BAB V
PENUTUP

5.1 Kesimpulan

Dalam melakukan pengujian keamanan menggunakan *framework* ISSAF dan OWASP berdasarkan dari seluruh kegiatan yang dilakukan maka dapat diambil beberapa kesimpulan antara lain.

1. Pengujian keamanan pada website instansi XYZ dilakukan dengan menggunakan dua pendekatan yaitu *framework* ISSAF dan OWASP yang sebelumnya telah di sepakati dengan beberapa segmen.
2. Berdasarkan hasil pengujian yang dilakukan sebelumnya *framework* ISSAF dan OWASP sangat efektif untuk dijadikan sebagai acuan pengujian dikarenakan *framework* ini memiliki panduan yang mudah untuk diikuti. Dalam melakukan *penetration testing* menggunakan *framework* ISSAF dan OWASP penulis menemukan 3 celah keamanan *diantaranya Identified Viruses, File Extensions Information dan Default Credentials*.
3. Setelah dilakukan *penetration testing* penulis membuat 12 rekomendasi berdasarkan hasil pengujian yang telah dilakukan sebagai upaya untuk melakukan peningkatan keamanan pada website dan meminimalisir serangan yang mungkin akan terjadi.

5.2 Saran

Berdasarkan hasil penelitian ada beberapa saran yang masih dapat dikerjakan dengan lebih baik dan dapat dikembangkan lebih lanjut untuk peneliti yang melakukan penelitian dengan topik yang sama.

1. Perlu dilakukan pengujian menggunakan seluruh *control* yang ada pada ISSAF dan OWASP.
2. Mentransformasikan analisis keamanan ke tingkat yang lebih baik seperti *bug bounty* atau sejenisnya yang berperan khusus dalam mencari celah keamanan pada suatu website atau aplikasi.
3. Mencoba untuk melakukan validasi ulang terkait dengan hasil *scanning* otomatis OWASP ZAP dan Burp Suite.