BAB V
PENUTUP

5.1 Simpulan

Berdasarkan kegiatan magang yang telah dilaksanakan di PT Sekuriti Siber Indonesia, khususnya pada kegiatan pengujian keamanan web *Human Resource* sebagai media pembelajaran terhadap celah XSS dan *SQL Injection*, maka dapat disimpulkan beberapa hal sebagai berikut:

1. Ditemukannya Kerentanan Keamanan

   Pengujian aplikasi web AbseninHR difokuskan pada dua jenis kerentanan keamanan, yaitu *Cross-Site Scripting* (XSS) dan *SQL Injection*. Kedua celah tersebut ditemukan melalui pendekatan *manual penetration testing*. *Payload* yang disisipkan berhasil dijalankan di sisi *target*, yang mengindikasikan bahwa kerentanan tersebut benar-benar dapat dieksploitasi.

2. Potensi Dampak yang Ditimbulkan

   Celah XSS memungkinkan pelaku menyisipkan *payload* berbahaya yang akan dieksekusi di sisi *Admin* (HR), sementara *SQL Injection* memungkinkan penyerang mengabaikan validasi kata sandi sehingga mengakses akun *admin* secara tidak sah. Kedua kerentanan ini menimbulkan risiko serius terhadap kerahasiaan, integritas, dan akses sistem.

5.2 Saran

Berdasarkan hasil pengujian keamanan aplikasi web, penulis memberikan beberapa saran yang dapat dipertimbangkan untuk meningkatkan keamanan aplikasi, khususnya dalam konteks keamanan web:

1. Menggunakan *Automated Penetration Testing*

   Selain pengujian manual, penggunaan tools seperti Nessus, Nikto, dan sejenisnya dapat membantu mengidentifikasi potensi celah keamanan

secara efisien dan melengkapi hasil pengujian dengan pendekatan otomatis.

2. Meningkatkan Cakupan Pengujian Keamanan

   Pengujian keamanan sebaiknya mencakup seluruh komponen aplikasi, termasuk area yang belum diuji seperti manajemen sesi, komponen pihak ketiga, dan lainnya. Cakupan yang lebih luas memungkinkan identifikasi kerentanan yang lebih beragam.

3. Menambahkan Pengujian Kerentanan Selain XSS dan *SQL Injection*

   Karena tugas akhir ini berfokus pada pengujian XSS dan *SQL Injection*, maka untuk pengujian selanjutnya disarankan menambahkan jenis kerentanan lain seperti *Broken Authentication*, *Insecure Deserialization*, *Directory Traversal*, atau *Server-Side Request Forgery* (SSRF) agar pengujian lebih komprehensif.

Dengan menerapkan saran-saran di atas, proses penetration testing terhadap aplikasi web diharapkan menjadi lebih efektif, sistematis, dan menyeluruh, sehingga mampu mengidentifikasi berbagai potensi kerentanan secara lebih maksimal.