

BAB V

KESIMPULAN DAN SARAN

Pada bab ini akan terdapat kesimpulan dan saran berdasarkan hasil analisis yang dilakukan pada bab tiga dan implementasi yang terdapat pada bab empat. Hal ini dilakukan untuk membantu Diskominfo Kabupaten Bandung untuk mengola keamanan sistem yang mereka miliki.

5.1. Kesimpulan

Berdasarkan hasil analisis dan pengujian dari ketiga *Framework* , *Penetration Testing Execution Standard (PTES)*, *Information System Security Assesment Framework (ISSAF)*, dan *Open Web Application Security Project (OWASP)* didapatkan hasil:

1. Menurut *Framework Penetration Testing Execution Standard (PTES)*, domain **diskominfo.bandung.go.id** memiliki kerentanan berlevel **Medium**, dengan *Risk Rating* 6, hal ini berdasarkan bahwa menurut penelitian dengan menggunakan *Framework* ini, domain diskominfo.bandung.go.id memiliki 3 kerentanan, yaitu *Application Error Message (CWE-209)*, *Error Message on Page (CWE-200)*, *Vulnerable Javascript Library (CWE-16)*. *Application Error Message (CWE-209)*.
2. Menurut *Framework Information System Security Assesment Framework (ISSAF)*, domain **diskominfo.bandung.go.id** memiliki 3 kerentanan yaitu *Application Error Message*, *Error Message On Page*, *Vulnerable Javascript Library (CWE-16)*.. *Framework* ini tidak memiliki memiliki *Risk Rating*.
3. Menurut *Framework Open Web Application Security Project (OWASP)*, domain **diskominfo.bandung.go.id** memiliki kerentanan berlevel **Medium**, berdasarkan perhitungan berdasarkan perhitungan dengan menggunakan *Risk Rating Methodology*.

4. Berdasarkan hasil penelitian ini, menurut penulis bahwa *Framework* yang tepat untuk digunakan pada DISKOMINFO kota Bandung ialah *Framework Penetration Testing Execution Standard (PTES)* dan *Open Web Application Security Project (OWASP)*, dikarenakan penilaian pada *Framework* ini menggunakan level-level yang dapat dimengerti oleh user yang bukan hanya orang yang berpengalaman dengan *Penetration Testing*, tetapi dapat juga dimengerti oleh *user* yang juga tidak memiliki pengalaman di bidang *Penetration Testing*. Sedangkan *Framework Information System Security Assesment Framework (ISSAF)* hanya dapat dimengerti oleh *user* yang berpengalaman pada bidang *Penetration Testing*, dikarenakan *reporting* pada *Framework* ini tidak memiliki level-level seperti pada kedua *Framework* yang lain.

5.2. Saran

Berikut ini adalah saran – saran berdasarkan penelitian di Dinas Komunikasi dan Informatika Kota Bandung guna untuk penelitian yang lebih lanjut adalah sebagai berikut :

1. Memberikan format laporan mengenai kerentanan - kerentanan berdasarkan ketiga *Framework* , *Penetration Testing Execution Standard (PTES)*, *Information System Security Assesment Framework (ISSAF)*, dan *Open Web Applicatin Security Project (OWASP)* yang bisa digunakan untuk penelitian dimasa yang akan datang
2. Menjaga *Website* dengan menggunakan acuan dari hasil laporan yang telah dilakukan dan berharap dapat mencegah kerentanan yang akan datang.