BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian yang telah dilakukan pada bab sebelumnya mengenai Audit Keamanan Sistem Informasi Akademik Menggunakan COBIT 5 pada Universitas Sultan Ageng Tirtayasa, hal ini dapat diberikan kesimpulan sebagai berikut:

1. Hasil identifikasi kerentanan menggunakan *tools* Vega dan Owasp Zap menunjukkan kerentanan yang berbeda. Vega memiliki 11 kerentanan sedangkan pada Owasp ZAP memiliki 14 kerentanan.
2. Hasil dari penelitian ini menujukkan level kemampuan pada proses pengelolaan keamanan (APO13) dan pengelolaan layanan keamanan (DSS05) di UPT PusdaInfo kondisi saat ini pada level 3 dan tingkat kemampuan yang diharapkan pada level 5 dengan masing–masing nilai kesenjangan APO13 2 dan DSS05 1,57.
3. Hasil rekomendasi dari metode ISSAF adalah mengkonfigurasi DNS SEC agar tidak dapat mengakibatkan serangan DNS *spoofing*, men*disable* SSLv3 untuk mencegah terjadinya serangan POODLE dan Man-in-the-Middle.

5.2 Saran

Penelitian ini masih terdapat kekurangan yang dapat dijadikan sebagai pengembangan penelitian berikutnya:

1. Dapat menggunakan *framework* penetrasi test lain seperti *Penetration Testing Execution Standard* (PTES) dan *framework* audit lainnya seperti ISO dan ITIL untuk memperoleh hasil uji yang lebih baik.
2. Melakukan perbaikan kerentanan sistem yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab sebagai kelemahan mengenai Siakad.
3. Pusat Data dan Informasi dapat memikirkan untuk menerapkan saran dari rekomendasi yang telah diajukan.