BAB I

PENDAHULUAN

1.1 Latar Belakang

Pemanfaatan sistem informasi saat ini sangat banyak digunakan untuk menunjang kinerja suatu organisasi. Sistem informasi berbasis web menjadi pilihan utama dikarenakan kemudahan dalam mengakses dan mendistribusikan. Semua sistem informasi berbasis web rentan terhadap peretasan (Nagendran, Adithyan, Chethana, Camillus & Bala, 2019). Dibutuhkan suatu keamanan dalam sebuah sistem informasi berbasis web (Nur, Na'am, Nurcahyo & Arlis, 2019).

Tahun 2019, terdata sebanyak 4241 (empat ribu dua ratus empat puluh satu) aduan yang terdiri dari 699 aduan tidak terverifikasi dan 3542 (tiga ribu lima ratus empat puluh dua) aduan terverifikasi. Proses verifikasi meliputi *proof of concept* dari bukti-bukti laporan (screenshoot, link, database, *correlated file*) maupun kelengkapan identitas pelapor. Kerentanan merupakan jenis aduan siber yang paling banyak diajukan (Badan Siber Sandi Negara [BSSN], 2019).

Sistem informasi puskesmas terpadu adalah aplikasi berbasis web yang dikembangkan Pemerintah Kota Payakumbuh melalui Dinas Komunikasi dan Informatika. Aplikasi ini dibangun untuk menunjang kinerja puskesmas. Mulai dari pendaftaran pasien hingga pengambilan obat di apotik dikelola oleh aplikasi ini. Aplikasi dapat diakses melalui jaringan publik di alamat https://sipaduko.payakumbuhkota.go.id. Dengan dibukanya akses melalui jaringan publik, aplikasi berpotensi diserang oleh peretas. Berdasarkan laporan Dinas Komunikasi dan Informatika Kota Payakumbuh, percobaan-percobaan peretasan banyak terjadi pada aplikasi tersebut.

Aktifitas peretasan sistem bukan berasal dari orang yang berada di luar organisasi saja, tetapi orang yang berada di dalam organisasi juga berpotensi melakukannya. Peretas biasanya menargetkan sistem informasi yang sudah mereka kenal dengan baik akses sebagai user (Votipka, Stevens, Redmiles, Hu & Mazurek, 2018). User yang telah diberikan otorisasi untuk

mengakses sistem, memiliki peluang yang besar untuk dapat meretas sistem tersebut.

Penetration test pada sistem perlu dilakukan untuk memastikan data yang disimpan pada server tetap aman (Setiawan & Setiyadi, 2018). *Penetration test* adalah proses yang dilakukan untuk mengungkap dan menemukan kerentanan pada suatu sistem (Simran & Sasikala, 2019). Ada tiga strategi *penetration test* berdasarkan lingkup dan jenis audit yaitu *Black Box Testing*, *White Box Testing* dan *Gray Box Testing* (Yunus, 2019). Computer Audit Assisted Techniques (CAATs) adalah teknik audit yang menggunakan bantuan perangkat lunak atau teknologi untuk membantu mempercepat penyelesaian proses audit (Wicaksono, Laurens & Novianti, 2018). *Zed Attack Proxy* (ZAP) adalah perangkat lunak proyek unggulan dari Open Web Application Security Project (OWASP) yang membantu proses *penteration test* (Ula, 2019).

Menggunakan *Web Application Firewall* (WAF) untuk melindungi aplikasi berbasis web memang dapat mencegah peretasan, akan tetapi belum menyelesaikan masalah dikarenakan kerentanan berada pada sisi aplikasi. Salah satu cara untuk mengatasi hal ini adalah dengan melakukan pengujian keamanan pada aplikasi (Clincy & Shahriar, 2018). Pada penelitian ini, penulis mengangkat judul penelitian **"Meningkatkan Keamanan Sistem Informasi Puskesmas Terpadu dengan Metode Grey-Box Penetration Test Menggunakan Computer Assisted Audit Techniques (Studi Kasus di Kota Payakumbuh)"**. Diharapkan dari hasil penelitian ini mampu meningkatkan keamanan sistem informasi puskesmas terpadu Kota Payakumbuh.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan sebelumnya, maka dapat merumuskan beberapa detail permasalahan sebagai berikut:

1. Bagaimana melakukan pengujian keamanan sistem informasi puskesmas terpadu Kota Payakumbuh dengan metode *grey-box penetration test* menggunakan *computer assisted audit techniques* (OWASP ZAP)?
2. Bagaimana hasil pengujian keamanan sistem informasi puskesmas terpadu Kota Payakumbuh dengan metode grey-box penetration test menggunakan computer assisted audit techniques (OWASP ZAP)?

3. Bagaimana memberikan rekomendasi peningkatan keamanan sistem informasi puskesmas terpadu Kota Payakumbuh dengan metode grey-box penetration test menggunakan computer assisted audit techniques (OWASP ZAP)?

1.3 Batasan Masalah

Dalam melaksanakan suatu penelitian diperlukan suatu batasan agar tidak terjadi penyimpangan dari apa yang telah direncanakan sehingga tujuan penelitian yang sebenarnya dapat tercapai. Batasan masalah yang diperlukan yaitu :

1. Sistem informasi yang dilakukan pengujian keamanan adalah sistem informasi puskesmas terpadu Kota Payakumbuh.
2. Pengujian keamanan dilakukan dengan *grey box penetration test* menggunakan teknik audit berbantuan komputer OWASP ZAP.

1.4 Tujuan Penelitian

Dalam penelitian ini dan pelaksanaannya ada beberapa tujuan yang hendak dicapai, diantaranya:

1. Melakukan pengujian keamanan pada sistem informasi puskesmas terpadu Kota Payakumbuh dengan metode *grey-box penetration test* menggunakan *computer assisted audit techniques* (OWASP ZAP) sehingga kerentanan aplikasi dapat ditemukan.
2. Menganalisis hasil pengujian kerentanan dengan metode *grey-box penetration test* menggunakan *computer assisted audit techniques* pada aplikasi sistem informasi puskesmas terpadu Kota Payakumbuh.
3. Meningkatkan keamanan sistem informasi puskesmas terpadu Kota Payakumbuh dengan metode *grey-box penetration test* menggunakan *computer assisted audit techniques* (OWASP ZAP) sehingga data dan informasi yang ada terjamin keamanannya.

1.5 Manfaat Penelitian

Penelitian ini memiliki manfaat dari sisi Pemerintah Kota Payakumbuh sebagai pemilik sistem informasi puskesmas terpadu dan dari sisi peneliti sebagai penguji keamanan:

1. Dari sisi Pemerintah Kota Payakumbuh, rekomendasi perbaikan keamanan sistem informasi puskesmas terpadu yang diberikan oleh peneliti, dapat digunakan sebagai acuan untuk meningkatkan keamanan.
2. Dari sisi peneliti dan pembaca, menambah pengetahuan dan wawasan mengenai keamanan sistem informasi.

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 :

BAB 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 pengujian keamanan 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 SISTEM

Bagian ini menjelaskan tentang proses pengujian keamanan dan hasil yang didapatkan.

BAB V IMPLEMENTASI DAN HASIL

Bagian ini membahas tentang rekomendasi perbaikan keamanan, berupa kerentanan yang ditemukan serta saran untuk memperbaikinya.

BAB VI KESIMPULAN DAN SARAN

Bagian ini berisikan kesimpulan dari penyusunan tesis serta saran-saran untuk pengembangan selanjutnya.