BAB 5
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan rangkaian pengujian keamanan menggunakan metode pendekatan PTES *(Penetration Testing Execution Standard)* yang bertujuan untuk mengukur keamanan pada Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta yang hasilnya bisa menjadi acuan bahan evaluasi terkait tingkat keamanan Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta. Kesimpulan penelitian ini sebagai berikut:

1. Metode pengujian dengan pendekatan *PTES (Penetration Testing Execution Standard)* cocok dalam pengujian sistem, terutama celah yang ditemukan pada bagian *landing page (wp)* dan *web application*. Karena poin yang diuji tercakup dalam fase atau tahapan metode pengujian dengan pendekatan PTES *(penetration testing execution standard)* yang berhasil menemukan sebuah *Bug,vulnerable* pada keamanan yang bersifat medium hingga *critical*. Jika hal tersebut tidak di patch atau di tindak lanjuti secara tekhnis dipastikan bisa dieksekusi oleh pihak yang tidak bertanggung jawab.
2. Pengujian keamanan pada *landing page(wp)* dan *web application* dengan menggunakan metode pendekatan PTES *(Penetration Testing Execution Standard)* pada Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta melalui pengujian serangan *Eavesdropping*, XSS *(Cross Site Scripting)*, *Business Logic Vulnerability, File Upload Vulnerability*, hasilnya menunjukan terdapat tingkat resiko pada masing-masing bagian. Pada *landing page(wp)* memiliki tingkat resiko pada level *medium* dan pada *web appliaction* (mahasiswa) berada pada *level high* dan *critical.* Adapun *list category* penilaian tingkat resiko menggunakan OWASP TOP 10 2021 yang

telah ditampilkan pada Tabel 4.4 *Hasil Pengkategorian Referensi OWASP TOP 10 2021* .

3. Assessment terhadap keamanan pada Situs *web* Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta pada bagian landing page (wp) dan *web application* (mahasiswa)menunjukan hasil yang cukup riskan atau mengkhawatirkan. Karena berdasarkan OWASP *Risk Assement Calculator* menunjukan berada pada level MEDIUM. Untuk mendapatkan hasil tersbut dilakukan penganalisaan dengan beberapa tahapan. Tahapan tersebut seperti, *threat agent factors, vulnerability factors, technical impact factors, businsess impact factor* dan penganalisaan tersebut sudah terakumulasi secara *automate*. Seperti yang ditampilkan pada Gambar 4.50 *(OWASP Risk Assement Calculator Pada Objek Penelitian).*

5.2 SARAN

Berdasarkan rangkaian tahapan yang telah dilaksanakan terdapat beberapa saran yang dapat di implementasi dalam pengembangan Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta dan juga bisa menjadi acuan penelitian berikutnya yang bisa diterapkan dalam melakukan penelitian terkait. Berikut saran:

A. Saran untuk penelitian berikutnya:

1. Penulis menyarankan untuk penelitian berikutnya bisa menerapkan full metode pengujian dengan PTES*(Penetration Testing Execution Standard)* dan juga bisa menentukan *scope* secara jelas dalam pengujian sesuai pada studi kasus terkait.
2. Penulis menyarankan untuk penelitian berikutnya menggunakan jenis pengujian *Double Grey Box Penetration Testing* seperti yang terlihat pada Gambar 3.2 jenis pengujian yang terdapat pada OSSTMM *(Open Source Security Testing Methodology Manual).* hal tersebut diharapkan bisa memberikan *insight* dan evaluasi lebih

dalam terkait dari keamanan situs *web* Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta.

3. Penulis menyarankan perlunya meningkatkan *skill* dalam mendalami teknik -teknik lainnya dalam pengujian fase *exploitation* agar hasil yang didapat lebih akurat.

B. Saran untuk staff IT:

1. Penulis menyarankan agar pihak Pusat Sistem Informasi Universitas Jenderal Achmad Yani Yogyakarta memperbaiki dan memperbaharui *CMS* dan *Framework* yang sudah *last update*, karena hal tersebut bisa memunculkan *Bug* atau kerentanan yang lain.
2. Penliti menyarankan perbaikan dan peningkatan keamanan pada situs web Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta oleh pihak *front end* dan *back end*, yang kemudian ditindak lanjuti oleh QA *(Quality Assurance)* untuk memvalidasi anomali yang membuat situs *web* menjadi *down (defacement)*. Hal tersebut tentunya akan mengganggu kegiatan pengguna sistem.

C. Saran untuk Pemilik Sistem:

Penulis menyarankan tahapan pengujian dilakukan kembali dan dilakukan oleh *Cyber Secuity Profesional (Penetration Tester)* yang berpengalaman minimal 5 -7 tahun dan bersertifikasi .