BAB V

PENUTUP

A. Kesimpulan

Berdasarkan hasil pengujian kerentanan keamanan pada website Disparbudpora Kabupaten Pacitan menggunakan metode NIST SP 800-115, dapat disimpulkan bahwa sistem masih memiliki tingkat kerentanan yang cukup signifikan. Pengujian dilakukan dengan pendekatan *white-box testing* pada *website* resmi yang dikelola Disparbudpora, dengan akses hingga ke *dashboard admin WordPress*. Dari total 38 temuan yang diidentifikasi selama tahap *discovery*, sebanyak 10 di antaranya (26,32%) dikategorikan sebagai kerentanan dengan risiko tinggi, termasuk aktivasi *xmlrpc.php*, potensi *Blind SQL Injection*, keterbukaan informasi akun administrator melalui REST API, dan konfigurasi DNS yang memungkinkan terjadinya *Subdomain Takeover*. Sementara itu, 28 temuan lainnya bersifat informasional, yang meskipun tidak langsung membahayakan sistem, tetap penting untuk diperhatikan sebagai bagian dari penguatan konfigurasi keamanan secara menyeluruh. Skor CVSS rata-rata sebesar 6,4 mengindikasikan tingkat kerentanan berada pada kategori sedang (*medium*), namun tetap menunjukkan potensi ancaman yang serius apabila tidak segera ditangani.

Sebagai respons terhadap temuan tersebut, penelitian ini berhasil merumuskan rekomendasi keamanan yang sesuai untuk meningkatkan

proteksi pada sistem. Rekomendasi mencakup penonaktifan fungsi *xmlrpc.php* dan *wp-cron.php*, pembatasan akses REST API, penyembunyian *URL login* standar, penghapusan file dan *plugin default WordPress* yang tidak diperlukan, serta penerapan *HTTP security headers*. Selain itu, penggunaan plugin keamanan seperti *Wordfence* dan *Limit Login Attempts Reloaded* juga direkomendasikan guna meminimalkan risiko eksploitasi lanjutan. Rekomendasi ini disusun berdasarkan hasil analisis dari kerentanan yang ditemukan selama proses pengujian.

Sebagian besar rekomendasi keamanan tersebut berhasil diimplementasikan langsung melalui *dashboard admin WordPress* selama tahap mitigasi. Tindakan-tindakan seperti konfigurasi plugin keamanan, pembatasan akses REST API, dan penghapusan komponen tidak penting telah dilaksanakan untuk mengurangi permukaan serangan. Namun, beberapa mitigasi yang menyangkut infrastruktur, seperti pengamanan konfigurasi DNS dan pembatasan akses ke direktori sensitif, masih membutuhkan kerja sama lebih lanjut dengan administrator sistem. Dengan demikian, penelitian ini tidak hanya mengidentifikasi permasalahan dan memberikan solusi, tetapi juga menunjukkan sejauh mana rekomendasi tersebut dapat diimplementasikan secara nyata untuk meningkatkan keamanan website Disparbudpora Kabupaten Pacitan.

B. Saran

Saran diberikan berdasarkan keterbatasan penelitian ini dan untuk keberlanjutan serta pengembangan penelitian selanjutnya:

1. Audit Keamanan Berkala

   Instansi Disparbudpora Kabupaten Pacitan disarankan untuk melakukan audit keamanan secara berkala dengan menggunakan metode penetration testing yang komprehensif, tidak hanya terbatas pada website, tetapi juga mencakup infrastruktur server dan aplikasi pendukung. Langkah ini penting dilakukan untuk mengantisipasi munculnya celah keamanan baru seiring dengan perkembangan teknologi dan meningkatnya ancaman siber, sebagaimana disarankan oleh (Annaufal et al., 2025).

2. Pembaruan Sistem Rutin

   Saran serupa juga disampaikan oleh (Prasetya, I. A., & Safriadi, 2024), yang menekankan pentingnya pembaruan rutin terhadap komponen website, termasuk inti WordPress, plugin, dan tema, guna menutup celah keamanan yang berpotensi dieksploitasi.

3. Pelatihan Keamanan Siber

   Peningkatan kesadaran dan pemahaman staf terhadap keamanan siber perlu dilakukan secara berkala melalui pelatihan. Penerapan praktik keamanan dasar yang baik, baik oleh pengguna maupun administrator, sangat penting untuk mencegah insiden yang bersumber dari kelalaian manusia, sebagaimana disampaikan oleh (Farmadika et al., 2024).

4. Fokus Penelitian Selanjutnya

Penelitian di masa mendatang dapat mengeksplorasi metode *penetration testing* lainnya, seperti *Black Box Testing* atau *Gray Box Testing*, untuk memperoleh perspektif yang lebih komprehensif. Selain itu, analisis kerentanan yang lebih mendalam terhadap plugin dan tema WordPress dapat dilakukan dengan memanfaatkan *WPScan API* menggunakan token yang valid. Peneliti juga disarankan untuk mempertimbangkan metodologi lain, seperti *OWASP Testing Guide* atau *PTES*, sebagai pembanding terhadap NIST SP 800-115, sebagaimana disampaikan oleh (Astriani, 2021). Apabila memungkinkan dan sesuai dengan prosedur etis, pengujian eksploitasi lanjutan juga dapat dilakukan guna mengukur dampak aktual dari kerentanan yang ditemukan.