BAB VI
PENUTUP

5.1 KESIMPULAN

Berdasarkan hasil penelitian dan analisis keamanan yang telah dilakukan pada *website* smpn6muarojambi.sch.id menggunakan metode *vulnerability assessment*, dapat ditarik beberapa kesimpulan utama. Secara keseluruhan, pemindaian menggunakan *OWASP Zed Attack Proxy* (ZAP) berhasil mengidentifikasi berbagai celah keamanan yang diklasifikasikan ke dalam tingkat risiko *Medium*, *Low*, dan *Informational*. Tidak ditemukannya kerentanan dengan tingkat risiko *High* menunjukkan bahwa *website* tersebut telah memiliki dasar keamanan yang cukup baik, namun tetap memerlukan penguatan pada beberapa aspek teknis untuk mencegah potensi eksploitasi di masa mendatang.

Hasil pemetaan kerentanan terhadap standar *OWASP Top 10* menunjukkan bahwa mayoritas celah keamanan yang ditemukan masuk ke dalam kategori *A05:2021 – Security Misconfiguration*. Hal ini mencakup ketiadaan *header* keamanan penting seperti *Content Security Policy* (CSP), *X-Frame-Options*, dan *X-Content-Type-Options*, serta terbukanya akses pada file sensitif seperti *italic*composer.lock*italic*. Selain itu, penggunaan pustaka *Javascript* versi lama (*jQuery* 3.4.1) yang tergolong dalam kategori *A06:2021 – Vulnerable and Outdated Components* dan ketiadaan *token* anti-CSRF dalam kategori *A01:2021 – Broken Access Control* menjadi poin kritis yang harus segera diperbaiki. Validasi melalui *Proof of concept* (POC) telah membuktikan bahwa celah-celah tersebut benar-benar

ada dan dapat diakses, sehingga mitigasi yang tepat sangat diperlukan untuk menjaga integritas dan kerahasiaan data pada sistem informasi sekolah.

5.2 SARAN

Berdasarkan kesimpulan di atas, terdapat beberapa saran yang dapat diberikan bagi pihak pengelola *website* SMPN 6 Muaro Jambi maupun bagi peneliti selanjutnya untuk meningkatkan kualitas keamanan sistem informasi:

1. Bagi Pengelola *Website*

   Sekolah Disarankan bagi administrator sistem untuk segera menerapkan rekomendasi perbaikan yang telah disusun, terutama melakukan pembaruan pada seluruh komponen pustaka pihak ketiga ke versi yang paling stabil dan aman. Penguatan konfigurasi peladen melalui penerapan *header* keamanan HTTP dan manajemen *cookie* yang lebih ketat menggunakan atribut *italic*Secure*italic* serta *italic*HttpOnly*italic* harus menjadi prioritas utama. Selain itu, perlu dilakukan audit keamanan secara berkala minimal setiap enam bulan sekali atau setiap kali terdapat pembaruan besar pada sistem guna mendeteksi adanya celah keamanan baru secara dini.

2. Bagi Peneliti Selanjutnya

   Peneliti selanjutnya disarankan untuk memperluas cakupan pengujian dengan menggunakan metode *penetration testing* yang lebih mendalam, termasuk pengujian pada lapisan basis data dan pengujian autentikasi pengguna secara manual. Penggunaan variasi perangkat lunak pemindaian lain selain *OWASP ZAP* juga dapat dipertimbangkan untuk mendapatkan hasil perbandingan yang lebih komprehensif. Selain itu, penelitian masa depan dapat

memfokuskan pada pengembangan mekanisme pertahanan otomatis atau sistem deteksi intrusi yang disesuaikan dengan arsitektur *website* institusi pendidikan.