang terjadi dan celah kemanan yang ada pada aplikasi Pemerintah Daerah sehingga perlu dilakukan pengujian kerentanan, untuk itu penulis melakukan penelitian yang dituangkan dalam bentuk tesis dengan

judul penelitian **"Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar".**

## 1.2 Perumusan Masalah

Pada tesis ini peneliti mempunyai beberapa rumusan masalah sesuai dengan permasalahan yang telah dijelaskan pada latar belakang, sebagai berikut :

1. Bagaimana melakukan pengujian kerentanan terhadap *webserver* dan aplikasi pelaporan pajak daerah pada Badan Keuangan Daerah Kota Payakumbuh.
2. Bagaimana hasil pengujian kerentanan terhadap *webserver* dan aplikasi pelaporan pajak daerah pada Badan Keuangan Daerah Kota Payakumbuh
3. Bagaimana analisis hasil pengujian kerentanan yang didapat dari *webserver* dan aplikasi Pajak Daerah tersebut.

## 1.3 Batasan Masalah

Penelitian ini memiliki beberapa batasan masalah yang bertujuan untuk mempermudah melakukan proses penelitian sehingga penelitian tidak keluar dari tujuan yang telah ditetapkan, adapun batasan masalahnya adalah sebagai berikut :

1. Penelitian ini dilakukan pada aplikasi dan *webserver* pelaporan pajak daerah di Badan Keuangan Daerah Kota Payakumbuh.
2. Menggunakan metode *Penetration Testing Execution Standar* dalam melakukan pengujuan kerentanan.
3. Jenis *exploitation* yang akan dilakukan adalah hasil dari *vulnerability analysis* yang ditemukan.

## 1.4 Tujuan Penelitian

Tugas akhir ini memiliki beberapa tujuan penelitian yang ingin dicapai sebagai berikut :

1. Menerapkan metode *Penetration Testing Execution Standar* dalam melakukan pengujian kerentanan terhadap aplikasi *webserver* pelaporan pajak daerah.
2. Menganalisis hasil pengujian kerentanan dengan metode *Penetration Testing Exceution Standar* pada aplikasi *webserver* pelaporan pajak daerah.
3. Meningkatkan keamanan aplikasi *webserver* pelaporan pajak daerah sesuai dengan standar keamanan informasi pada metode *Penetration Testing Execution Standar.*

## 1.5 Manfaat Penelitian

Berdasarkan dari tujuan penelitian yang telah ditetapkan, maka manfaat yang didapat dari penelitian adalah sebagai berikut :

1. Dari sisi Badan Keuangan Daerah memiliki manfaat :
   a. Mengetahui celah-celah keamanan pada aplikasi dan *webserver* yang dibangunnya.
   b. Memberikan rekomendasi kepada administrator server untuk melakukan perbaikan celah-celah kemanan yang ditemukan.
2. Dari sisi peneliti dan pembaca memiliki manfaat :
   a. Menambah pengetahuan dan wawasan mengenai celah-celah keamanan pada aplikasi *webserver*.
   b. Mengetahui jenis-jenis serangan yang terjadi pada aplikasi dan server.
   c. Untuk referensi dalam melakukan penelitian berikutnya.

## 1.6 Sistematika Penulisan

Penulisan penelitian ini telah mengikuti sistematika *template* yang diatur dengan tata penulisan penelitian ilmiah program studi Pascasarjana Magister Ilmu Komputer Universitas Putra Indonesia “YPTK” Padang. Sistematika penulisan laporan penelitian ini adalah sebagai berikut :

**BaBAB I PENDAHULUAN**

Pada bagian ini akan ditemukan hal-hal yang melatar belakangi penelitian, perumusan masalah, ruang lingkup penelitian, tujuan penelitian, manfaat penelitian dan sistematika penelitian.

**BAB II LANDASAN TEORI**

Menjelaskan teori dan penerapan metode Penetration Testing Execution Standar yang digunakan dalam tahap-tahap penyelesaian masalah sesuai dengan topik penelitian.

**BAB III METODOLOGI PENELITIAN**

Bagian ini menjelaskan jenis penelitian yang dilakukan, pendekatan yang digunakan, sumber data, lokasi penelitan, metode dan alat pengumpulan data serta teknik pengolahan dan analisa.

**BAB IV ANALISA DAN PERANCANGAN**

Bab ini melakukan analisa kerentanan dengan metode yang *Penetration Testing Execution Standar* dan menjelaskan perancangan software dan hardware yang akan digunakan saat penelitian berlangsung dan termasuk didalamnya perancangan pengujian yang dilakukan secara sistematis

**BAB V IMPLEMENTASI DAN HASIL**

Bagaimana mengimplementasikan pengujian kerentanan dengan melakukan exploitation pada aplikasi webserver target dan hasil pengujian yang telah dilakukan pada aplikasi webserver target.

**BAB VI KESIMPULAN DAN SARAN**

Berisikan kesimpulan dan sarah dari hasil penelitian.