

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan terhadap pengujian kerentanan *website* dengan pendekatan *Penetration Testing* menggunakan metode *OWASP* pada SMK Taruna Bangsa dapat disimpulkan beberapa hal sebagai berikut.

1. Tingkat kerentanan *website* SMK Taruna Bangsa terhadap serangan siber tergolong pada kategori medium, berdasarkan hasil pengujian yang mencakup tahapan *Planning*, *Discovery*, *Attacking*, dan *Reporting*. *Website* belum sepenuhnya memenuhi standar keamanan *web* dan masih memiliki celah yang dapat dieksploitasi oleh pihak tidak bertanggung jawab.
2. Beberapa kategori kerentanan yang ditemukan dalam pengujian mencakup beberapa kategori dari *OWASP Top 10*, seperti *Cross-Site Scripting (XSS)*, *Clickjacking*, konfigurasi direktori yang tidak aman (*directory listing*), dan tidak menerapkan *header* keamanan penting seperti *HSTS* dan *CSP*. Selain itu, ditemukan *internal path disclosure* dan file konfigurasi pengembangan seperti *.gitignore* yang dapat diakses publik.
3. Kerentanan yang teridentifikasi berpotensi mengganggu aspek *Confidentiality*, *Integrity*, dan *Availability (CIA)* sistem. Sebagai contoh, *XSS* dapat dimanfaatkan untuk pencurian data atau injeksi skrip berbahaya, sementara direktori dan file konfigurasi yang terbuka memungkinkan akses tidak sah terhadap informasi sensitif.

4. Peningkatan keamanan *website* dapat dicapai melalui implementasi *security headers* seperti *HSTS*, *CSP*, dan *X-Frame-Options*, pengaturan akses terbatas pada direktori dan file sensitif, serta validasi input yang ketat untuk mencegah *XSS*. Disarankan pula pelaksanaan audit dan pemantauan sistem secara berkala, penyusunan SOP keamanan, serta penguatan kapasitas pengelola dalam bidang literasi keamanan siber.

5.2 Saran

Penelitian ini masih banyak keterbatasan yang dapat menjadi bahan pengembang untuk penelitian selanjutnya. Berikut beberapa saran yang dapat diberikan sebagai berikut.

1. Disarankan agar pengelola *website* menambahkan *security headers* seperti *HSTS*, *CSP*, *X-Content-Type-Options*, dan *X-Frame-Options* untuk memperkuat pertahanan dari serangan umum seperti *Clickjacking* dan *XSS*.
2. Lakukan audit keamanan dan *penetration testing* secara berkala untuk memastikan tidak ada kerentanan baru yang muncul seiring dengan pembaruan sistem atau penambahan fitur.
3. Pastikan direktori sensitif tidak dapat diakses secara publik, serta file konfigurasi tidak tersedia secara terbuka. Gunakan konfigurasi yang sesuai standar keamanan saat *deploy website*.
4. Disarankan untuk membuat dan menerapkan *Standar Operasi Prosedur* (SOP) untuk menangani insiden keamanan siber, memantau log akses, dan mengelola data sensitif.