BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis dan pengujian keamanan yang telah dilakukan terhadap *website* BagiBagi.co, ditemukan beberapa kerentanan yang dapat berpotensi dieksploitasi oleh penyerang. Kerentanan utama yang ditemukan diantaranya: *SQL Injection*: Meskipun percobaan pertama gagal karena adanya proteksi *Web Application Firewall* (*WAF*) dari *Cloudflare*, teknik *bypass firewall* berhasil mengonfirmasi *bahwa SQL Injection* memang menjadi ancaman bagi sistem. *Security Misconfiguration*: Ditemukan direktori tersembunyi (*https*://*bagibagi.co*/*api*/) yang berpotensi menyimpan informasi sensitif. Walaupun beberapa direktori terlindungi dengan respon "*403 Forbidden*", fakta bahwa direktori ini dapat diidentifikasi menunjukkan adanya kelemahan dalam konfigurasi keamanan server. *Broken Access Control*: Pengujian menggunakan teknik *Insecure Direct Object References* (*IDOR*) menemukan bahwa profil pengguna dengan *ID* tertentu dapat diakses melalui *tools Python*, meskipun eksploitasi lebih lanjut terhalang oleh mekanisme otorisasi dan autentikasi yang membatasi akses berdasarkan peran pengguna.

5.2 Saran

Pada penelitian ini penulis ingin memberikan saran kepada peneliti selanjutnya berdasarkan dari penelitian yang telah dilakukan, diantaranya. :

1. Penggunaan Metode Pengujian yang Lebih Luas.
   Penelitian ini telah mengidentifikasi beberapa kerentanan, namun masih terdapat potensi celah keamanan lain yang belum diuji secara mendalam. Oleh karena itu, peneliti selanjutnya disarankan untuk menggunakan metode pengujian tambahan, seperti *Dynamic Application Security*

Testing (*DAST*) dan *Static Application Security Testing* (*SAST*), guna mendapatkan hasil yang lebih menyeluruh.

2. Analisis Keamanan dari Perspektif Pengembang

   Selain melakukan pengujian sebagai penyerang (*vulnerability assessment*), penelitian ke depan dapat mengeksplorasi pendekatan dari sisi pengembang, seperti menerapkan *Secure Software Development Lifecycle* (*SDLC*). Hal ini bertujuan untuk memastikan keamanan sudah diterapkan sejak tahap awal pengembangan aplikasi.

3. Pengujian terhadap Sistem Autentikasi dan Manajemen Sesi

   Mengingat pentingnya sistem autentikasi dalam melindungi data pengguna, peneliti selanjutnya dapat lebih fokus pada analisis keamanan autentikasi, termasuk pengelolaan token sesi, perlindungan terhadap *brute force attack*, serta penerapan autentikasi *multi-faktor* (*MFA*) untuk meningkatkan keamanan akses.

Dengan adanya saran ini, diharapkan penelitian selanjutnya dapat memberikan kontribusi yang lebih signifikan dalam meningkatkan keamanan sistem web serta membantu pengembang dalam menerapkan praktik keamanan yang lebih baik.