BAB 5
Kesimpulan dan Saran

5.1. *Kesimpulan*

Berdasarkan hasil penelitian penetration testing yang telah dilakukan menggunakan metode PTES (*Penetration Testing Execution Standard*), mulai dari tahap pra-engagement hingga pelaporan, dengan menggunakan serangan *cross-site scripting (XSS), SQL injection*, dan *forceful browsing* terhadap kerentanan *website* JKL untuk mengidentifikasi kelemahan keamanan *website*, kesimpulannya adalah sebagai berikut:

1. Terdapat dua jenis kerentanan yang ditemukan pada *website* JKL yaitu *cross-site scripting (XSS*) dan *broken access control. cross-site scripting (XSS*) rentan akan serangan *XSS via host header* namun, serangan ini memiliki dampak yang relatif kecil terhadap sistem *website* JKL. Meskipun demikian, serangan ini masih dapat digunakan untuk mendapatkan kredensial akun pengguna *website* JKL. Sedangkan *broken access control* rentan akan serangan *forceful browsing* serangan ini berdampak terhadap kerahasian sistem karena Terdapat beberapa direktori di dalam *website* yang dapat diakses oleh semua pengguna. Di beberapa direktori tersebut, terdapat data pengguna seperti foto profil pengguna yang seharusnya hanya dapat diakses oleh pengguna terkait. Selain itu, format foto tersebut dapat memberikan petunjuk tentang identitas pengguna di balik foto tersebut

2. Untuk mencegah atau mengatasi kerentanan yang ditemukan pada website JKL seperti *cross-site scripting (XSS*) pemilik website dapat melakukan konfigurasi pada file "*httpd.conf*" untuk menghapus atau menghilangkan nilai dari header yang ditentukan. Sedangkan untuk kerentanan *broken access control* pemilik website dapat melakukan

dua cara yaitu Membuat file *.htaccess* pada direktori yang ingin di tutup atau Memodifikasi konfigurasi pada file "*httpd.conf*" agar memblokir seluruh akses ke semua direktori

5.2. *Saran*

Berdasarkan penelitian yang telah dilakukan dalam bidang uji penetrasi, terdapat beberapa rekomendasi yang perlu dipertimbangkan untuk pengujian dan pengembangan lebih lanjut terkait kerentanan server. Berikut adalah beberapa saran untuk penelitian ini:

1. Membuat anggaran biaya terhadap solusi dari kelemahan yang diatasi untuk mempermudah pihak yang terkait dengan objek penelitian ini dalam melakukan perbaikan

2. Melakukan otomatisasi *pentest* dari tahap *Intelligence Gathering* hingga *Post Exploitation* agar dapat mempercepat proses uji keamanan