BAB 5
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan dengan metode OWASP *Web Security Testing Guide* (WSTG) pada website SMAN 77 Jakarta, dapat disimpulkan bahwa tingkat keamanan website dalam menghadapi ancaman serangan masih memerlukan peningkatan. Dari pengujian yang difokuskan pada form login dan halaman admin menggunakan pendekatan penetration testing, ditemukan adanya sejumlah potensi kerentanan dengan tingkat keparahan yang bervariasi. Penilaian menggunakan metode CVSS pada *base score metrics* memperlihatkan nilai risiko mulai dari kategori rendah hingga tinggi, yang menunjukkan bahwa *website* belum sepenuhnya aman dari ancaman serangan siber sehingga memerlukan prioritas mitigasi lebih lanjut. Berikut, merupakan daftar potensi kerentanan yang ditemukan dengan tingkat keparahan yang bervariasi:

1. *Fingerprint Web Server* dengan tingkat keparahan *medium* dan skor 5.3 dari 10.
2. *Test Application Platform Configuration* dengan tingkat keparahan *medium* dan skor 5.3 dari 10.
3. *Testing for Account Enumeration and Guessable User Account* dengan tingkat keparahan *medium* dan skor 5.3 dari 10.
4. *Testing for Default Credentials* dengan tingkat keparahan *high* dan skor 7.0 dari 10.
5. *Testing for Weak Password Policy* dengan tingkat keparahan *medium* dan skor 6.5 dari 10.
6. *Testing for Bypassing Authorization Schema* dengan tingkat keparahan *low* dan skor 3.3 dari 10.
7. *Testing for Privilege Escalation* dengan tingkat keparahan *low* dan skor 3.3 dari 10.
8. *Testing for Cookies Attributes* dengan tingkat keparahan *medium* dan skor 4.3 dari 10.

9. *Testing Session Timeout* dengan tingkat keparahan *medium* dan skor 5.4 dari 10.

Sementara itu, penelitian ini juga berhasil mengidentifikasi jenis-jenis serangan yang berpotensi mengancam website SMAN 77 Jakarta, antara lain terkait kerentanan pada kontrol akses file atau direktori, *SQL Injection*, kegagalan dalam identifikasi dan otentikasi pengguna, serta kesalahan dalam konfigurasi keamanan server. Beberapa di antaranya meliputi fingerprint web server, metode HTTP yang tidak perlu aktif, penggunaan kredensial default, kebijakan kata sandi yang lemah, hingga manajemen sesi yang belum optimal. Rekomendasi mitigasi yang telah disusun diharapkan dapat menjadi acuan dalam meningkatkan perlindungan website dari upaya eksploitasi yang dapat dimanfaatkan pihak tidak bertanggung jawab.

5.2 Saran

Sebagai tindak lanjut dari temuan penelitian ini, penulis memberikan beberapa saran, diantaranya:

1. Segera memperkuat kebijakan kata sandi dengan menerapkan aturan kompleksitas minimum dan perlindungan *brute force*.
2. Melakukan *penetration testing* secara rutin dan memanfaatkan *tools* pemantauan untuk mendeteksi aktivitas mencurigakan sedini mungkin.
3. Melakukan pengujian keamanan yang lebih luas, tidak hanya terbatas pada form login dan halaman admin, tetapi juga mencakup area publik website.
4. Menggunakan *framework* atau *tools* tambahan seperti OWASP ZAP untuk memperoleh pendekatan pengujian yang lebih variatif dan memperluas cakupan identifikasi kerentanan.