Perancangan Aplikasi Kasir Berbasis Web Menggunakan Pendekatan Metode S-SDLC (Studi Kasus :Toko Aldy Jaya)

Aldy Irfansyah[1], Elvi Rahmi[2]
Politeknik Negeri Bengkalis
cdraldyptra@gmail.com[1], elvirahmi@polbeng.ac.id[2]

Abstract

The manual management of transactions and inventory poses challenges for traditional stores, including Aldy Jaya Store, which often faces issues such as recording errors, service delays, and the lack of real-time stock information. This study develops a web-based cashier application using the Secure Software Development Life Cycle (S-SDLC) approach to address these problems. The S-SDLC method ensures security integration at every stage of development from requirement analysis, design, development, testing, to deployment and maintenance. The application is built with the Laravel framework and MySQL database, while OWASP ZAP is utilized to detect vulnerabilities. SSL/TLS-supported hosting is implemented to secure data communication between users and the server. The results show that the web-based cashier application improves operational efficiency, reduces human errors, and provides accurate sales reports. The application facilitates better transaction and inventory management while ensuring data security and operational continuity. Regular security audits and user training are recommended to maintain optimal performance and address emerging security threats effectively.

Keywords : Design, Cashier Application, S-SDLC Method Approach

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini sangat memudahkan para pengusaha dalam memperoleh informasi yang terkini dan terbuka. Oleh karena itu, banyak pengusaha yang memanfaatkan teknologi informasi. Salah satu aspek yang memerlukan dukungan teknologi komputer adalah komputerisasi penjualan dan pelaporan produk (Pangestu and Astutik, 2024).

Toko Aldy Jaya merupakan salah satu toko penjual perlengkapan, yang mana menjual perlengkapan pancing, perlengkapan ikan dan perlengkapan burung. Namun, toko ini pencatatan hanya pada teransaksi pelanggan, dengan cara mencatat di buku dan perhitungan total harga cuma bergantung pada kalkulator sehingga pelayanan tidak maksimal dan terkadang saat toko dalam keadaan rame teransaksi tidak tercatat. Sehingga kondisi ini memiliki kelemahan antara lain kesalahan saat mencatat, perhitungan total harga yang masih manual, kesulitan saat mencari laporan penjualan, dan tidak adanya informasi khusus yang menginformasikan tentang stok barang hal ini membuat pemilik toko sering kehabisan stok tanpa bisa melihatnya sehingga mengecewakan pelanggan.

Aplikasi kasir merupakan aplikasi yang biasa digunakan pada bisnis untuk mengelola transaksi dan keuangan. Aplikasi ini memiliki keunggulan dalam mempercepat dan mempermudah proses penjualan pengelolaan inventaris serta menghasilkan laporan keuangan yang akurat. Penggunaan aplikasi mesin kasir diharapkan dapat meminimalisir terjadinya *human error*, mempersingkat waktu dalam menyelesaikan banyak transaksi penjualan, dan memberikan pelaporan yang efektif dan efisien (Nuryamin and Risyda, 2021).

Dari masalah tersebut sangat diperlukan aplikasi kasir berbasis web yang berguna untuk mencatat setiap transaksi penjualan maupun pembelian dan dapat memantau stok barang yang

tersedia, sehingga memudahkan dalam pelaporan. yang dimana dalam perancangan aplikasi kasir ini menggunakan metode *Secure Software Development Life* (SSDLC).

2. TINJAUAN PUSTAKA

Penelitian dengan judul Perancangan Aplikasi Kasir Berbasis Website Pada Toko Sembako Menggunakan Metode Waterfall yang mana permasalahannya adalah pada checkout toko kelontong sampai sekarang pakai metode manual saat memasukkan informasi pada pencatatan transaksi dan pencarian informasi harus mendata dengan catatan yang cukup banyak dan juga Belum tersedia cara untuk mencari info stok persediaan, jadi sering pemilik toko mengetahui ketika proses transaksi mengalami masalah yang membuat pelanggan kecewa, sehingga ditemukan solusi dengan adanya sistem penjualan kasir dengan basis website/web dimana dapat memudahkan olah statistik data informasi yang nantinya akan dilakukan oleh pelayan kasir. Metode yang dipakai merupakan metode waterfall, yang didalam produksi mesin kasir dimulai tahapan analisa, perancangan aplikasi, implementasi pengkodean, pengujian aplikasi, evaluasi kesalahan dan pengembangan (Ihza dkk., 2023).

Penelitian dengan judul Implementasi Aplikasi Kasir Berbasis Web Pada Toko Ghafya Fruits Shop yang mana permasalahannya adalah setiap harinya petugas toko harus mencatat banyak transaksi penjualan secara manual dan harga seiring waktu sering berubah sehingga petugas tidak hafal semua harga buah, menyebabkan konsumen merasa tidak nyaman karena harus menunggu lama untuk melakukan transaksi, sehingga ditemukan solusi dengan membuat aplikasi kasir berbasis, yang memberi kemudahan untuk pemilik toko dan petugas dalam melakukan transaksi penjualan serta laporan penjualan dan aplikasi ini dibuat menggunakan bahasa pemrograman PHP dengan database MySQL untuk menyimpan datanya (Pakusadewa dan Chotijah, 2023).

2.1 Kasir

Aplikasi kasir merupakan aplikasi yang biasa digunakan pada bisnis untuk mengelola transaksi dan keuangan. Aplikasi ini memiliki keunggulan dalam mempercepat dan mempermudah proses penjualan pengelolaan inventaris serta menghasilkan laporan keuangan yang akurat. Penggunaan aplikasi mesin kasir diharapkan dapat meminimalisir terjadinya human error, mempersingkat waktu dalam menyelesaikan banyak transaksi penjualan, dan memberikan pelaporan yang efektif dan efisien (Nuryamin and Risyda, 2021).

2.2 Website

Website adalah salah satu sumber daya teknologi yang paling cepat berkembang. Informasi web kini lebih terbatas dan mudah didistribusikan, memungkinkan teks, gambar, atau objek lain dijadikan sebagai referensi dasar untuk membuka halaman Web lain. Hal ini tentunya perlu dipertimbangkan secara matang oleh organisasi bisnis dengan menerapkan sumber daya teknologi yang sedang dikembangkan yaitu teknologi berbasis web. Adanya teknologi berbasis website ini menjadi salah satu alternatif yang dapat diterapkan pada organisasi bisnis (Wibowo and Ulum, 2023).

2.3 Perancangan

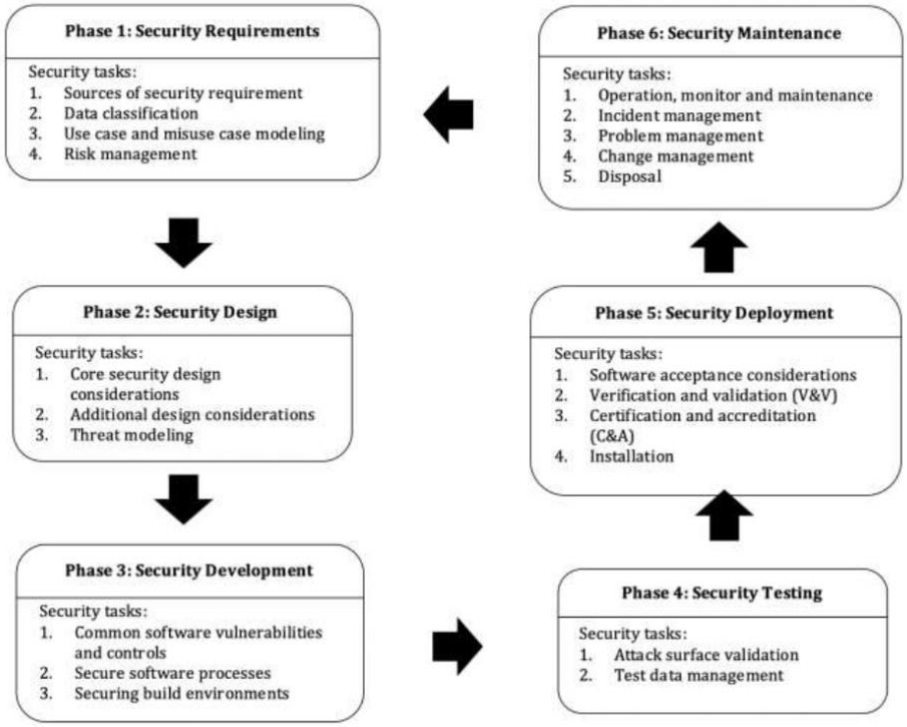
Perancangan merupakan suatu proses pemecahan masalah yang memerlukan pemikiran kreatif untuk mencapai hasil yang maksimal. Definisi bahasa Inggris dari "desain" adalah "perancangan dan manajemen yang lebih baik." Hal ini juga mengacu pada persiapan atau penyesuaian tindakan untuk mencapai hasil yang lebih baik (Purnama dkk., 2023).

2.4 Metode S-SDLC (*Secure Software Development Life Cycle*)

S-SDLC adalah konsep metodologis yang termasuk dalam *Software Development Life Cycle*, yang didalamnya melakukan analysis, design, implementation (building), testing, dan evaluation (*deployment dan maintenance*). S-SDLC berfokus pada pengintegrasian keamanan ke dalam siklus hidup pengembangan perangkat lunak. Mencapai perangkat lunak yang aman tidaklah mudah, namun kita tahu bahwa meningkatkan proses pengembangan perangkat lunak dapat meminimalkan jumlah kerentanan dalam pengembangan perangkat lunak. Namun, proses S-SDLC mencakup banyak praktik dan aktivitas keamanan untuk mencapai tujuan keamanan. Menerapkan langkah-langkah ini dengan benar untuk meningkatkan keamanan perangkat lunak merupakan masalah penting (Hasan dkk., 2021).

3. METODE PENELITIAN

Metode yang digunakan dalam menganalisis sistem yaitu *Secure Software Development Life Cycle* (S-SDLC). Proses S-SDLC adalah proses SDLC yang ditambah dengan berbagai praktik keamanan atau aktivitas seperti bahasa spesifikasi keamanan, proses rekayasa persyaratan keamanan, aman bahasa spesifikasi desain, kumpulan pedoman desain yang aman, pola desain yang aman, pengkodean yang aman dan metode jaminan keamanan perangkat lunak (misalnya, pengujian penetrasi, analisis statis untuk keamanan, dan tinjauan kode untuk keamanan) (Fujdiak dkk., 2019).



Gambar 1. Siklus S-SDLC

1. Security Requirements (Persyaratan keamanan)

Tahapan ini melakukan identifikasi dan menentukan persyaratan keamanan yang relevan bagi perangkat lunak yang dikembangkan, perlu dilakukan persiapan keamanan yang matang. Persiapan ini meliputi identifikasi kebutuhan perlindungan dengan menggunakan klasifikasi data, pemodelan kasus penggunaan dan penyalahgunaan, serta manajemen risiko. Terdapat empat jenis tugas pengamanan yaitu, sumber kebutuhan pengamanan, klasifikasi data, pemodelan use case dan misuse case, manajemen risiko.

a. Sumber persyaratan keamanan

Untuk secara jelas menetapkan dan menangani tujuan atau target keamanan organisasi. Ini melibatkan pengidentifikasian persyaratan yang relevan untuk konteks bisnis dan fungsi perangkat lunak yang digunakan dalam konteks tersebut.

b. Klasifikasi data

Bertujuan untuk memastikan bahwa data atau informasi yang dianggap sebagai aset digital paling berharga dan akan mendapatkan perlindungan yang sesuai.

c. Pemodelan use case dan misuse case

Untuk mengidentifikasi kemungkinan perilaku buruk dan merekomendasikan persyaratan keamanan yang relevan berdasarkan fungsionalitas perangkat lunak yang dikembangkan.

d. Manajemen risiko

Untuk melindungi perangkat lunak yang menyimpan, memproses, atau mengirimkan informasi organisasi. Ini membantu manajemen dalam membuat keputusan yang tepat tentang alokasi anggaran untuk perangkat lunak, berdasarkan evaluasi risiko yang dilakukan. Ini juga mendukung proses otorisasi atau akreditasi perangkat lunak dengan menggunakan dokumentasi yang dihasilkan dari penilaian risiko.

2. Security Design (Desain keamanan)

Tahapan ini untuk merancang arsitektur yang aman, penting mempertimbangkan elemen keamanan serta memahami dan menganalisis ancaman terhadap perangkat lunak sebelum dibangun. Terdapat tiga jenis tugas keamanan yang harus dilakukan untuk mencapai tahap desain keamanan yaitu, pertimbangan desain keamanan inti, pertimbangan desain tambahan, dan pemodelan ancaman.

a. Pertimbangan desain keamanan inti

Untuk merancang perangkat lunak untuk mengatasi elemen keamanan inti kerahasiaan, integritas, ketersediaan, otentikasi, otorisasi, dan audit.

b. Pertimbangan desain tambahan

Untuk merancang perangkat lunak yang membahas pertimbangan desain lain yang diperlukan saat membangun perangkat lunak yang aman.

c. Pemodelan ancaman

Untuk mengidentifikasi, mengukur, dan mengatasi risiko keamanan yang terkait dengan perangkat lunak.

3. Security Development (Pengebangan keamanan)

Dalam mencapai fase pengembangan keamanan, penting untuk menerapkan teknologi dan aspek proses penulisan kode yang aman. Hal ini memastikan bahwa pengendalian keamanan yang ditentukan dalam persyaratan keamanan diterapkan dalam kode dan ancaman yang diidentifikasi dari pemodelan ancaman dihindari selama pengkodean. Ada tiga jenis tugas keamanan yang harus dilakukan yaitu, mengidentifikasi kerentanan dan kontrol perangkat lunak yang umum, memastikan proses perangkat lunak yang aman, serta mengamankan lingkungan pembangunan.

a. Kerentanan dan pengendalian perangkat lunak yang umum

Untuk mengidentifikasi kerentanan umum yang muncul dari kode yang tidak aman dan menerapkan kontrol keamanan dalam kode untuk melawan dan mencegah serangan dari pihak yang mencoba mengancam sistem.

b. Mengamankan proses perangkat lunak

Untuk menjamin keamanan perangkat lunak dengan melakukan proses tertentu sebagai tambahan pada penulisan kode yang aman.

c. Mengamankan lingkungan pembangunan

Untuk melindungi kode sumber agar tidak diakses oleh pihak yang tidak terkait selama tahap pengembangan, langkah-langkah keamanan seperti pengaturan akses yang ketat dan penggunaan kontrol versi yang aman sangat dianjurkan. Selain itu, penting juga untuk menjamin integritas kode sumber dengan melakukan pengujian lintas platform, pemeriksaan

kode secara berkala, dan mengimplementasikan prosedur untuk mendeteksi dan memperbaiki kerentanan yang mungkin muncul.

4. Security Testing (Pengujian keamanan)

Tahap ini digunakan untuk memvalidasi dan memverifikasi fungsionalitas serta keamanan perangkat lunak, diperlukan pengujian jaminan kualitas. Pengujian ini memastikan bahwa kode yang dikembangkan berjalan sesuai dengan yang diharapkan. Ada dua jenis tugas keamanan yang harus dilakukan untuk menyelesaikan tahap pengujian keamanan yaitu, validasi permukaan serangan dan pengujian manajemen data.

a. Validasi permukaan serangan

Untuk memverifikasi keberadaan dan efektivitas kontrol keamanan yang dirancang dan diterapkan dalam perangkat lunak.

b. Uji pengelolaan data

Untuk menentukan data yang digunakan untuk menguji input dan hasil yang seharusnya keluar setelah perangkat lunak beroperasi secara normal.

5. Security Deployment (Penerapan keamanan)

Selama fase penerapan, Untuk mencapai fase penerapan keamanan, diperlukan penyelesaian rencana operasi dan dokumentasi aplikasi. Hal ini memastikan persetujuan manajemen dan penerimaan risiko untuk penerapan, serta memastikan bahwa aplikasi memenuhi fungsinya dan aman. Lingkungan dan konfigurasi juga harus dijamin keamanannya untuk penerapan. Terdapat empat jenis tugas keamanan yang harus dilakukan: pertimbangan penerimaan perangkat lunak, verifikasi dan validasi (V&V), sertifikasi dan akreditasi (C&A), serta instalasi.

a. Pertimbangan penerimaan perangkat lunak

Untuk memastikan bahwa dokumentasi aplikasi dan rencana operasi sudah siap, serta untuk memperoleh persetujuan dan penerimaan risiko.

b. Verifikasi dan validasi (V&V)

Merupakan dua proses penting yang dilakukan untuk memastikan bahwa sebuah aplikasi atau sistem telah teruji dengan baik dan siap untuk digunakan dalam lingkungan produksi, dengan memperhatikan baik fungsionalitasnya maupun aspek keamanannya.

c. Sertifikasi dan akreditasi (K&A)

Memastikan bahwa aplikasi telah diverifikasi secara teknis dalam hal fungsionalitasnya. Hal ini penting untuk memastikan bahwa aplikasi dapat diterima secara keseluruhan dan diimplementasikan dengan sukses dalam lingkungan produksi.

d. Instalasi

Bertujuan untuk mengamankan lingkungan dan mengonfigurasi aplikasi produksi dengan benar. Hal ini penting untuk memastikan bahwa setiap komponen aplikasi berjalan sesuai dengan kebutuhan keamanan dan performa yang ditetapkan.

6. Security Maintenance (Pemeliharaan keamanan)

Untuk mencapai tahap pemeliharaan keamanan, perlu memantau dan menjamin bahwa perangkat lunak terus berfungsi dengan andal, tangguh, dan dapat dipulihkan. Selain itu, perlu mengidentifikasi kondisi di mana perangkat lunak perlu dibuang atau diganti. Terdapat lima jenis tugas pengamanan yang harus dilakukan yaitu, operasi, pemantauan dan pemeliharaan, manajemen insiden, pengelolaan masalah, manajemen perubahan, serta pembuangan.

a. Pengoperasian, pemantauan dan pemeliharaan

Untuk memberikan layanan kepada bisnis atau pengguna akhir dalam pengoperasian dan pemeliharaan perangkat lunak, perlu memastikan aspek jaminan pemrosesan yang andal, tangguh, dan dapat dipulihkan.

b. Manajemen insiden

Untuk mendeteksi dan memantau kejadian pelanggaran keamanan guna meminimalkan dampak dan mencegah insiden serupa di masa mendatang.

c. Manajemen masalah

Untuk menentukan dan menghilangkan akar penyebab masalah (insiden yang tidak diketahui) dan untuk meningkatkan layanan yang diberikan perangkat lunak kepada bisnis agar hal tersebut tidak terulang kembali.

d. Manajemen perubahan

Untuk menentukan pemulihan dan penyelesaian masalah setelah akar permasalahan teridentifikasi, penting untuk melacak kerentanan dan memantau penyelesaian masalah. Hal ini memastikan efektivitas solusi dan mencegah terulangnya masalah yang sama.

e. Pembuangan

Untuk mengidentifikasi perangkat lunak yang tidak berfungsi dengan baik agar dapat dibuang, sehingga dapat mengurangi risiko keamanan yang diakibatkan oleh keberadaan perangkat lunak yang tidak aktif atau tidak terpakai.

4. HASIL PENELITIAN DAN PEMBAHASAN

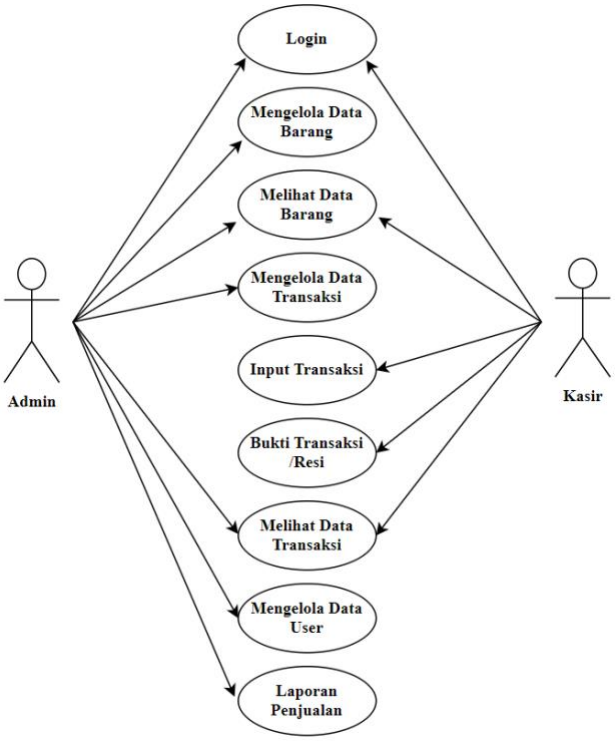
Perancangan aplikasi kasir berbasis web menggunakan pendekatan metode S-SDLC dengan tahapan sebagai berikut:

4.1 Security Requirements

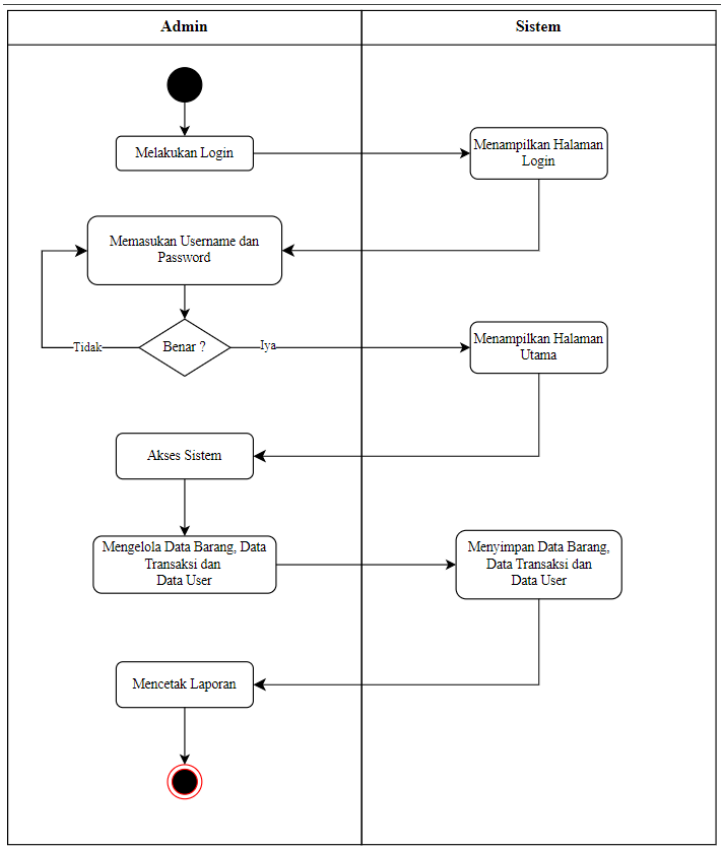
Data classification (Klasifikasi data) merupakan salah satu keamanan yang ada pada tahapan security requirements. Langkah pertama dalam merancang aplikasi kasir berbasis web adalah mengidentifikasi dan menentukan persyaratan keamanan yang relevan, terutama mengenai data barang (nama,harga,stok), data transaksi (tanggal, harga barang, total harga), dan data pengguna (username, password, peran).

4.2 Security Design

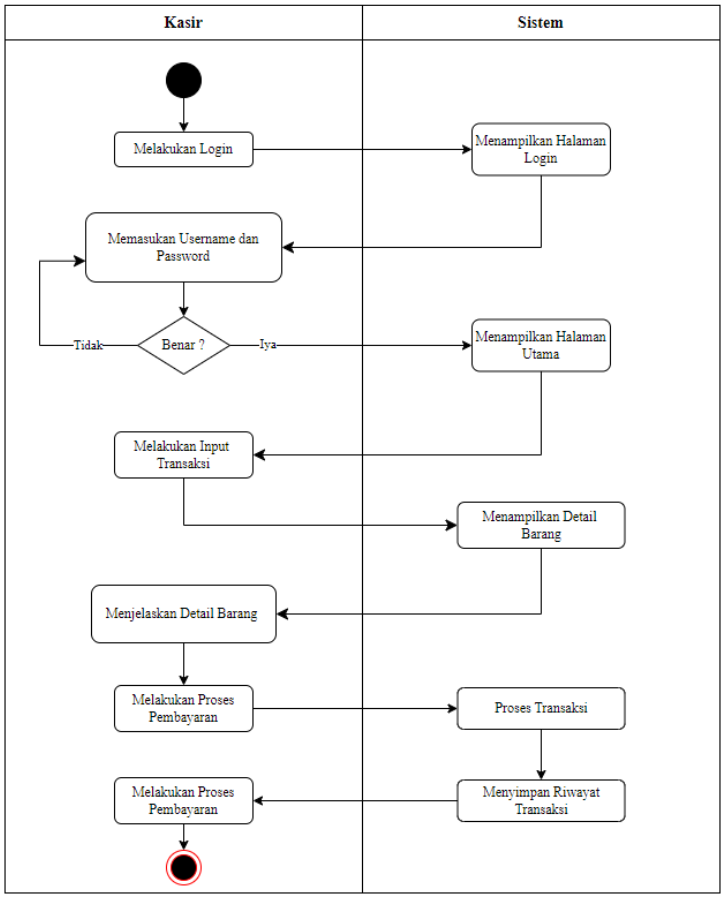
Tahapan pertama ini membuat desain atau ide tampilan untuk website yang akan dirancang. Core security design considerations (pertimbangan desain keamanan inti), merupakan salah satu keamanan yang ada pada security design. Tahapan ini menggunakan Github untuk membantu dalam manajemen kode tetapi juga menyediakan hash untuk setiap commit, serta memastikan integritas versi kode.



Gambar 2. *Usecase* diagram



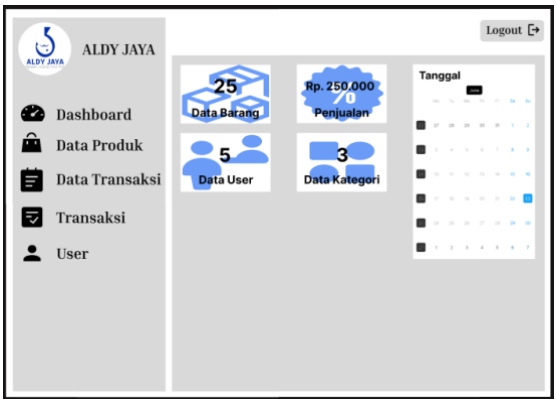
Gambar 3. *activity diagram* admin



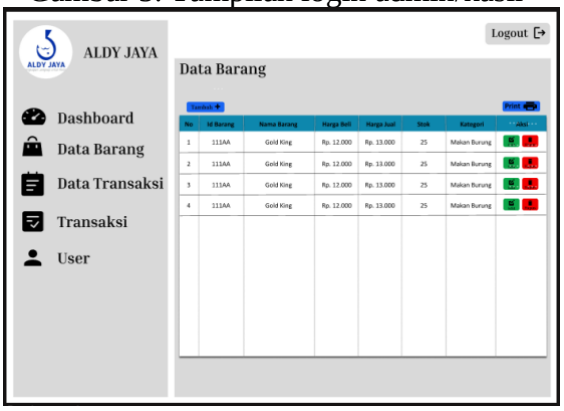
Gambar 4. *activity diagram* kasir

Tahap ini adalah membuat prototype dari website yang akan dibangun. Bertujuan untuk menetapkan desain sehingga aplikasi website lebih mudah di pemrograman. Banyak alat untuk membuat prototype, namun dipenelitian ini menggunakan tools Figma untuk melakukan perancangan jangka pendek.

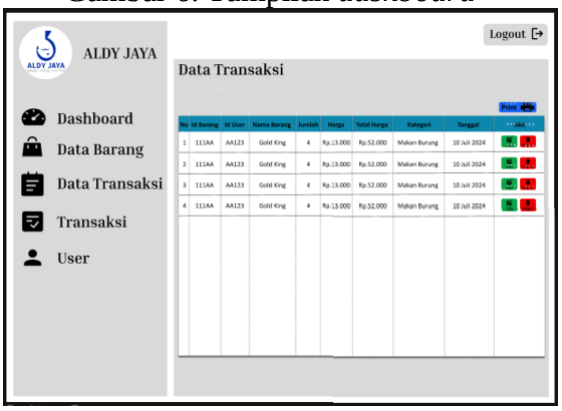
Gambar 5. Tampilan login admin/kasir



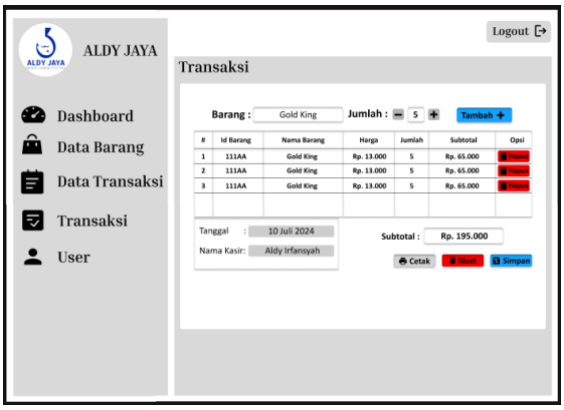
Gambar 6. Tampilan *dashboard*



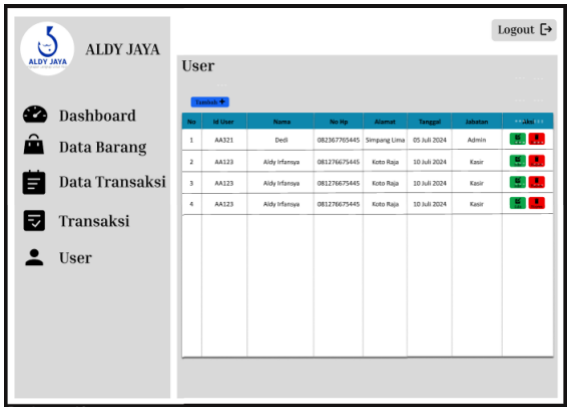
Gambar 7. Tampilan data barang



Gambar 8. Tampilan data transaksi



Gambar 9. Tampilan transaksi



Gambar 10. Tampilan user

4.3 Security Development

Dalam tahap ini, melakukan pengkodean sistem dengan bahasa pemograman PHP dengan framework Laravel dan menggunakan database MySQL. Common software vulnerabilities and controls (kerentanan dan pengendalian perangkat lunak yang umum), Tahapan ini mengidentifikasi dan mengatasi kerentanan yang sering terjadi pada pengembangan perangkat lunak seperti error pada pengkodean, tidak ada batasan hak akses dan enkripsi pada data penting. Sehingga OWASP ZAP akan digunakan untuk mengidentifikasi dan menganalisis kerentanan dalam pengkodean aplikasi web.

4.4 Security Testing

Test data management (uji pengelolaan data) merupakan salah satu tahap keamanan pada security testing, pengujian ini menggunakan teknik data dummy untuk memantau siklus hidup data pengujian, termasuk pembuatan, penggunaan, dan penghapusan. Hal ini termasuk menghapus data yang tidak diperlukan lagi dengan benar untuk menghindari risiko kebocoran atau penyalahgunaan data. Sehingga, perlu menyusun laporan yang mencakup deskripsi masalah, melacak bug pengkodean, kerentanan perangkat lunak dan prioritas untuk perbaikan.

4.5 Security Deployment

Installation (instalasi), Pada tahapan ini, bagaimana perogram aplikasi kasir yang telah dibuat dan berjalan sesuai tahapan yang diinginkan, maka dilakukan hosting agar dapat dioperasikan secara online dan dapat diakases kapan dan diamanapun. Pemilihan hosting harus ada menyediakan Secure Socket Layer (SSL). Secure Socket Layer adalah cara situs web membuat koneksi aman dengan browser web pengguna. Validasi sertifikat dengan protokol Secure Socket Layer atau Transport Layer Security (SSL/TLS) sangat penting untuk keamanan Internet. Secured Socket Layer sering digunakan untuk autentikasi karena dapat melindungi komunikasi antar pihak saat transmisi data terenkripsi antara web browser dan server.

4.6 Security Maintenance

Tahapan ini, untuk melakukan pemantauan dan menjamin bahwa aplikasi kasir sudah berfungsi dengan baik dan dapat dipulihkan saat ada yang bermasalah. Problem management (manajemen masalah) merupakan salah satu keamanan yang ada pada security maintenance. Dalam pembangunan aplikasi, baik itu aplikasi kasir tidak jauh dari permasalahan paling sering terjadi adalah bug atau error pada pengkodean program maupun data tidak tersimpan ke database. Maka dari itu, perlu dilakukan tindakan yang tepat dalam menangani masalah ini dengan selalu memantau dan memperbaiki masalah yang akan muncul. Sehingga perlunya pelaporan dan pencatatan sehingga ada masalah yang serupa mudah dalam mengatasinya. Dengan menggunakan GitHub untuk melaporkan dan melacak bug atau masalah terkait aplikasi kasir dan setiap issue akan didokumentasikan dengan detail dan status yang jelas.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan, perancangan aplikasi kasir berbasis web dengan metode *Secure Software Development Life Cycle* (S-SDLC) terbukti efektif dalam meningkatkan efisiensi dan keamanan dalam pengelolaan transaksi penjualan dan inventaris. Integrasi keamanan di setiap tahap pengembangan, mulai dari analisis kebutuhan, desain, pengembangan, pengujian, hingga penerapan dan pemeliharaan, memungkinkan aplikasi meminimalkan risiko kesalahan dan ancaman keamanan. Penggunaan framework Laravel dan database MySQL mendukung performa optimal, sementara alat seperti OWASP ZAP membantu dalam mengidentifikasi dan menangani kerentanan. Selain itu, penerapan hosting dengan dukungan SSL/TLS memastikan keamanan komunikasi data antara pengguna dan server, melindungi informasi penting seperti data transaksi dan akun. Manajemen masalah dan pemeliharaan melalui platform seperti GitHub juga memudahkan pelacakan dan perbaikan bug secara efektif untuk menjaga keberlanjutan operasional aplikasi.

Agar aplikasi dapat berfungsi lebih optimal, beberapa langkah lanjutan perlu dilakukan. Audit keamanan dan uji penetrasi secara berkala sangat disarankan untuk mengantisipasi ancaman baru dan menjaga aplikasi tetap aman. Selain itu, pelatihan bagi pengguna aplikasi sangat penting untuk memastikan operasional berjalan lancar dan meminimalkan risiko kesalahan. Penerapan sistem pemantauan otomatis juga akan membantu deteksi dini masalah,

sehingga perbaikan dapat segera dilakukan. Aplikasi ini juga dapat dikembangkan lebih jauh dengan integrasi sistem manajemen pelanggan (CRM) dan fitur laporan keuangan otomatis untuk mendukung analisis bisnis yang lebih mendalam.

6. DAFTAR PUSTAKA

Pangestu, S. D., & Astutik, I. R. I, 2024, Rancangan Aplikasi Kasir Toko Kelontong Berbasis Website Menggunakan Metode Waterfall, JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), Vol.9, No.1, 125-135.

Nuryamin, Y., & Risyda, F, 2024, Perancangan Aplikasi Kasir Pada Kedai Kopi Berbasis Web Menggunakan Model Waterfall, JSI (Jurnal sistem Informasi) Universitas Suryadarma, Vol.11, No.1, 191-198.

Ihza, N., Rahmawati, D., & Sukrim, S, 2023, Sistem Informasi Aplikasi Kasir Berbasis Website Dengan Menggunakan Metode Waterfall, Jurnal Ilmiah Fakultas Teknik, Vol.3, No.1, 18-26.

Pakusadewa, C. R, 2023, Perancangan Sistem Informasi Aplikasi Kasir Unit Pelayanan Jasa Toko Raya Computer Berbasis WEB, Jurnal Nasional Komputasi dan Teknologi Informasi, Vol.4, No.1, 1-9.

Wibowo, M. H., & Ulum, F, 2023, Sistem Informasi Koperasi Simpan Pinjam Berbasis Website pada PRIMKOPPABRI Bandar Lampung, Jurnal Teknologi dan Sistem Informasi, Vol.4, No.1, 22-27.

Purnama, W. C., Annas, F., Musril, H. A., & Darmawati, G, 2023, Perancangan Media Pembelajaran PAI Berbasis Android Menggunakan Kodular Kelas X di SMA N 1 IV Koto, JATI (Jurnal Mahasiswa Teknik Informatika), Vol.7, No.2, 1304-1311.

Hasan, M. R., Suhermanto, S., & Suharmanto, S, 2021, Keamanan Sistem Perangkat Lunak dengan Secure Software Development Lifecycle, Jurnal Ilmu Komputer dan Bisnis, Vol.12, No.1, 88-101.

Fujdiak, R., Mlynek, P., Mrnustik, P., Barabas, M., Blazek, P., Borcik, F., & Misurec, J, 2019, June, Managing the secure software development, In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) pp. 1-4.