BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan hasil analisis dan pengujian terhadap *website* Rumah Sakit Umum Daerah (RSUD) Provinsi NTB. Dapat disimpulkan bahwa:

1. Dengan menggunakan metode *Penetration Testing Execution Standard* (PTES) mampu memberikan hasil yang terstruktur dan efektif.
2. setelah melakukan pengujian dan analisis pada sistem web server. *website* RSUD Provinsi NTB memiliki 23 kerentanan, dimana dari 23 kerentanan ini terdapat *risk Severity* dengan Resiko *Medium* yaitu 9 diantaranya (*Absence of anti-CSRF token, Content security Policy (CSP) header not set, Cross-Domain Misconfiguration, Missing anti-clicjacking, Secure page includes mixed content (including scripts), Seassion ID in URL Rewrite, Cross-domain JavaScript Source File Inclusion, X-Content-type-options header Missing, User Controllabel HTML Element Attribute (Potential XSS),*) dan sedangkan *risk Severity* dengan Resiko *Low* yaitu 13(*Cookie with SameSite Attribute none, Cookie without SameSite Attribute, Secure Pages Includes Mixed Content, Server Leaks Server Leaks Information via "X-Powere-By" http Response header field, Server Leaks version information via "server" http Response header field, Strict-Transport-security header not yet, Timestamp Disclosure-unix, Information Disclosure-sensitif Information in URL, Information Disclosure-Suspicious comment, Lossely Scoped Cookie, Modern Web Application, Re-examine Cache-control Directive, Retrieved From Cache, Session Management Response Identiffied*).
3. kerentanan web server pada pihak instansi RSUD Provinsi dapat diketahui dengan menggunakan metode *Penetration Testing Execution Standard* (PTES) dengan beberapa tahapan yaitu *pre-*

engagement, Intelligence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post-Exploitation. Kemudian tingkat keamanan di ukur dengan menggunakan OWASP ZAP *Risk Rating*, sehingga tingkat kerentanan dapat dipetakan dalam kategori *low, medium* dan *High*. Dari hasil pengukuran kerentanan dengan menggunakan OWASP ZAP risk Rating terdapat beberapa kerentanan yang memang harus segera di perbaiki yaitu kerentanan *clickjacking X-Frame-Options Header Missing, cross-Domain Misconfiguration, x-content-type-options header Missing*.

5.2. Saran

Berdasarkan hasil analisis dan kesimpulan yang diambil, maka penulis mengusulkan hal-hal sebagai berikut:

1. Memastikan agar web server tidak ada kesalahan dalam mengkonfigurasikan *system website* agar terhindar dari kerentanan-kerentanan yang sudah di temukan.
2. Pihak instansi dapat menguji Kembali hasil analisis yang dilakukan dengan berbagai *tools vulnerability* agar hasil lebih detail.
3. Untuk penelitian selanjutnya dapat dilakukan lebih mendalam yang meliputi uji coba yang lebih luas dan analisis lebih dalam dengan menggunakan beberapa metode yang lain.