BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang terus berkembang, penggunaan *website* telah menjadi elemen penting bagi pemerintah, perusahaan, dan masyarakat global sebagai pusat pengelolaan data dan transaksi digital. Namun, keamanan *website* sering kali menjadi tantangan utama karena ancaman yang datang dari pihak yang tidak bertanggung jawab. Salah satu pendekatan penting untuk menjaga keamanan adalah melalui *penetration testing*, sebuah metode pengujian keamanan yang dirancang untuk mengidentifikasi keamanan dalam sistem.

Penetration testing, atau biasa disebut *pentest*, bertujuan untuk mensimulasikan serangan siber secara sah agar dapat menemukan celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Dalam kasus ini, penggunaan *tools* seperti *Burp Suite* dan *SQL Map* memungkinkan pengujian keamanan secara menyeluruh, termasuk terhadap ancaman seperti *SQL Injection*, *HTML Injection*, *IDOR* (*Insecure Direct Object References*), yang menjadi salah satu metode serangan paling umum dan berbahaya.

Studi kasus ini akan memfokuskan pada pengujian keamanan *website* MyApp menggunakan berbagai *tools*, dengan tujuan mengidentifikasi kerentanan yang mungkin ada. Proses ini melibatkan

scanning *website* untuk mencari celah keamanan, melakukan eksploitasi terkontrol untuk menguji potensi ancaman, serta memberikan solusi untuk menutup celah tersebut.

Hasil dari *penetration testing* tidak hanya membantu meningkatkan keamanan *website* MyApp, tetapi juga memberikan perlindungan terhadap data penting, mencegah potensi kerugian, dan menciptakan rasa percaya bagi pengguna. Dengan analisis yang tepat dan implementasi solusi berbasis hasil pentest, keamanan MyApp dapat ditingkatkan secara signifikan untuk menghadapi tantangan di era digital.

1.2 Deskripsi Pekerjaan

Selama melaksanakan magang di PT Siber Securiti Indonesia (Nemo Security) mengembangkan sebuan *website* MyApp dengan fitur yang sudah ditentukan kemudian melakukan *penetrion testing website* tersebut untuk memeastikan bawha *website* tersebut memiliki keamanan yang sangat terjaga dan mengantisipasi dari kejahatan *cyber* yang melakukan tindakan yang tidak bertanggung jawab.

1. Mengembangkan *website* MyApp

   Mengembangkan *website* MyApp dengan fitur seperti chat antar user dan transakasi yang dapat dilakukan oleh user begitu juga membuat dashboard admin yang dapat mengelola langsung data atau aktivitas yang dilakukan oleh user.

2. *Penetration Testing Website* MyApp

   Setelah mengembangkan *website* MyApp selanjutnya melakukan *penetration testing website* MyApp dengan tujuan untuk mencari celah atau kerentanan dalam *website* tersebut agar terhindar dari kejahatan *cyber*.

3. Report dan Rekomendasi

   Dalam melakukan penetration testing terdapat beberapa kerentanan yang ditemukan ketika melakukan *penetration testing* celah yang ditemukan harus di report dalam bentuk tabel yang sudah di tentukan oleh pihak PT Sekuriti Siber Indonesia (Nemo Security), kemudian memberikan rekomendasi dalam bentuk solusi agar *website* diperbaiki untuk memperbaiki celah yang ditemukan dengan tujuan saat melakukan *penetration testing* celah yang ditemukan sebelumnya sudah diatasi.

1.3 Tujuan

Tujuan yang diharapkan selama magang di PT Sekurity Siber Indonesia (Nemo Security) memberikan pengalaman kepada mahasiswa dalam bidang keamanan *siber*, khususnya penerapan dalam penetration testing pada aplikasi ataupun website. Dengan demikian adapun tujuan yang di inginkan untuk dicapai selama kegiatam magang adalah sebagai berikut :

1. Memperdalam pengetahuan tentang *penetration testing* yaitu dari segi metode, teknik, dan *tools* yang digunakan dalam *penetration*

testing untuk menganalisa serta mengevaluasi kerentanan pada aplikasi ataupun *website.*

2. Mengembangkan kemampuan teknis, seperti *eksploitasi* kerentanan, pengujian sistem keamanan, dan analisa log untuk mengidentifikasi potensi ancaman *siber*. Dan mengasah keterampilan dalam mengidentifikasi masalah kemananan dan memberikan solusi yang efektif untuk mengatasi kerentanan yang ditemukan.
3. Mendapatkan wawasan dan pengalaman langsung mengenai proses kerja di bidang keamanan *siber*, termasuk kolaborasi dengan tim profesional serta pemahaman terhadap kebutuhan industri di sektor ini.

1.4 Manfaat

Manfaat yang dapat diambil dari pelaksanaan magang di PT Sekurity Siber Indonesia (Nemo Security) adalah memberikan pengalaman dan wawasan di bidang keamanan *siber*, Dengan demikian adapun manfaat yang diperoleh selama kegiatan magang adalah sebagai berikut :

1. Peningkatan dalam *penetration testing*, dengan memperdalam pengetahuan mengenai metode, teknik, dan *tools* yang digunakan dalam *penetration testing*, mahasiswa magang dapat memiliki kemampuan yang lebih baik dalam menganalisis serta mengevaluasi kerentanan pada aplikasi ataupun *website*.

2. Kemampuan eksploitasi kerentanan, pengujian sistem keamanan, dan analisi log akan membantu mahasiswa magang dalam menghadapi ancamanan *siber* yang kompleks. Selain itu, keterampilan dalam mengidentifikasi masalah keamanan dan memberikan solusi efektif menjadi nilai tambahan untuk mendukung di dunia kerja.
3. Melindungi data sensitif seperti informasi mengani instansi, atau dokumen internal instansi akan lebih terlindungi, sehingga mengurangi resiko pelanggaran data yang dapat merusak kepercayaan pelanggan.
4. Menemukan dan memperbaiki kerentanan yang dapat dimanfaatkan oleh penyerang, instansi dapat menghindari kerugian finansial akibat pencurian data, kehilangan pelanggan, atau biaya pemulihan setelah terjadi nya *hacking*.