BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dinas Informasi dan Pengolahan Data Angkatan Darat (Disinfolahtad) merupakan Badan Pelaksana Pusat di tingkat MABESAD yang berkedudukan langsung dibawah pimpinan Kasad dalam menyelenggarakan fungsi Pembina sistem informasi dan pengolahan data secara elektronis di tingkat pusat. Disinfolahtad terletak di Jalan Veteran Raya No. 5 Jakarta Pusat, DKI Jakarta [1].

Dalam rangka menunjang dan mengimplementasikan fungsi khusus pada sistem informasi dan pengolahan data khususnya di bidang anggaran, Disinfolahtad membangun dan mengembangkan aplikasi berbasis *website* bernama Aplikasi Laporan Pelaksanaan Anggaran (LAPLAKGAR) untuk membantu satuan jajaran di lingkungan Angkatan Darat dalam mengelola data anggaran secara elektronik. Tujuannya adalah untuk mewujudkan pelaksanaan anggaran yang tertib administrasi, transparan, dan akuntabel [2].

Berdasarkan hasil wawancara dengan Bagian sistem informasi administrasi perencanaan dan anggaran serta pengawasan dan pemeriksaan (Bagsisfominrengarwasrik) menyatakan bahwa dari 2 aplikasi anggaran yang dikelola, yaitu E-Audit dan LAPLAKGAR, memang tingkat kerentanan aplikasi LAPLAKGAR dinilai masih rentan dari segi sistem keamanannya karena aplikasi LAPLAKGAR perlu mempertimbangkan aspek lainnya pada saat pembangunan sehingga aplikasi ini digunakan oleh pengguna dengan berbagai keterbatasan. Karena itu, disiapkan dua versi aplikasi LAPLAKGAR, yaitu versi *online* dan *offline*. Versi *offline* digunakan untuk menginput data anggaran pada tingkat satuan dan kotama, sedangkan *online* digunakan untuk menginputkan serta menggabungkan data anggaran dari setiap satuan, kotama dan dapat diakses oleh setiap Kotama dan Pusat. Namun, adanya dua versi ini mempengaruhi efektivitas dan efisiensi produktivitas pekerjaan.

Pada tahun 2019, Personel Satgas *Cyber Defence* melaporkan kepada Kadisinfolahtad bahwa aplikasi LAPLAKGAR terkena serangan siber.

Adapun serangannya adalah, aplikasi LAPLAKGAR dijadikan alamat untuk menyerang situs atau web negara lain. Hal ini tentu membuat mobilisasi aplikasi LAPLAKGAR menjadi terganggu, serta mengancam keamanan informasi data, membahayakan sistem dan juga menimbulkan kekhawatiran jika sewaktu-waktu terjadi aksi peretasan kembali. Adapun penanganan awal yang dilakukan oleh Bagsisfominrengarwasrik adalah menginformasikan kepada Bagian Instalasi Pengolahan Data (Bagstallahta) untuk dilakukan penanganan, Adapun penanganan yang diberikan adalah dengan melakukan penguatan *security* jaringan.

Dengan penanganan yang diberikan sebelumnya, tentu hal ini tidak cukup untuk memberikan perlindungan sistem keamanan aplikasi LAPLAKGAR secara menyeluruh, dengan melakukan perancangan dan pengembangan aplikasi pengujian celah keamanan sesuai dengan standarisasi OWASP, tentu dapat membantu Bagsisfominrengarwasrik untuk melakukan perlindungan sistem keamanan yang dibutuhkan sesuai dengan hasil monitoring secara berkala. Software monitoring keamanan merupakan sebuah aplikasi yang dapat digunakan untuk melakukan *Vulnerability Assessment*, dimana *Vulnerability Assessment* adalah suatu metode yang mengikuti pendekatan terstruktur dan proaktif untuk menemukan kerentanan, tujuannya untuk menemukan masalah yang dikenal maupun tidak dikenal pada sistem [3]. OWASP TOP 10 merupakan sebuah *standard awareness* yang ditetapkan oleh OWASP yang dimana OWASP merupakan suatu organisasi nirlaba yang menyediakan dokumentasi dan alat yang lengkap, memiliki tingkat keandalan yang tinggi, bersifat *open source*, serta mudah dipahami, dengan menggunakan OWASP maka dapat membantu untuk mengetahui dan meningkatkan keamanan aplikasi website dengan baik [4]. OWASP TOP 10 dapat digunakan untuk mengelompokan 10 serangan yang sering menyerang aplikasi *website* [5]. Standard ini akan diimplementasikan untuk memberikan acuan tambahan dalam pengelompokan hasil pemindaian pada tahap *vulnerability assessment*. Dalam pengembangan aplikasi monitoring keamanan peneliti akan menggunakan metode *iterative*. Metode *iterative*

merupakan sebuah metode pengembangan sistem perangkat lunak yang dilakukan secara bertahap hingga mencapai hasil yang diharapkan [6].

Dalam penelitian sebelumnya pada tahun 2020 oleh Dedy Hariyadi, Fazlurrahman dan Hendro Wijayanto mengembangkan aplikasi Bangkolo yang memiliki antarmuka *GUI* yang dapat digunakan untuk *pentesting* dengan menggunakan *Electron Framework* dalam mengembangkan aplikasi *Vulnerability Identification* (aplikasi pengujian keamanan) yang masih memiliki antarmuka *CLI*. Bangkolo dikembangkan dengan menggunakan *framework ISSAF* dan pendekatan *Hybrid Apps*, adanya penelitian ini didasari bahwa masih banyak dan minimnya pengembang sistem dan jaringan untuk mengutamakan keamanannya [7]. Penelitian lain pada tahun 2018 oleh Fietyata Yudha dan Andi Muhammad Panji juga memberikan sebuah rancangan aplikasi terintegrasi yang dapat digunakan untuk melakukan pengujian celah keamanan terhadap aplikasi berbasis web (yang dibatasi seperti : *Phising*, *SQL Injection* dan *XSS*) dengan menggunakan bahasa python untuk mengidentifikasi titik kerentanan dari aplikasi web dimana platform ini dinilai cukup rentan terhadap serangan seperti *SQL Injection*, *Phising*, *XSS*, dan lainnya [8].

Sebagai upaya untuk mengatasi beberapa permasalahan yang dimiliki oleh aplikasi LAPLAKGAR dalam sisi keamanan aplikasi, maka peneliti akan melakukan pengembangan aplikasi monitoring keamanan untuk pengujian celah keamanan aplikasi laporan pelaksanaan anggaran berbasis website dengan standarisasi OWASP untuk membantu menemukan celah kerentanan yang ada pada aplikasi LAPLAKGAR.

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah tersebut maka dapat diuraikan identifikasi masalah sebagai berikut:

1. Diperlukan sebuah upaya yang dapat membantu meningkatkan keamanan Aplikasi LAPLAKGAR.
2. Diperlukan upaya yang dapat mengidentifkasi celah kerentanan dari Aplikasi LAPLAKGAR untuk meminimalisir aksi peretasan dan memberikan keyakinan pada Bagsisfominrengarwasrik agar aplikasi LAPLAKGAR dapat diakses online dengan menyeluruh.
3. Diperlukan aplikasi yang dapat menguji celah keamanan Aplikasi LAPLAKGAR guna dapat meningkatkan efektivitas dan efisiensi pekerjaan setiap Satker dan Kotama dalam mengelola data anggaran.

1.3 Maksud dan Tujuan

1.3.1 Maksud

Melakukan identifikasi atau pengujian celah keamanan dengan melakukan pengembangan aplikasi monitoring keamanan untuk pengujian celah keamanan LAPLAKGAR berbasis website dengan standarisasi OWASP.

1.3.2 Tujuan

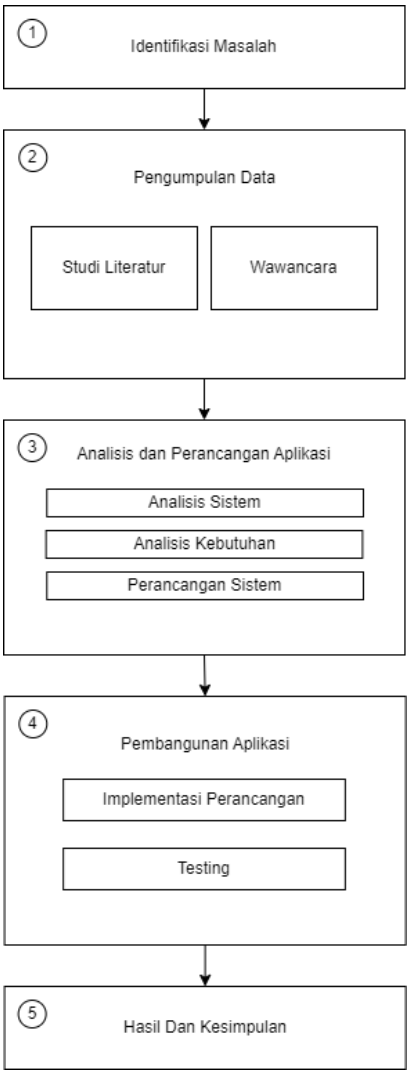
1. Melakukan identifikasi celah kerentanan pada aplikasi LAPLAKGAR.
2. Melakukan pengujian celah keamanan Aplikasi LAPLAKGAR.
3. Membangun sebuah Aplikasi monitoring keamanan untuk menunjang pengujian celah keamanan aplikasi LAPLAKGAR yang dapat digunakan sebagai acuan atau rekomendasi yang disarankan oleh OWASP untuk melakukan konfigurasi terhadap sistem keamanan aplikasi LAPLAKGAR.

1.4 Batasan Masalah

1. Penelitian ini hanya dilakukan didalam lingkungan Dinas Informasi dan Pengolahan Data Angkatan Darat (DISINFOLAHTAD).
2. Aplikasi Website yang dijadikan sebagai objek penelitian adalah Aplikasi Laporan Pelaksanaan Anggaran (LAPLAKGAR).
3. Penelitian ini hanya pada ruang lingkup pengujian celah keamanan untuk aplikasi berbasis website.
4. Penelitian ini membangun aplikasi monitoring keamanan berbasis website yang tidak bersifat destruktif atau merusak sistem.
5. Penelitian ini membatasi tingkat pengujian celah keamanan pada level aplikasi.
6. Standarisasi yang diimplementasikan dalam software monitoring keamanan menggunakan OWASP.
7. API yang digunakan untuk mengembangkan aplikasi menggunakan OWASP ZAP.
8. Pemodelan sistem dilakukan menggunakan UML.
9. Pengembangan aplikasi menggunakan metode objek oriented.
10. Pengembangan aplikasi menggunakan bahasa pemrograman Python.
11. Aplikasi dibangun menggunakan framework Flask.
12. Aplikasi monitoring keamanan akan dilakukan pengujian API, Performa, *Whitebox*, *blackbox*, UAT dan perbandingan temuan kerentanan.
13. Hasil dari penelitian berupa aplikasi (*Software* monitoring keamanan) yang dapat dijadikan sebagai acuan untuk meningkatkan sistem keamanan Aplikasi LAPLAKGAR oleh Bagsisfominrengarwasrik.
14. Hasil temuan kerentanan pada aplikasi monitoring keamanan dapat diunduh dengan format PDF.
15. Perbaikan berdasarkan hasil temuan kerentanan pada aplikasi LAPLAKGAR berfokus pada tingkat kerentanan *High-Medium*.

1.5 Metodologi Penelitian

Berikut merupakan metodologi atau alur penelitian yang dapat dilihat pada gambar 1.1.



Gambar 1.1. Alur Penelitian

Berdasarkan gambar 1.1, menjelaskan terkait dengan tahapan atau alur dari penelitian dengan detail sebagai berikut :

1. Identifikasi Masalah

   Identifikasi masalah merupakan sebuah proses untuk menentukan dan memahami masalah yang ada. Identifikasi masalah dalam penelitian, dapat membantu peneliti untuk mencari topik penelitian dengan melakukan analisis data dan informasi untuk mengidentifikasi

permasalahan yang mendasar dan mengkategorikan masalah sebagai solusi yang dapat diterapkan untuk menyelesaikan permasalahan, artinya dari topik penelitian yang diangkat akan didapat hasil sebagai solusi dari permasalahan yang ditemukan.

2. Pengumpulan Data

   Pengumpulan data bertujuan untuk mengumpulkan informasi atau data yang relevan dan berkualitas untuk menjawab pertanyaan penelitian. Data dikumpulkan melalui berbagai sumber dan teknik. Pada penelitian ini pengumpulan data dilakukan dengan membaca dan mengkaji studi literatur yang relevan untuk memperkuat topik penelitian dan melakukan wawancara sebagai tahap awal pengumpulan data, objek dan tempat penelitian. Data ini kemudian dianalisis untuk memperoleh hasil yang valid dan dapat dipercaya dalam penelitian

3. Analisis dan Perancangan Aplikasi

   Pada tahap ini, dilakukan analisis dan juga perancangan aplikasi. Peneliti menggunakan metode analisis dan design berorientasi objek dengan tahapan analisis kebutuhan dilakukan untuk memenuhi tujuan dan kebutuhan yang ditentukan seperti analisis data, analisis sistem yang berjalan, analisis kebutuhan fungsional hingga analisis kebutuhan non fungsional. Perancangan dilakukan sebagai upaya untuk melibatkan memahami dan memecahkan masalah yang akan ditemui oleh aplikasi, serta memastikan bahwa aplikasi tersebut mudah digunakan, *scalabel*, dan sesuai dengan kebutuhan pengguna. Perancangan sendiri terbagi menjadi perancangan arsitektur, perancangan pesan, perancangan jaringan semantik, hingga perancangan antarmuka.

4. Pembangunan Aplikasi

   Dalam proses ini, dilakukan tahap-tahap seperti implementasi perancangan, pemrograman, dan pengujian. Setelah melalui tahap perancangan, maka dilanjutkan dengan tahap pemrograman, dimana peneliti akan melakukan implementasi dari hasil perancangan sebelumnya sesuai dengan bahasa pemrograman yang telah ditentukan.

Pada tahap pengujian aplikasi, peneliti menggunakan metode *blackbox* dan *whitebox*, dimana peneliti akan melakukan pengujian aplikasi secara fungsional dan juga *design* serta kode sumber. Selain itu, aplikasi juga akan diuji berdasarkan fungsi API, Performa, hingga temuan kerentanan. Untuk memastikan bahwa aplikasi yang dibangun telah sesuai dengan yang diharapkan pengguna, maka akan dilakukan uji UAT (*User Acceptance Testing*) untuk mencapai tujuan akhir dari pembangunan aplikasi dalam penelitian yaitu memperoleh hasil penelitian sesuai dengan tujuan penelitian yang sedang dilakukan.

5. Hasil dan Kesimpulan

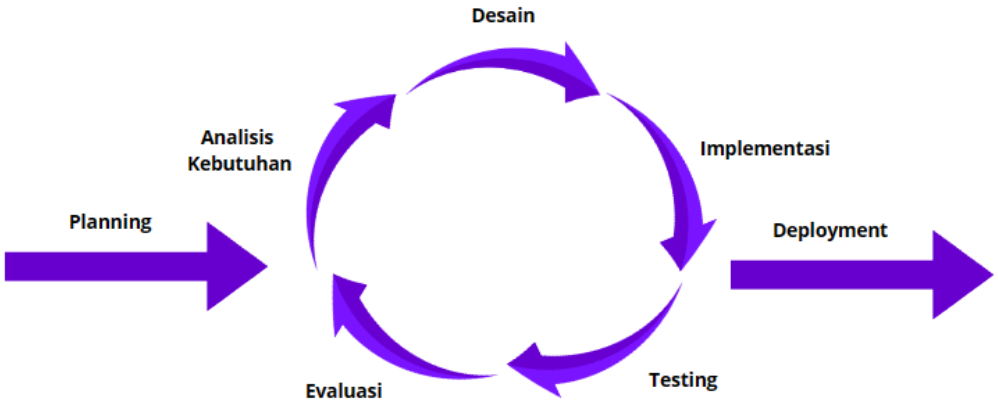
   Tahap ini merupakan tahap terakhir dari penelitian, dimana peneliti dapat memberikan kesimpulan dan hasil dari penelitian. Peneliti dapat mengungkapkan hasil akhir dari penelitian yang mengacu pada temuan yang diperoleh. Peneliti dapat memberikan kesimpulan sesuai dengan rumusan tujuan yang diharapkan. Kesimpulan dan hasil dalam penelitian sangat penting karena membantu memahami hasil penelitian dan menentukan arah untuk penelitian selanjutnya.

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan oleh peneliti yaitu menggunakan metode kuantitatif. Dimana peneliti melakukan wawancara langsung dengan Bagsisfominrengarwasrik yang bertanggung jawab terhadap operasional aplikasi LAPLAKGAR untuk mengetahui informasi, latar belakang masalah yang terjadi, serta cara kerja dari aplikasi dan diperoleh data kuantitas seperti jumlah aplikasi yang dikelola, jumlah serangan siber yang berhasil meretas aplikasi setiap bulannya, jumlah data setiap satker, kotama dan sebagainya. Selain itu, peneliti juga menggunakan teknik studi literatur untuk menunjang penelitian dengan melakukan pengumpulan studi literatur yang memiliki keterkaitan atau relevansi dengan penelitian.

1.5.2 Metode Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak dalam penelitian ini mengadopsi metode *iterative*. Pada penelitian pada tahun 2017 oleh Maikel Bolung dan Henry Ronald Karunia mengemukakan bahwa *iterative* memiliki kejelasan kebutuhan pengguna, penguasaan teknologi, tingkat kerumitan sistem, tingkat kehandalan sistem yang baik dan waktu pelaksanaan serta visibilitas jadwal pelaksanaan yang baik sekali [9].



Gambar 1.2 Metode Itterative

1. *Planning*

   Planning merupakan tahap awal dimana peneliti menentukan rencana dan strategi dalam proses pengembangan aplikasi. Tahap ini mencakup identifikasi tujuan dan harapan dari aplikasi yang akan dibuat, menentukan waktu yang diperlukan, dan lainnya. Tahap *planning* ini membantu peneliti untuk memahami konteks dan memastikan bahwa rencana pengembangan aplikasi dapat terintegrasi dengan baik.

2. Analisis Kebutuhan

   Pada tahap ini, merupakan tahap pengumpulan informasi dan analisis kebutuhan dari masing-masing *stakeholder* terkait aplikasi yang akan dikembangkan.

3. Desain

   Tahap ini merupakan tahap perencanaan dan perancangan aplikasi, seperti membuat sebuah diagram sistem dan desain antarmuka aplikasi yang akan dikembangkan.

4. Implementasi

   Tahap ini merupakan tahap pembuatan kode dan pengembangan aplikasi sesuai dengan implementasi desain yang telah dibuat pada tahap sebelumnya.

5. *Testing*

   Tahap ini merupakan tahap pengujian aplikasi untuk memastikan bahwa aplikasi bekerja sesuai dengan kebutuhan dan spesifikasi yang telah ditentukan.

6. Evaluasi

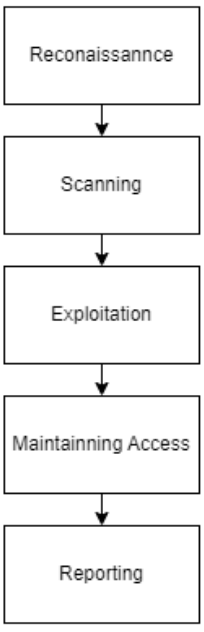
   Tahap ini merupakan tahap evaluasi dan pengecekan ulang aplikasi yang sudah dikembangkan, peneliti dapat melakukan perbaikan jika diperlukan.

7. *Deployment*

   Tahap ini merupakan tahap penerapan aplikasi ke lingkungan produksi.

1.6 Tahapan – Tahapan Metode Pengujian OWASP

Gambar 1.3 merupakan langkah-langkah pada metode OWASP yang dapat digunakan untuk melakukan pengujian kerentanan.



Gambar 1.3. Tahapan Metode OWASP [10]

1. *Reconaissannce*

   Reconnaissance merupakan tahapan awal pada pengujian kerentanan dengan OWASP. Pada fase ini, bertujuan untuk mengumpulkan informasi target guna memperoleh wawasan dan memahami lebih lanjut terkait target yang akan diuji. Pengumpulan informasi dapat berupa pemerolehan alamat URL, teknologi yang digunakan, sistem operasi, arsitektur sistem, melakukan pemetaan aplikasi seperti mengidentifikasi parameter input, hingga mengidentifikasi komponen sistem yang dapat diakses dari luar seperti halaman web, API, dan sebagainya. Pada proses ini, dapat dilakukan dengan cara melakukan pengamatan langsung, pencarian publik, hingga menggunakan alat bantu.

2. *Scanning*

   Scanning merupakan tahapan kedua setelah fase *reconnaissance*. Fase ini bertujuan untuk mengidentifikasi kerentanan yang ada pada alamat target untuk mendapatkan informasi lebih lanjut mengenai kelemahan yang ada pada sistem atau aplikasi yang diuji. Pada fase ini, dapat didukung dengan menggunakan alat dan teknik untuk mengidentifikasi kerentanan. Umumnya, pada fase *scanning* disesuaikan dengan kebutuhan pengujian yang terdiri dari *port scanning, web application scanning, vulnerability scanning, service scanning,* hingga *network scanning*.

3. *Exploitation*

   Exploitation merupakan tahapan ketiga setelah fase *scanning*. Fase ini bertujuan untuk melakukan eksploitasi kerentanan yang telah diidentifikasi pada target yang diuji sebelumnya. Tujuan utamanya ialah untuk membuktikan bahwa kerentanan yang ditemukan pada fase *scanning* benar dapat dieksploitasi. Selain itu, pada fase ini dapat dilakukan identifikasi potensi dampak yang ditimbulkan terhadap sistem atau aplikasi dari serangan tersebut.

4. *Maintainning Access*

   Maintainning Access merupakan tahapan keempat setelah fase *exploitation*. Setelah berhasil melakukan eksploitasi pada sistem atau aplikasi, maka terdapat beberapa upaya yang dapat dilakukan untuk mempertahankan akses atau memperluas kontrol untuk waktu yang lama. Tujuan dari mempertahankan akses ini ialah untuk memperoleh akses yang berkelanjutan, melakukan penyusupan jangka panjang, hingga menciptakan jalan atau pintu masuk alternatif.

5. *Reporting*

   Reporting merupakan tahapan terakhir dalam proses pengujian kerentanan OWASP. Pada fase ini, akan diperoleh hasil pengujian kerentanan yang didapat pada fase sebelumnya untuk dilakukan analisis dan diimplementasikan dalam bentuk laporan yang komperhensif sehingga dapat memberikan informasi berguna yang dapat dipahami oleh pemilik sistem atau aplikasi yang diuji, sehingga dapat membantu untuk meningkatkan keamanan sistem atau aplikasi. Laporan ini dapat dijadikan sebagai bukti atau dokumentasi yang berguna bagi pemilik sistem atau aplikasi untuk menentukan langkah selanjutnya yang harus diambil, dimana laporan ini menyajikan informasi gambaran lengkap mengenai nama kerentanan, level kerentanan, deskripsi kerentanan, potensi resiko, hingga rekomendasi perbaikan dari kelemahan yang ditemukan.

1.7 Sistematika Penulisan

Sebagai acuan agar penulisan skripsi dapat tersusun secara sistematis dan sesuai dengan harapan, serta memberikan gambaran umum terkait penulisan penelitian maka berikut sistematika penulisan dalam penelitian ini:

BAB 1 PENDAHULUAN

Pada bab ini, berisikan uraian secara umum terkait latar belakang masalah, identifikasi masalah, maksud dan tujuan, batasan masalah, metodologi penelitian, serta sistematika penulisan penelitian yang dilakukan.

BAB 2 TINJAUAN PUSTAKA

Pada bab ini, berisikan tinjauan umum mengenai berbagai teori pendukung serta konsep dasar mengenai aplikasi yang dibangun.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini, berisikan pemaparan terkait dengan analisis sistem yang terdiri dari analisis masalah, analisis sistem yang sedang berjalan, analisis data, analisis solusi yang diusulkan, analisis aplikasi sejenis, analisis sistem yang dibangun, analisis teknologi yang digunakan, analisis kebutuhan *nonfungsional*, dan analisis kebutuhan *fungsional*. Hasil dari analisis akan digunakan sebagai acuan perancangan perangkat lunak yang terdiri dari perancangan struktur menu, perancangan antarmuka, perancangan pesan, dan perancangan jaringan semantik.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini, berisikan hasil implementasi analisis yang didapat dari BAB 3 dan pembangunan aplikasi yang telah dilakukan, serta hasil pengujian aplikasi untuk mengetahui apakah sistem keamanan yang dibangun sudah sesuai dan memenuhi kebutuhan.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini, berisikan kesimpulan yang diperoleh dari hasil penelitian dan saran untuk pengembangan aplikasi di masa mendatang.