BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian terhadap website Woodenloka.store menggunakan pendekatan penetration testing sesuai dari referensi keamanan OWASP Top 10 tahun 2021, diperoleh beberapa kesimpulan sebagai berikut:

1. Website Woodenloka.store teridentifikasi memiliki sejumlah kerentanan keamanan, khususnya pada konfigurasi header HTTP (seperti tidak adanya X-Frame-Options dan X-Content-Type-Options). Hal ini dikategorikan sebagai Security Misconfiguration sesuai OWASP A05:2021.
2. Melalui alat pemindai WPScan, ditemukan plugin WordPress bernama instagram-feed dengan versi 6.6.1 yang rentan terhadap Stored Cross Site Scripting (XSS) melalui atribut data-plugin (CVE-2025-4583).disarankan untuk melakukan pembaruan ke versi terbaru untuk mengatasi kerentanan tersebut
3. Melalui alat pemindai Nikto, ditemukan bahwa Drupal versi 4.2.0 rentan terhadap serangan Cross Site Scripting (XSS). Oleh karena itu, disarankan untuk melakukan pembaruan ke versi terbaru untuk mengatasi kerentanan tersebut.
4. Hasil port scanning menunjukkan bahwa port FTP (21) masih terbuka, yang berpotensi disalahgunakan untuk serangan seperti credential sniffing atau Man-in-the-Middle (MitM). Hal ini menunjukkan pentingnya penggantian layanan FTP dengan protokol yang lebih aman seperti SFTP atau FTPS.
5. Tools WhatWaf menunjukkan bahwa website belum memiliki Web Application Firewall (WAF) yang aktif, sehingga lapisan proteksi terhadap serangan otomatis seperti SQL Injection, Brute Force, atau Botnet menjadi sangat terbatas.

5.2 Saran

Berdasarkan penelitian yang sudah dilakukan terdapat beberapa saran yang dapat diterapkan pada penelitian selanjutnya dan juga khususnya terhadap sistem keamanan website woodenloka sebagai objek penelitian. Dan terdapat beberapa

keterbatasan pada penelitian ini dengan harapan dapat dikembangkan lebih lanjut pada penelitian selanjutnya antara lain

1. Perlunya dilakukan pengecekan dan pemeliharaan secara berkala pada seluruh sistem keamanan website woodenloka.store agar segala dari celah keamanan dapat diketahui lebih dini dan segera dapat ditanggulangi jika terdapat kebocoran pada celah keamanan.
2. Perlu dilakukan update secara berkala terhadap plugin yang terdapat pada web yang dikelola