BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian kerentanan keamanan pada aplikasi *website* Apotek XYZ dengan menggunakan metode OWASP Top 10, didapatkan kesimpulan sebagai berikut:

1. Ditemukan adanya 13 celah keamanan yang ditemukan oleh OWASP ZAP dengan 5 celah keamanan berada pada tingkat resiko *Medium*, 3 celah keamanan pada tingkat resiko *Low*, dan 5 celah keamanan pada tingkat *Informational*.
2. Hasil pengujian menunjukkan terdapat 8 kategori kerentanan keamanan OWASP Top 10 2021 yang rentan yaitu *Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures* dan *Software and Data Integrity Failures*. Terdapat 1 kerentanan dengan tingkat resiko *High* yaitu *Parameter Tampering*, Kemudian 7 kerentanan dengan tingkat resiko *Medium* yaitu *Access Control Issue - Improper Authorization, SQL Injection, Absence of Anti-CSRF Tokens, Application Error Disclosure, Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header, Vulnerable jS Library, Cookie No HttpOnly Flag, Cookie without SameSite Attribute* dan *Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*.
3. Untuk memperbaiki celah keamanan website Apotek XYZ, direkomendasikan untuk mengaudit dan meningkatkan kontrol akses dengan validasi server-side dan prinsip least privilege, mengimplementasikan prepared statements dan sanitasi input untuk mencegah SQL Injection, menambahkan flag HttpOnly, Secure, dan atribut SameSite pada cookie, menyertakan anti-CSRF tokens dan validasi Referrer dan Origin, mengonfigurasi error handling yang tepat dan mengimplementasikan monitoring serta alerting, memperbarui libraries JavaScript dan menerapkan Content Security Policy (CSP), menambahkan header keamanan seperti X-Frame-Options dan menghapus header X-Powered-By, melakukan pelatihan keamanan bagi pengembang dan pengguna, melakukan pengetesan keamanan berkala dengan alat seperti OWASP ZAP, menggunakan Web Application Firewall (WAF), dan memastikan enkripsi data sensitif dengan SSL/TLS untuk meningkatkan keamanan secara menyeluruh.

5.2 Saran

Berdasarkan hasil pengujian kerentanan keamanan yang telah dilakukan terdapat beberapa saran yang dapat digunakan untuk penelitian selanjutnya ataupun sistem pada *website*:

1. Peneliti selanjutnya disarankan untuk menggunakan teknik pengujian keamanan yang lebih canggih seperti *fuzzing* dan *dynamic analysis* untuk menemukan kerentanan yang mungkin tidak terdeteksi oleh metode OWASP Top 10.
2. Pastikan setiap halaman dan fitur yang terbatas hanya dapat diakses oleh pengguna yang memiliki hak akses yang sesuai dan uji secara menyeluruh untuk memastikan tidak ada celah yang dapat dieksploitasi.
3. Menambahkan algoritma kriptografi yang kuat pada *form password* dan sistem *captcha* pada *field login* untuk mencegah spam selama sesi *login*.