BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang terus berkembang pesat, keamanan informasi menjadi prioritas utama bagi setiap organisasi. Website, sebagai salah satu media utama dalam penyebaran informasi dan interaksi dengan pengguna, sangat rentan terhadap berbagai ancaman siber. Serangan terhadap website dapat menyebabkan kerugian besar, baik dari segi finansial, reputasi, maupun kepercayaan pengguna. Oleh karena itu, pengujian penetrasi atau penetration testing menjadi langkah penting dalam mengidentifikasi dan memperbaiki kerentanan yang ada pada suatu sistem.

Penetration testing adalah proses simulasi serangan terhadap sistem untuk menemukan dan mengeksploitasi kelemahan yang ada. Tujuannya adalah untuk mengidentifikasi celah keamanan sebelum penyerang yang sebenarnya melakukannya. Melalui serangkaian pengujian yang terstruktur dan sistematis, penetration testing dapat memberikan gambaran menyeluruh mengenai kondisi keamanan suatu website, mulai dari konfigurasi server, aplikasi web, hingga kebijakan keamanan yang diterapkan.

Pada laporan ini, kami melakukan penetration testing terhadap beberapa website Pemerintah Provinsi Semarang. Pengujian dilakukan dengan fokus pada identifikasi kerentanan umum seperti injeksi SQL, cross-site scripting (XSS), serta analisis terhadap konfigurasi server dan kebijakan keamanan yang ada. Hasil dari pengujian ini diharapkan dapat memberikan rekomendasi yang berguna untuk meningkatkan tingkat keamanan website, serta mencegah terjadinya serangan siber yang dapat merugikan.

Melalui laporan ini, kami berharap dapat memberikan kontribusi positif dalam upaya menjaga keamanan informasi di era digital, serta mendorong langkah-langkah proaktif dalam melindungi aset digital yang berharga.

1.2 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat keamanan website pemerintah Semarang terhadap serangan siber?
2. Apa saja kerentanan yang ada pada website pemerintah Semarang yang dapat dimanfaatkan oleh pihak tidak berwenang?
3. Bagaimana metode penetration testing dapat digunakan untuk mengidentifikasi dan mengatasi kerentanan keamanan pada website?

1.3 Tujuan

Tujuan dari penelitian ini adalah untuk:

1. Mengidentifikasi dan mengelompokkan potensi kerentanan keamanan pada website pemerintah Semarang.
2. Menilai keefektifan kebijakan keamanan yang ada dan seberapa baik sistem dapat bertahan terhadap serangan siber.
3. Memberikan rekomendasi perbaikan untuk meningkatkan keamanan website.

1.4 Manfaat

Penelitian ini memberikan berbagai manfaat bagi berbagai pihak, di antaranya:

1. Meningkatkan kesadaran akan pentingnya keamanan digital di antara staf dan pemangku kepentingan.
2. Memberikan panduan untuk memperkuat kebijakan dan prosedur keamanan.
3. Membantu pemerintah Semarang dalam melindungi aset digital yang berharga dan memastikan kepatuhan terhadap standar keamanan yang berlaku.