

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

Berdasarkan hasil analisa dan pembahasan yang telah diuraikan pada bab sebelumnya, dapat ditarik kesimpulan berkaitan dengan *penetration testing* website menggunakan *open web application security project* yaitu sebagai berikut :

1. Dengan adanya *penetration testing* terhadap website ini, dapat mengetahui dan merekomendasikan perbaikan celah keamanan kepada *administrator* terhadap website agar terhindar dari *cyber attacker* dikemudian hari.
2. Dapat meningkatkan sistem keamanan website yang lebih baik untuk kedepannya.
3. Sudah diperoleh *file report* dari hasil *penetration testing* yang sudah dilakukan terhadap website tersebut.

Setiap website memiliki *vulnerability* yang berbeda. Untuk itu tidak setiap langkah yang penulis lakukan dapat persis di implementasikan untuk *penetration testing* website lain. Karena *vulnerability* yang berbeda ditangani dengan cara yang beda dan dengan *tools* yang berbeda juga.

#### **5.2 Saran**

*Penetration testing* website ini dilakukan berdasarkan sebatas pengetahuan penulis, untuk itu tidak menutup kemungkinan untuk dapat melakukan pengujian lainnya yang berkaitan dengan *penetration testing* website untuk mencapai tingkat keamanan yang lebih baik. Berikut ini adalah saran untuk memperbaiki kerentanan pada website yang sudah diuji sebagai berikut :

1. Melakukan *update* semua aplikasi secara berkala.
2. Menutup semua hak akses kepada semua *user* biasa, hanya *user* admin yang mendapat hak akses penuh terhadap attribut website.
3. Mengkonfigurasi fungsi keamanan secara benar dan tidak *default*.
4. Melakukan *monitoring server* secara berkala.