ABSTRAK

ANALISIS RESIKO KEAMANAN TERHADAP WEBSITE DINAS PENANAMAN MODAL DAN PELAYANAN TERPADU SATU PINTU PEMERINTAHAN XYZ MENGGUNAKAN *STANDAR PENETRATION TESTING EXECUTION STANDARD* (PTES)

Oleh:

AULIA FAKHRI

NIM: 1202164092

Perkembangan teknologi yang pesat dapat mempengaruhi setiap individu, organisasi, bahkan pemerintahan dalam penyampaian informasi secara akurat, efektif, dan efisien. Pemerintahan daerah XYZ adalah instansi yang bertugas melayani masyarakat dalam pengurusan administrasi di daerah XYZ. Informasi pemerintahan dikelola oleh Dinas Komuniasi, Informatika dan Statistika (Diskominfo) daerah XYZ sebagai instansi yang bergerak dibidang teknologi informasi. Diskominfo memanfaatkan kemajuan teknologi untuk menyampaikan informasi kepada masyarakat daerah XYZ dan di luar daerah XYZ melalui *website* dengan tujuan mempermudah dalam penyampaian informasi. Seiring perkembangan teknologi, keamanan terhadap suatu *website* menjadi sesuatu hal yang penting karena dapat mencegah serangan dari orang yang tidak bertanggung jawab, karena dapat merusak sistem atau merugikan proses bisnis yang berjalan. Dengan begitu, kita perlu melakukan pengujian terhadap kerentanan yang dimiliki oleh website tersebut yaitu dengan cara melakukan *Vulnerability Assessment* dan *Penetration Testing*. Sebelum melakukan pengujian kita perlu melakukan analisis terhadap celah keamanan yang ditemukan. Pada proses analisis ini dimana seorang penguji mesimulasikan dirinya sebagai *cracker* yang berusaha melakukan analisis celah keamanan untuk dapat masuk kedalam sistem menggunakan standar PTES. Melakukan analisis terhadap celah keamanan yang ditemukan bertujuan untuk menentukan tingkat resiko terhadap *website* target. Pada pengujian terhadap *website* pemerintahan XYZ terdapat beberapa celah keamanan dengan tingkat resiko yang berbeda, namun dilakukan verifikasi terhadap satu celah keamanan yaitu SQL *Injection.* Pada celah keamanan yang telah diverifikasi mendapatkan beberapa data pengguna berupa No.Resi, Nama Pengguna, dan tanggal perizinan beserta alasannya. Adanya celah keamanan yang ditemukan dapat dilakukan pencegahan berupa menggunakan *parameterized* SQL *query*, validasi *input* data menggunakan *reguler expression*, menambahkan escape karakter, pengecekan mode debug, pengecekan keamanan *database* yang digunakan, melakukan pengujian keamanan aplikasi *website* secara berkala, dan menggunakan perangkat keamanan *web application firewall*.

Kata kunci: analisis celah kemanan, *website*, PTES.