BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil pembahasan dapat disimpulkan bahwa pembuatan web aplikasi tanpa memperhatikan keamanan sangat rentan terhadap serangan *hacker*. Cara untuk mengetahui bahwa web aplikasi rentan terhadap serangan atau tidak adalah dengan mengetahui cara *hacker* bekerja. Ada dua level keamanan, yaitu berbahaya dan sedang.

Level berbahaya terdapat pada celah :

1. Injeksi (A1)
2. *Cross-Site Script ing* – XSS (A2)
3. Otentifikasi dan Manajemen Sesi Yang Buruk (A3)
4. *Cross-Site Request Forgery* – CSRF (A5)
5. Kesalahan Konfigurasi Keamanan (A6)
6. Penyimpanan Kriptografi Yang Tidak Aman (A7)
7. Redireksi *Forward* Yang Tidak Divalidasi (A10)

Dikatakan berbahaya karena celah ini berdampak langsung pada web aplikasi.

Level sedang terdapat pada celah :

1. Referensi Obyek Langsung Yang Tidak Aman (A4)
2. Gagal Membatasi Akses URL (A8)

Dikatakan sedang karena tidak berdampak langsung pada web apikasi. Tetapi di kalangan keamanan informasi ini tetap dianggap

celah, karena merupakan salah satu fase *hacking yaitu Information Gathering* atau Pengumpulan Informasi.

Sehingga Web Aplikasi ini sudah layak untuk di jadikan pembelajaran keamanan web aplikasi.

5.2 Saran

Berdasarkan hasil evaluasi terhadap penelitian ini, terdapat saran-saran untuk pengembangan penelitian selanjutnya sebagai berikut :

1. Mengimplementasikan celah untuk Perlindungan Layer Transport Yang Tidak Cukup (A9).
2. OWASP selalu mengupdate OWASP Top 10. sehingga 10 celah yang ada pada penlitian kali ini memungkinkan perubahan pada OWASP Top 10 berikutnya.
3. Banyak celah yang bisa diimplementasikan pada penelitian ini, salah satunya RFI (*Remote File Inclusion*).
4. Menyempurnakan Web Aplikasi dengan yang digunakan sehingga pembelajarannya bisa lebih baik