BAB V
PENUTUP

5.1 Kesimpulan

Dalam melakukan uji *penetration testing* ini yang bertujuan untuk menguji tingkat keamanan pada sistem X maka penulis mendapatkan beberapa poin hasil dari penelitian ini sebagai berikut:

1. Identifikasi Risiko dilakukan untuk memfasilitasi analisis kerentanan dengan menguraikan informasi rinci tentang setiap kerentanan yang ditemukan. Identifikasi risiko ini menyajikan deskripsi umum, dampak, penyebab, dan metode serangan yang digunakan.
2. Analisa risiko dilakukan dengan menggunakan salah satu metodologi OWASP10 yaitu *Risk Rating* , hasilnya di temukan celah keamanan yang ditemukan secara rinci sebagai berikut:
    a. Sebanyak 1 celah keamanan yang memiliki *Severity risk rating* yang kategorikan sebagai celah keamanan yang tingkat *vulnerability* nya *Critical*.
    b. Sebanyak 2 celah keamanan yang memiliki *Severity risk rating* yang kategorikan sebagai celah keamanan yang tingkat *vulnerability* nya *High*.
    c. Sebanyak 2 celah keamanan yang memiliki *Severity risk rating* yang kategorikan sebagai celah keamanan yang tingkat *vulnerability* nya *Medium*.
3. Upaya untuk mengelola dampak yang dihasilkan dapat dilakukan dengan menerapkan mitigasi sesuai standar *CWE*. Berikut adalah langkah-langkah mitigasi yang diimplementasikan untuk satu kerentanan dengan tingkat kekritisan dan empat kerentanan keamanan dengan tingkat kerentanan Tinggi.

5.2 Saran

Berdasarkan penelitian yang sudah dilakukan terdapat beberapa saran yang dapat diterapkan pada penelitian berikutnya. Berikut ini merupakan saran-saran yang dapat diberikan penulis untuk penelitian selanjutnya:

1. Penelitian ini merupakan bersifat *Blackbox Testing*, sementara itu ada nya beberapa pengujian yang ada pada metodologi *web application penetration* testing milik *OWASP10* yang mengharuskan pengujian ini dilakukan dengan *Whitebox Testing* , contoh nya seperti pengujian dalam *role* yang ada pada aplikasi . Sehingga pengujian masih belum dikatakan maksimal.
2. Beberapa *tools* yang ada pada rekomendasi *OWASP10* tidak *up to date* sehingga untuk ke depan nya akan susah untuk memenuhi kebutuhan *evaluasi* celah keamanan yang lebih *up to date* juga.