BAB I

PENDAHULUAN

1.1 Latar Belakang

Penggunaan internet telah meningkat pesat secara global, dan penggunaan aplikasi *web* dalam banyak bidang kehidupan sehari-hari, seperti pendidikan, kesehatan, keuangan, dan hiburan, juga meningkat. Namun, terdapat peningkatan jumlah masalah keamanan aplikasi *web* yang secara langsung mengancam kerahasiaan, ketersediaan, dan integritas data (Albalawi *et al.*, 2023). Menurut Alotaibi and Vassilakis, (2023) aplikasi *web* rentan terhadap serangan keamanan, seperti *SQL injection*, yang dapat membahayakan data dan privasi pengguna. Berbagai solusi telah diusulkan untuk mengurangi keparahan ancaman ini, seperti *firewall* aplikasi web (WAF). Serangan *SQL Injection Attack* (*SQLIA*) merupakan salah satu serangan yang paling parah yang dapat digunakan terhadap aplikasi web berbasis database (Aliero *et al.*, 2020). Aplikasi *web* merupakan platform yang populer dalam menyampaikan informasi melalui internet, menyediakan berbagai layanan online seperti situs jejaring sosial, email, perbankan internet, dan aplikasi *e-commerce* dengan memanfaatkan beragam teknologi dan komponen *web*. Meskipun demikian, aplikasi *web* rentan terhadap serangan keamanan, seperti *cross-site scripting* (XSS) dan injeksi kode, yang dapat mengancam keamanan data dan privasi pengguna (Indushree *et al.*, 2022). Dengan adanya berbagai ancaman ini, penting untuk menerapkan solusi keamanan yang efektif guna melindungi aplikasi web dan data pengguna dari potensi serangan.

Rumah Sakit Unand merupakan Rumah sakit Perguruan tinggi Negeri (RSPTN) yang berada dibawah pengelolaan Universitas Andalas. Rumah sakit yang berada di kompleks kampus Unand Limau Manis, kecamatan Pauh, kota Padang, Sumatera Barat. Rumah sakit ini berdiri di atas tanah seluas 3.5 Ha dengan luas bangunan 21.306 m^2 didirikan dengan dana dari *Islamic Development Bank* (*IDB*) (RS Unand, 2023). Menteri Kesehatan RI (2022), mengeluarkan Peraturan Menteri

Kesehatan (Permenkes) yang mengatur semua fasilitas kesehatan wajib penggunaan rekam medis elektronik di fasilitas pelayanan kesehatan.

Rekam Medis adalah dokumen yang memuat data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang diberikan kepada pasien. Rekam Medis Elektronik adalah bentuk rekam medis yang disusun menggunakan sistem elektronik untuk pengelolaan rekam medis (Menteri Kesehatan RI, 2022). Seorang perekam medis harus memiliki keahlian dalam merancang manajemen Risiko Manajemen Etika dan literasi IT. Mampu membuat perencanaan rekam medis elektronik dengan langkah-langkah mulai dari menganalisis kebutuhan fungsional dan non-fungsional, merancang sistem, menguji sistem, hingga mengoperasikan sistem secara efektif (Meirina *et al.*, 2022).

Rekam Medis Elektronik harus memenuhi prinsip keamanan data dan informasi, meliputi: kerahasiaan; integritas; dan ketersediaan. Kerahasiaan sebagaimana dimaksud merupakan jaminan keamanan data dan informasi dari gangguan pihak internal maupun eksternal yang tidak memiliki hak akses, sehingga data dan informasi yang ada dalam Rekam Medis Elektronik terlindungi penggunaan dan penyebarannya (Menteri Kesehatan RI, 2022).

Undang-Undang Informasi dan Transaksi Elektronik (Presiden Republik Indonesia, 2024), tidak secara spesifik menyebutkan tentang keamanan data dalam pasal-pasal tertentu. Namun, beberapa pasal yang berkaitan dengan perlindungan data dan keamanan informasi dalam UU ITE antara lain.

1. Pasal 26 UU ITE menyatakan bahwa setiap orang memiliki hak untuk perlindungan data pribadi yang dihasilkan, diproses, disimpan, dikelola, dan/atau diumumkan oleh pihak lain melalui perangkat elektronik. Pasal ini mengakui hak setiap individu untuk memiliki kendali atas data pribadi mereka sendiri yang diperoleh atau diolah melalui perangkat elektronik. Hal ini menegaskan pentingnya perlindungan privasi dan kontrol atas informasi pribadi dalam lingkungan digital.
2. Pasal 27 UU ITE menyatakan bahwa setiap orang yang menyimpan dan mengelola data pribadi orang lain wajib memastikan bahwa data tersebut diolah sesuai dengan ketentuan undang-undang yang berlaku. Penyimpanan dan pengelolaan data pribadi harus dilakukan secara aman dan terlindungi dari akses yang tidak sah.

Pasal ini menegaskan tanggung jawab bagi pihak yang menyimpan dan mengelola data pribadi untuk memastikan bahwa data tersebut dikelola dengan benar dan sesuai dengan ketentuan hukum. Hal ini mencakup perlindungan data dari akses yang tidak sah serta memastikan keamanan data secara umum.

3. Pasal 28 UU ITE menyatakan bahwa setiap pemilik data pribadi bertanggung jawab untuk menjaga keamanan data pribadinya dari kerugian, kebocoran, atau akses yang tidak sah. Pemilik data pribadi juga bertanggung jawab untuk memberikan informasi yang benar, jelas, dan lengkap kepada pihak yang meminta data tersebut. Pasal ini menekankan tanggung jawab individu sebagai pemilik data pribadi untuk melindungi informasi mereka dari risiko kerugian, kebocoran, atau akses yang tidak sah. Selain itu, pemilik data pribadi juga diharapkan untuk memberikan informasi yang akurat dan lengkap ketika diminta oleh pihak lain. Ini merupakan bagian dari upaya untuk menjaga keamanan dan integritas data pribadi dalam lingkungan digital.

Pasal tersebut diatas menggaris bawahi pentingnya perlindungan, penyimpanan, pengelolaan, dan keamanan data pribadi dalam konteks penggunaan teknologi informasi dan transaksi elektronik, serta memberikan kerangka hukum untuk perlindungan privasi dalam lingkungan digital.

Penelitian ini mengidentifikasi dan mengatasi kerentanan *SQL Injection (SQLi)* pada server *web* melalui pengujian menggunakan berbagai alat, termasuk *Whois*, *SSL Scan*, *Nmap*, *OWASP Zap*, dan *SQL Map*. Hasil pengujian menunjukkan adanya 14 kerentanan, dengan lima di antaranya pada level sedang (35%), tujuh pada level rendah (50%), dan dua pada level informasional (14%). Pengujian menggunakan *SQL Map* berhasil mengakses *database* dan nama pengguna pada server *web*. Untuk mengurangi risiko serangan *SQLi*, penelitian ini merekomendasikan pemasangan *firewall* sebagai langkah mitigasi. Kontribusi utama dari penelitian ini adalah pengembangan metodologi terstruktur untuk mengidentifikasi dan menangani kerentanan *SQLi* pada server *web*, yang penting untuk menjaga keamanan dan integritas data dalam lingkungan online yang terus berkembang (Fadlil, Riadi and Mu'Min, 2024). Penilaian kerentanan aplikasi *web* melibatkan deteksi, analisis, dan peringatan organisasi terhadap komponen rentan dalam aplikasi *web*. Pengujian penetrasi dilakukan dengan tujuan mengeksploitasi kerentanan untuk menilai kelayakan ancaman dunia maya yang berpotensi memengaruhi organisasi (Jarupunphol *et al.*, 2023).

Penilaian kerentanan aplikasi *web* adalah langkah penting dalam menjaga keamanan aplikasi *web*. Terdapat dua metode yang umum digunakan dalam melakukan pengujian kerentanan, yaitu manual dan otomatis. Sebagian besar alat penguji kerentanan dapat secara otomatis memindai dan menganalisis kerentanan, serta menyediakan laporan terperinci untuk membantu mengatasi kerentanan yang berpotensi dieksploitasi oleh ancaman siber. Selain itu, alat-alat tersebut juga mengumpulkan informasi tentang kerentanan dalam *database web* mereka, memudahkan tindakan lebih lanjut dalam penilaian kerentanan. Alat-alat seperti *OWASP ZAP* dan *Burp Suite* adalah contoh alat yang digunakan untuk melakukan penilaian kerentanan aplikasi *web*. Mereka mengumpulkan informasi dalam aplikasi *web* dan memindai kerentanan yang mungkin dieksploitasi. Setelah menyelesaikan operasinya, prosedur yang sama diulangi untuk meningkatkan akurasi dalam melacak serangan pada aplikasi *web* (Jarupunphol *et al.*, 2023).

Open Web Application Security Project (*OWASP*) *Top* 10, telah menganalisis lebih dari 130.000 aplikasi, mengidentifikasi masalah keamanan aplikasi *web* yang paling umum pada tahun 2021. Temuannya mengungkapkan bahwa hampir 68% aplikasi memiliki kerentanan yang tercantum dalam *OWASP Top* 10. Daftar ini mencakup *Cross-Site Scripting*, *Insecure Deserialization*, *Insufficient Authentication*, *Sensitive Data Exposure*, *XML External Entities*, *Security Misconfiguration*, *Broken Access Control*, dan *Insufficient Logging and Monitoring*. *OWASP* menyediakan metodologi komprehensif untuk menilai dan memitigasi risiko ini, yang bertujuan untuk memandu pengembang dalam menciptakan aplikasi yang aman (Adeniran *et al.*, 2024).

Perubahan yang sangat cepat terkadang mengabaikan pentingnya pengujian aplikasi yang dibangun oleh pengembang. Pengujian merupakan tahap yang krusial dalam pengembangan perangkat lunak berkualitas tinggi. Kesalahan kecil yang dianggap remeh dapat menjadi celah berbahaya bagi penyerang untuk mengeksploitasi informasi yang dicuri melalui serangan terhadap situs *web* atau aplikasi. *Vulnerability assessment* menjadi sangat penting dalam pengelolaan situs *web* atau aplikasi berbasis *web*. Kebutuhan akan *vulnerability assessment* sering diabaikan, dianggap sebagai formalitas belaka, dan dilakukan oleh sedikit orang (Setiawan and Saedudin, 2022).

Website Vulnerability Scanner merupakan simulasi serangan pada sistem dengan cara mendapatkan akses ke data sensitif, dan menentukan apakah suatu sistem

aman atau tidak (Deeptha, 2023). *Vulnerability Assessment* (VA) merupakan sebuah cara penilaian kerentanan dengan melakukan pengujian celah keamanan untuk mengetahui seluruh potensi kelemahan kritis dari *website* (Darojat *et al.*, 2022). Penelitian mengenai pengujian dan analisis keamanan *website* menggunakan Acunetix *Vulnerability Scanner* menjelaskan bahwa proses dilakukan dalam dua iterasi, di mana setiap iterasi melibatkan dua kali scanning. Pada iterasi pertama, setelah dua kali scanning dilakukan, ditemukan bahwa *website* yang diuji memiliki tingkat ancaman 3, masuk dalam kategori tinggi. Setelah menganalisis dan melakukan perbaikan pada *website*, dilakukan iterasi kedua dengan melakukan dua kali *scanning* ulang. Hasil pengujian menunjukkan perubahan, dengan *website* yang sebelumnya memiliki tingkat ancaman 3, kini berada pada tingkat 1, yang termasuk dalam kategori rendah. Penelitian ini menggunakan *tool Acunetix WVS* untuk melakukan assessment dan perbaikan guna mengurangi kerentanan yang ditemukan pada *website* (Zirwan, 2022).

Acunetix Vulnerability Scanner, yang merupakan pemindai keamanan *web* pertama yang diluncurkan pada tahun 2005, terus mengalami peningkatan dan pengembangan. Alat khusus ini telah dikembangkan oleh para ahli pengujian keamanan *web*, sehingga menghasilkan solusi yang lebih efektif daripada banyak alat serupa. Mesin pemindai kerentanan Acunetix, yang ditulis dalam bahasa pemrograman C++, menjadikannya salah satu alat keamanan *web* tercepat di pasaran, sebuah aspek yang sangat penting ketika melakukan pemindaian terhadap aplikasi *web* yang kompleks dan memanfaatkan banyak kode *javaScript* (Invicti, 2023).

Keunikan lain dari *Acunetix* adalah penggunaan algoritma pemindaian yang cerdas, dikenal sebagai *SmartScan*, yang mampu menemukan hingga 80% kerentanan dalam 20% pemindaian pertama. Sebagai pemindai kerentanan *web DAST* (*Dynamic Application Security Testing*) otomatis terbaik, *Acunetix* mampu memeriksa ratusan aplikasi *web* dalam waktu singkat dan mendeteksi ribuan kerentanan dengan akurasi tinggi. Alat ini juga mendukung beragam teknologi termasuk *JavaScript* dan *HTML5*, memastikan bahwa kerentanan pada aplikasi yang menggunakan teknologi terbaru dan terhebat pun dapat terdeteksi dengan baik (Invicti, 2023).

Vulnerability Assessment (VA) merupakan bagian dari *risk assessment* yang terdiri dari *risk analysis, policy development, training and implementation*, dan *vulnerability assessment and Penetration Testing. Vulnerability Assessment* (*VA*) adalah proses pemindaian sistem atau *software* dan jaringan untuk mengetahui

kelemahan dan celah yang ada, celah ini memberikan *backdoor* ke penyerang untuk menyerang korban. Sebuah sistem sebaiknya memiliki akses kontrol terhadap *vulnerability, boundary condition vulnerability, input validation vulnerability, authentication vulnerabilities, configuration weakness vulnerabilities, dan exception handling vulnerabilities* (Zirwan, 2022).

Identifikasi masalah dalam penilaian kerentanan *Web API* menggunakan alat tradisional, yang sering kali tidak memadai karena banyaknya *endpoint* dan parameter dalam *Web API*. Untuk mengatasi masalah ini, penelitian Ishida *et al.* (2024) mengusulkan metode otomatis untuk menilai kerentanan *Web API* dengan memanfaatkan referensi, permintaan, dan respons *Web API*. Evaluasi eksperimen menunjukkan bahwa metode yang diusulkan efektif dalam mendeteksi kerentanan terkait otorisasi pada lingkungan pengujian yang rentan dan Sistem Manajemen Konten terkenal seperti *Wordpress, Ghost CMS, dan Joomla*.

Penelitian mengenai *Vulnerability Assessment* (*VA*) ini juga pernah dilakukan oleh Listartha *et al.* (2021), peneliti mencari kerentanan dengan teknik yang terotomatis dan manual dengan mencari kerentanan yang diketahui berdasarkan *OWASP 2017* dengan menggunakan aplikasi *Burp Suite*. Hasil deteksi kerentanan kemudian dipetakan dalam tiga tingkat bahayanya dengan melihat risiko eksploitasinya. Hasil penelitian ini mampu mengeksploitasi celah-celah keamanan yang ada pada *website* target meskipun sistem tersebut dibangun menggunakan *framework* yang telah teruji sekalipun.

Penggunaan *security scanner* pada penelitian yang dilakukan Arta *et al.* (2024), untuk mengidentifikasi kelemahan aplikasi *web* sebelum dirilis sangat penting untuk keberlangsungan *web*. Penelitian ini menganalisis keamanan *web* menggunakan *OWASP* dan *Arachni* pada aplikasi *web*. Hasilnya menunjukkan bahwa beberapa penelitian sebelumnya tidak dapat mengukur efektivitas pemindai secara terukur. Dalam studi ini, *OWASP ZAP* memperoleh skor 75,61, sedangkan *Arachni* mendapatkan skor 62,20%. Dengan menggunakan tolok ukur ini, analisis hasil pemindai menjadi lebih terukur dan dapat dinilai secara statistik, memungkinkan organisasi untuk mengambil langkah-langkah yang tepat untuk mengatasi celah keamanan yang ditemukan.

Penelitian oleh Carlos P. Flores Jr. (2024) menganalisis kerentanan keamanan pada situs *web* universitas negeri dan perguruan tinggi di Filipina dengan menggunakan alat *open-source OWASP Zed Attack Proxy* (*ZAP*). Berdasarkan panduan *OWASP Top 10*, penelitian ini mengidentifikasi berbagai risiko keamanan di 17 *SUC* (*State Universities and Colleges*), termasuk kerentanan terhadap injeksi (23,53%), desain yang tidak aman (40,06%), komponen yang sudah usang (70,59%), konfigurasi keamanan yang salah (88,24%), dan kontrol akses yang rusak (94,12%). Kerentanan ini dapat dieksploitasi oleh pihak jahat untuk mendapatkan akses yang tidak sah dan membahayakan ketersediaan, kerahasiaan, atau integritas data. Penelitian ini merekomendasikan agar *SUC* mengadopsi panduan *OWASP Top 10* dan mengambil langkah-langkah untuk mengurangi risiko yang terkait dengan situs web mereka.

Penelitian yang dilakukan oleh Kristianto, Rahman and Bahri (2022) pada *Website* servio diperoleh kerentanan–kerentanan seperti *HTML* tanpa perlindungan *CSRF, clickjacking*, dan beberapa *web alert informational*. Hasil yang ditemukan *Acunetix* berada pada *level medium*, yang berarti kerentanan terjadi karena kesalahan konfigurasi dan *site coding* yang lemah. Sandy and Solihin, (2021) menyebutkan bahwa untuk mengurangi kerentanan pada keamanan sistem serta mengurangi risiko kemungkinan kehilangan data, maka perlu dilakukannya audit pada sistem *e-Learning* yang diangun menggunakan sistem *NIST*.

Penelitian yang dilakukan Arromdoni, Kusuma and Sugiantoro (2024) terhadap aplikasi *Cyber Security and Digital Forensics* (*CSFD*) *Open Journal System* (*OJS*) milik PTIPD Universitas Islam Negeri Sunan Kalijaga Yogyakarta mengungkapkan beberapa kerentanan keamanan. Berdasarkan pemindaian menggunakan *Acunetix*, ditemukan 18 kerentanan dengan risiko *medium*, 8 dengan risiko *low*, dan 10 kerentanan *informational*. Sebagai perbandingan, pemindaian menggunakan *OWASP-ZAP* menemukan 17 kerentanan, termasuk 1 dengan status *high*, 4 dengan status *medium*, 8 dengan status *low*, dan 4 *informational*.

Penelitian pengujian keamanan domain *web* PT. Sadikun Niagamas Raya terhadap serangan dari pihak luar dan menghasilkan laporan yang dapat dipahami mengenai hasil uji penetrasi. Metode yang digunakan adalah *Penetration Testing*, yang mencakup langkah-langkah mulai dari pengumpulan informasi hingga pembuatan laporan. Hasil penelitian menunjukkan adanya tiga celah keamanan: 1) Kemungkinan

penyisipan dan eksekusi skrip melalui kolom pencarian, 2) Akses ke nama pengguna dan kata sandi dalam database akibat parameter ID yang rentan terhadap serangan *SQL injection*, dan 3) Kemungkinan pengunduhan database melalui *URL* karena kesalahan konfigurasi di sisi server. Temuan ini sesuai dengan kerentanan umum yang terdaftar dalam kerangka *OWASP*, yang dapat membahayakan PT. Sadikun Niagamas Raya (Ikhsan, Alwi and Hasanuddin, 2024).

Aplikasi *web e-marketplace* merupakan fitur penting dalam bisnis modern, namun sering kali keamanan dianggap kurang penting dibandingkan aspek lainnya. Penelitian yang dilakukan Ula, Adek and Bustami (2023) bertujuan untuk menilai kerentanan keamanan dari *e-marketplace* yang dikembangkan sendiri dengan menggunakan dua framework, yaitu *CodeIgniter* dan *Content Management System* (*CMS*). Metode yang digunakan adalah *OWASP Risk Rating Methodology*, dengan tahap penelitian meliputi perencanaan pengujian, proses pengujian, analisis kerentanan, dan penilaian risiko *OWASP*. Hasil penelitian menunjukkan bahwa *platform* pengembangan aplikasi *web* menggunakan *CodeIgniter* dan *CMS* memiliki tingkat kemungkinan kerentanan dengan tingkat keparahan Menengah, sementara dampaknya berada pada tingkat Rendah. Kesimpulannya, meskipun hasilnya menunjukkan bahwa tidak ada jaminan bahwa platform ini akan bebas dari celah keamanan, pengembangan *framework e-marketplace* dengan keamanan yang lebih tinggi sangat diperlukan.

Penilaian kerentanan pada aplikasi web universitas, termasuk *Burp Suite* dan *OWASP ZAP*, berdasarkan tiga kriteria jumlah kerentanan menurut metrik risiko dan kepercayaan, jumlah jenis kerentanan dan peringatan *URL*, serta kerentanan yang termasuk dalam 10 kerentanan teratas *OWASP 2021*. Hasil penelitian Jarupunphol *et al.* (2023) menunjukkan bahwa *Burp Suite* mendeteksi lebih banyak kerentanan dan peringatan dengan proporsi kerentanan risiko tinggi yang lebih besar dibandingkan *OWASP ZAP*, sementara *OWASP ZAP* memiliki proporsi kerentanan kepercayaan menengah yang lebih tinggi. Perbandingan juga mengungkapkan perbedaan peringkat kerentanan dalam *OWASP Top* 10 antara kedua alat dan variasi dalam prioritas risiko. Meskipun ada perbedaan, hasil penilaian kerentanan dari kedua alat tetap bermanfaat bagi analis keamanan dan administrasi universitas dalam mengatasi ancaman siber terhadap aplikasi web mereka.

Aanalisis kerentanan keamanan pada situs web AB dan XY *Service* di Jawa Timur oleh Zaidan *et al.* (2023), dengan menggunakan pemindaian data, analisis

kerentanan, dan eksperimen *Brute Force*. Meski terbatas pada dua situs *web* dan menggunakan analisis statistik deskriptif, hasilnya mengidentifikasi kelemahan seperti konfigurasi situs *web* dan penanganan kerentanan yang tidak memadai. Temuan ini memberikan pemahaman mendalam tentang ancaman keamanan dan dasar untuk perbaikan keamanan yang lebih efektif dan perlindungan data yang lebih baik.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang disampaikan, terdapat beberapa masalah yang bisa diangkat. Penelitian ini akan difokuskan pada dua perumusan masalah diantaranya sebagai berikut:

1. Bagaimana penggunaan *Acunetix Vulnerability Scanner* dapat mengoptimalkan keamaman pengujian dan menganalisis *vulnerability* pada aplikasi RME di RS Unand dalam mengurangi kerentangan keamanan?
2. Bagaimana pengujian *Acunetix Vulnerability Scanner* dapat mengetahui tingkat kerentanan keamaman pada aplikasi RME di RS Unand?
3. Bagaimana penerapan *Acunetix Vulnerability Scanner* dengan metode *OWASP Top 10* dapat meningkatkan tingkat keamanan aplikasi RME di RS Unand?

1.3 Batasan Masalah

Pembatasan masalah dilakukan agar penelitian yang dilakukan lebih terarah dan mencapai sasaran yang ditentukan, maka penelitian ini akan diberi batasan masalah sebagai berikut :

1. Aplikasi berbasis *web* yang menjadi target *Vulnerability Assessment* (*VA*) adalah Aplikasi Rekam Medis Elektronik di RS UNAND.
2. Perbaikan kerentanan hanya dilakukan pada Aplikasi Rekam Medis Elektronik di RS UNAND dengan *threat level medium* hingga *threat level high.*

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah dan batasan masalah yang disampaikan, maka tujuan penulis dalam melakukan penelitian ini adalah sebagai berikut:

1. Penggunaan *Acunetix Vulnerability Scanner* dapat mengoptimalkan keamaman pengujian dan analisis *vulnerability* pada aplikasi RME di RS Unand dalam mengurangi kerentangan keamanan.
2. Pengujian *Acunetix Vulnerability Scanner* dapat mengetahui tingkat kerentanan keamaman pada aplikasi Rekam Medis Pengujian *Acunetix Vulnerability Scanner* dapat mengetahui tingkat kerentanan keamaman pada aplikasi RME di RS Unand.
3. Penerapan *Acunetix Vulnerability Scanner* dengan metode *OWASP Top 10* dapat meningkatkan tingkat keamanan aplikasi RME di RS Unand.

1.5 Manfaat Penelitian

Beberapa manfaat yang ingin dicapai dalam penelitian ini adalah sebagai berikut :

1. Bagi Peneliti :

   Mendalami pengetahuan tentang pengujian keamanan menggunakan metode *vulnerability assessment*, dan dapat melakukan perbaikan dan peningkatan keamaan pada aplikasi aplikasi berbasis *web*.
2. Bagi Rumah Sakit Universitas Andalas :

   Mampu memberikan bantuan kepada RS UNAND khususnya Instalasi SIMRS di lingkungan RS Unand dalam meningkatkan kerentanan Aplikasi Rekam Medis Elektronik.

1.6 Sistematika Penulisan

Sistematika penulisan dilakukan agar lebih mudah untuk dibaca dan dimengerti, maka penulis berusaha menyusun laporan penelitian ini dengan tata urutan secara sistematis. Berdasarkan hal itu, peneliti mengklasifikasikan penelitian ini kedalam enam bab, antara bab satu dengan bab yang lain saling berhubungan.

BAB I : PENDAHULUAN

Pada Bab I menjelaskan latar belakang, perumusan masalah, Batasan-batasan masalah, tujuan dari penelitian, manfaat dari penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Pada Bab II menjelaskan tentang teori-teori pendukung yang berkaitan dengan penelitian dan penerapan metode yang digunakan dari literatur jurnal, artikel, makalah, dan lain-lain yang berkaitan dengan penelitian.

BAB III : METODE PENELITIAN

Pada Bab III menjelaskan tentang kerangka kerja, perangkat penelitian yang digunakan, menguraikan tahap-tahap analisis, menjelaskan proses perbaikan threat hasil *scanning* hingga menganalisa hasil *scanning* setelah dilakukan perbaikan.

BAB IV : ANALISA DAN PERANCANGAN

Pada Bab IV menjelaskan tentang analisa data dan pembahasan hasil yang didapat dari analisis berdasarkan *tool* dan *threat* yang digunakan.

BAB V : IMPLEMENTASI DAN HASIL

Pada Bab V menjelaskan tentang tahap implementasi dan pembahasan hasil yang didapat dari analisis berdasarkan *tool* yang digunakan dan *threat* yang ditemukan, serta analisa pengujian *threat* kedua.

BAB VI : KESIMPULAN DAN SARAN

Pada Bab VI berisi kesimpulan dan saran yang berkaitan dengan hasil akhir yang diperoleh dari hasil pengujian dan analisis *vulnerability* pada Rekam Medis Elektronik berbasis *web* di lingkungan Rumah Sakit Universitas Andalas menggunakan *Acunetix Web Vulnerability Scanner.*