BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan temuan yang diperoleh selama proses penelitian, berikut adalah poin-poin kesimpulan yang dihasilkan:

1. Penelitian ini berhasil menerapkan metode *penetration testing* dengan pendekatan *black box testing* berdasarkan kerangka kerja NIST SP 800-115**,** yang meliputi fase *planning*, *discovery*, *attack*, dan *reporting*, sehingga proses pengujian keamanan aplikasi web dapat dilakukan secara sistematis dan terstruktur.
2. Fase *discovery* yang dilakukan menggunakan *tools* nslookup**,** nmap**,** dan OWASP ZAP terbukti efektif dalam mengidentifikasi konfigurasi sistem, permukaan serangan, serta indikasi awal kerentanan pada lapisan aplikasi web yang diuji, yang selanjutkan digunakan sebagai dasar penentuan focus dan validasi kerentanan pada fase *attack*.
3. Hasil pengujian menunjukkan bahwa aplikasi web diakses melalui layanan Cloudflare sebagai *reverse proxy*, yang berfungsi menyembunyikan alamat IP server origin dan membatasi pengujian langsung pada lapisan jaringan, sesuai dengan karakteristik pendekatan *black box testing.*
4. Validasi pada fase *attack* mengonfirmasi keberadaan kerentanan *SQL Injection* pada fitur autentikasi, kondisi ini menyebabkan pengujian keamanan difokuskan pada lapisan aplikasi web, di mana manipulasi input pengguna terbukti mampu mengintervensi eksekusi kueri basis data. Kerentanan iniberpotensi mengancam kerahasiaan dan integritas informasi, serta menunjukkan lemahnya mekanismevalidasi input pada sisi server
5. Berdasarkan evaluasi menggunakan standar CVSS v3.1, kerentanan *SQL Injection* diklasifikasikan memiliki risiko tinggi (*High*), yang mengindikasikan adanya potensi dampak serius terhadap keamanan sistem dan menuntut penerapan tindakan mitigasi sebagai prioritas utama.

6. Pengujian *Cross-Site Scripting* (XSS) menunjukkan bahwa kerentanan berhasil dieksploitasi. Namun hanya setelah penyerang berhasil melakukan autentikasi ke dalam system, sehingga ruang lingkup serangan dan dampak menjadi terbatas. Oleh karena itu, meskipun pemindaian menggunakan OWASP ZAP mengindikasikan tingkat risiko *high*, hasil analisis manual dan penilaian menggunakan CVSS v3.1 menetapkan tingkat risiko kerentanan XSS erada pada kategori *low.*
7. Hasil penelitian menunjukkan bahwa tidak seluruh indikasi kerentanan yang terdeteksi pada fase *discovery* terbukti dapat dieksploitasi, sehingga proses validasi pada fase *attack* merupakan tahapan krusial untuk memastikan ingkat risiko actual alam pengujian keamanan aplikasi web.
8. Penyusunan rekomendasi mitigasi berdasarkan hasil pengujian dan klasifikasi Tingkat risiko memberikan acuan teknisyang aplikatif bagi pengelola system dalam meningkatkan keamanan aplikasi web, khususnya pada lapisan aplikasi dan mekanisme komunikasi data sebagai bagian dari sistem informasi berbasis jaringan.

5.2 Saran

Berdasarkan evaluasi terhadap seluruh rangkaian penelitian, terdapat beberapa rekomendasi yang disarankan bagi pengembangan sistem maupun penelitian di masa mendatang, yaitu:

1. Pengujian keamanan paada penelitian selanjutnya dapat diperluas dengan mengevaluasi konfigurasi mekanisme proteksi tambahan, seperti *Web Application Firewall* (WAF) pada layanan Cloudflare, guna menilai efektivitasnya dalam mendeteksi, mencegah, dan memitigasi serangan pada lapisan aplikasi web.
2. Penelitian mendatang disarankan untuk memperluas cakupan pengujian dengan menerapkan variasi *payload* dan parameter input yang lebih kompleks dan beragam konsistensi serta ketahanan mekanisme keamanan aplikasi dapat divalidasi secara lebih komprehensif terhadap

berbagai scenario erangan, khususnya pada fitur yang memproses data dinamis

3. Pengujian ulang (*retesting*) disarankan untuk dilakukan setelah seluruh rekomendasi mitigasi diimplementasikan, guna memverifikasi efektivitas perbaikan keamanan yang diterapkan serta memastikan bahwa perubahan tersebut tidak menimbulkan kerentanan baru pada fitur atau komponen sistem lainnya
4. Penelitian selanjutnya disarankan membandingkan antara metode *black box*, *gray box*, dan *white box penetration testing*, sehingga analisis keamanan yang dihasilkan menjadi lebih komprehensif, mengingat setiap pendekatan memiliki sudut pandang dan tingkat visibilitas yang berbeda dalam mengidentifikasi kerentanan pada suatu sistem.