BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi di era sekarang ini sangatlah pesat, salah satu dampaknya adalah meningkatnya peran teknologi informasi dan komunikasi dalam berbagai aspek kehidupan. *Website* menjadi salah satu komponen utama yang digunakan untuk mengelola dan mendistribusikan informasi secara cepat dan efisien, baik dalam dunia bisnis, pendidikan, layanan publik, maupun transaksi keuangan. Namun, di sisi lain, meningkatnya pengguna *website* juga diiringi oleh tingginya risiko ancaman terhadap keamanan informasi atau data yang disimpan di dalamnya.

Ancaman keamanan seperti serangan *hacking*, pencurian data, hingga *eksploitasi* kerentanan menjadi isu serius yang dapat menimbulkan kerugian besar bagi berbagai pihak. Serangan-serangan ini sering kali memanfaatkan celah keamanan dalam sistem yang tidak terdeteksi sebelumnya. Oleh karena itu, pengujian keamanan menjadi langkah yang sangat penting untuk memastikan bahwa suatu *website* mampu menghadapi berbagai pola ancaman yang terus berkembang.

Salah satu cara yang bisa untuk mengidentifikasi dan mengatasi kerentanan dalam sistem adalah dengan melakukan *penetration testing*. *Penetration testing* atau uji *penetrasi* merupakan simulasi serangan secara Sah yang dirancang untuk.

Mengevaluasi dan menguji ketahanan keamanan suatu sistem. Dalam konteks ini, *penetration testing* berperan penting dalam mengidentifikasi celah keamanan yang mungkin ada pada *website* HANFIR, sehingga dapat segera diatasi sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Salah satu bentuk ancaman keamanan yang sering terjadi pada *website* adalah serangan *Cross-Site Scripting (XSS)* dan *Insecure Direct Object References (IDOR).* Untuk mengidentifikasi dan mengatasi kerentanan ini, penetration testing atau uji penetrasi menjadi langkah yang sangat penting. *Penetration testing* adalah metode pengujian keamanan yang dilakukan dengan mensimulasikan serangan terhadap sistem untuk mengevaluasi ketahanan dan mengidentifikasi potensi celah keamanan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab. Dalam konteks ini, pengujian terhadap *website* HANFIR dilakukan untuk mengidentifikasi dan mengatasi celah keamanan, terutama yang berkaitan dengan serangan *XSS* dan *IDOR*.

Dengan demikian, penerapan *penetration testing* menggunakan *Burp Suite* sangat penting dalam memastikan keamanan *website* HANFIR. Pengujian ini tidak hanya membantu dalam mengidentifikasi dan menutup celah keamanan yang ada, tetapi juga meningkatkan.

1.2 Deskripsi Pekerjaan

Selama melakukan magang di PT Sekuriti Siber Indonesia, kegiatan yang dilakukan berfokus pada pengembangan *website* HANFIR Multi dan pelaksanaan *penetration testing* untuk mengidentifikasi serta mengatasi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Berikut adalah rincian lengkap mengenai kegiatan tersebut:

a. Pengembangan *website* HANFIR Multi dilakukan untuk memenuhi kebutuhan sistem berbasis *website* yang aman, cepat, dan efisien. *Website* ini dirancang untuk mendukung berbagai fungsi, seperti komunikasi dan transaksi. Fokus utama dalam pengembangan ini adalah mengintegrasikan fitur keamanan ke dalam setiap lapisan arsitektur sistem.

b. *Penetration testing* bertujuan untuk mengevaluasi tingkat keamanan sistem *website* HANFIR Multi. Kegiatan ini mencakup simulasi serangan untuk mengidentifikasi potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. *Tools* utama yang digunakan adalah *Burp Suite* sebagai alat analisis dan eksploitasi keamanan.

c. Implementasi Solusi dan Perbaikan Kerentanan, Setelah kerentanan berhasil diidentifikasi, langkah berikutnya adalah menerapkan solusi untuk mengatasi masalah tersebut. Solusi yang diterapkan dirancang untuk meningkatkan keamanan sistem secara signifikan tanpa mengganggu fungsi utamanya.

d. Dokumentasi dan Pelaporan Akhir, Seluruh aktivitas selama magang, termasuk pengembangan dan pengujian keamanan, didokumentasikan dengan detail untuk memberikan gambaran lengkap mengenai proses, hasil, dan rekomendasi perbaikan.

1.3 Tujuan

Magang di PT Sekuriti Siber Indonesia memiliki tujuan utama untuk memberikan kontribusi nyata dalam pengembangan dan pengamanan sistem berbasis *website*, sekaligus memberikan pengalaman praktis kepada peserta magang. Berikut adalah tujuan yang lebih terperinci:

a. Mengidentifikasi celah keamanan dengan melakukan simulasi serangan yang sah dan terkontrol dan mengevaluasi tingkat risiko dari setiap kerentanan yang ditemukan, serta memberikan gambaran dampaknya terhadap sistem.

b. Merancang langkah-langkah untuk menutup celah keamanan yang ditemukan selama pengujian. Mengoptimalkan keamanan sistem tanpa mengganggu fungsionalitas utama *website*.

1.4 Manfaat

Program magang ini memberikan berbagai manfaat baik bagi mahasiswa magang, perusahaan, industri secara keseluruhan. Berikut adalah manfaat yang dideskripsukan secara rinci :

a. Mendapatkan pengalaman langsung dalam pengembangan website dan pelaksanaan penetration testing, termasuk penggunaan alat seperti *Burp Suite.*

b. Meningkatkan kemampuan di bidang keamanan siber, khususnya dalam menganalisis risiko dan mengimplementasikan solusi.

c. Memahami proses pengamanan sistem secara *end-to-end*, mulai dari identifikasi kerentanan hingga penerapan langkah.

d. Melatih kemampuan analisis dan penyusunan laporan teknis yang mendalam dan terstruktur.