BAB 5
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan tahapan-tahapan pemindaian kerentanan pada *website repository.unjaya.ac.id* menggunakan metode *Open Source Security Testhing Methodoogy Manual* (OSSTMM) yang hasilnya bisa dijadikan acuan terhadap evaluasi terkait tingkat keamanan sistem *Repository* Unjaya. Kesimpulan dari penelitian ini adalah sebagai berikut:

1. Analisis kerentanan menggunakan metode *Open Source Security Testhing Methodology Manual* (OSSTMM) berhasil menemukan celah/kerentanan yang ada pada *domain repository.unjaya.ac.id*. Celah-celah ini ditemukan pada *Oprational Security*, *Loss Control* dan *Limitation,* jika kerentanan ini tidak segera diatasi potensi untuk terjadinya serangan dari pihak-pihak tidak bertanggung jawab bisa terjadi.
2. Analisis kerentanan menggunakan metode *Open Source Security Testhing Methodology Manual* (OSSTMM) pada *domain repository.unjaya.ac.id* melalui empat tahap pemindaian yaitu *reconnaissance/information gathering* menggunakan *tools* Netcraft, *scanning network* menggunakan *tools* Nmap, *scanning vulnerability* menggunakan Nikto *Scanner*, dan *penetration testhing* menggunakan OWASP ZAP. Hasilnya menunjukan bahwa *website Repository* Unjaya memiliki *RAV Score* sebesar 82,8676 *ravs* ditunjukan oleh Gambar 4.13 dan berdasarkan pada Tabel 3.2 *website* ini termasuk ke dalam kategori *website* dengan keamanan kurang.

5.2 SARAN

Berdasarkan tahap penelitian yang sudah dilakukan terdapat beberapa saran yang dapat penulis berikan untuk perkembangan *website Repository* unjaya kedepannya, ini juga bisa menjadi acuan yang dapat diterapkan pada penelitian selanjutnya yang akan menggunakan metode *Open Source Security Testing Methodology Manual* (OSSTMM). Berikut saran dari penulis:

1. Saran untuk penelitian selanjutnya
    a. Penelitian selanjutnya dapat menggunakan tipe tes *Double Blind* atau tes yang dilakukan dengan keterlibatan kedua pihak yaitu peneliti dan pengelola, sehingga hasil yang didapat dapat memberikan *insight* dan evaluasi lebih mendalam terkait keamanan *website Repository* Unjaya.
    b. Penulis menyarankan pada penelitian selanjutnya bisa menerapkan penilaian penuh menggunakan *Security Testing Audit Report* (STAR) agar hasil STAR dapat lebih terperinci.
    c. Diperlukan peningkatan pemahaman terkait pemindaian atau bahkan pengujian menggunakan metode *Open Source Security Testing Methodology Manual* (OSSTMM), dikarenakan masih belum cukup banyak studi kasus nasional yang menggunakan metode serupa, jadi sebaiknya mencari studi kasus dari publikasi internasional.
2. Saran untuk pengelola *website*
    a. Untuk mengurangi atau mengatasi kerentanan yang ditemukan peneliti menyarankan agar penelola :
        1) Meningkatkan keamanan sertifikat SSL. Dengan memastikan konfigurasi SSL sudah optimal dan menggunakan *cipher suite* yang kuat.
        2) Perbaiki kelemahan autentikasi. Implementasi mekanisme autentikasi yang lebih kuat dan lakukan pengujian penetrasi secara berkala.
        3) Audit konfigurasi server atau melakukan audit dan perbaikan terhadap konfigurasi server Apache untuk mengurangi risiko yang teridentifikasi.

4) *Monitoring* dan *alerting*. Implementasi sistem *monitoring* dan *alerting* untuk mendeteksi anomali dan potensi serangan lebih dini.

b. Penulis menyarankan pengujian dilakukan kembali *bersama Cyber Security Profesional (Penetration Tester*) yang sudah bersertifikasi dan sudah berpengalaman.