

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

PT Sekuriti Siber Indonesia adalah perusahaan konsultan keamanan siber yang menawarkan beberapa layanan, yaitu solusi keamanan seperti *penetration testing*, *security assessment*, *security operation center*, *system hardening*, dan *digital forensic*. Selain itu, PT Sekuriti Siber Indonesia juga menyediakan layanan kepatuhan terhadap standar seperti PCI DSS dan ISO 27001, serta layanan pelatihan seperti *security awareness*, *penetration testing*, dan *secure code*.

Salah satu layanan yang ditawarkan oleh PT Sekuriti Siber Indonesia adalah *penetration testing*, yaitu layanan yang membantu klien untuk mengidentifikasi kerentanan sebelum dieksploitasi oleh pihak tidak bertanggung jawab. Selama menjalani program magang di PT Sekuriti Siber Indonesia, penulis diberi tugas salah satunya untuk melakukan *penetration testing*, khususnya pada aplikasi web.

Aplikasi web yang menjadi objek pengujian dan pembahasan dalam tugas akhir ini adalah AbseninHR, yaitu sebuah aplikasi berbasis web yang menyediakan fitur kehadiran karyawan dan manajemen cuti karyawan. Web ini memiliki dua jenis pengguna, yaitu *Admin* (HR) dan *User* (Karyawan). Tugas akhir ini berfokus pada pengujian terhadap aplikasi web yang telah dijelaskan sebelumnya. Pengujian dilakukan menggunakan metode *manual penetration testing*, dengan fokus pada dua jenis kerentanan yang termasuk dalam daftar OWASP Top Ten, yaitu *Cross-Site Scripting* (XSS) dan *SQL Injection*.

### 1.2 Deskripsi Pekerjaan

Selama menjalani program magang di PT Sekuriti Siber Indonesia, penulis mendapatkan berbagai tugas yang berfokus pada pengujian keamanan

aplikasi web. Rangkaian kegiatan magang yang menjadi fokus utama dalam penyusunan tugas akhir ini adalah sebagai berikut:

1. Menentukan Fokus Pengujian

Penulis menentukan fokus pengujian terhadap dua jenis kerentanan utama yang termasuk dalam daftar OWASP Top Ten, yaitu *Cross-Site Scripting (XSS)* dan *SQL Injection*, karena keduanya dinilai relevan dengan fitur-fitur input pengguna pada aplikasi AbseninHR.

2. Melakukan *Penetration Testing* terhadap AbseninHR

Penulis diberi tugas untuk melakukan *penetration testing* terhadap aplikasi AbseninHR. Pengujian dilakukan secara manual, mencakup tahap perencanaan, pemetaan ruang lingkup (*scope*), dan eksekusi. Fokus utama pengujian adalah pada identifikasi terhadap celah keamanan *Cross-Site Scripting (XSS)* dan *SQL Injection*.

3. Menyusun Laporan Hasil Pengujian

Setelah proses pengujian selesai dilakukan, penulis mendokumentasikan seluruh temuan dalam bentuk laporan teknis. Laporan ini mencakup deskripsi celah yang ditemukan dan *proof of concept (PoC)*.

### 1.3 Tujuan

Tujuan dari tugas akhir ini adalah menguji keamanan aplikasi web melalui metode manual *penetration testing*, dengan fokus pada dua jenis kerentanan yang termasuk dalam daftar OWASP Top Ten, yaitu *Cross-Site Scripting (XSS)* dan *SQL Injection*, serta membuat laporan *penetration testing* mengenai hasil pengujiannya.

### 1.4 Manfaat

Manfaat yang diperoleh dari kegiatan magang di PT Sekuriti Siber Indonesia antara lain adalah meningkatnya keterampilan teknis, khususnya dalam melakukan *penetration testing*, serta komunikasi dan kerja sama tim. Selain itu, magang ini juga memberikan pengalaman langsung dalam

mengidentifikasi celah keamanan pada aplikasi web, serta cara mendokumentasikan hasil temuannya.