Politeknik Caltex Riau

LAPORAN PROYEK AKHIR

PERANCANGAN APLIKASI PENJUALAN KARYA DIGITAL DENGAN SISTEM KEAMANAN TWO-FACTOR AUTHENTICATION (2FA)

Rima Amalia Rahmawati

NIM. 2256301028

Pembimbing

Dini Nurmalasari, S.T., M.T.

PROGRAM STUDI

TEKNOLOGI REKAYASA KOMPUTER

POLITEKNIK CALTEX RIAU

2026

LEMBAR PENGESAHAN

PERANCANGAN APLIKASI PENJUALAN KARYA DIGITAL DENGAN SISTEM KEAMANAN TWO-FACTOR AUTHENTICATION (2FA)

Rima Amalia Rahmawati

NIM. 2256301028

Proposal Proyek Akhir ini disusun untuk memenuhi salah satu persyaratan memperoleh gelar **Sarjana Terapan Teknik (S.Tr.T)** di Politeknik Caltex Riau

Pekanbaru, 3 Agustus 2026

Disetujui oleh:

Pembimbing 1	:	Dini Nurmalasari S.T., M.T. NIP. 048108	( )
Penguji 1	:	Ibnu Surya S.T., M.T. NIP. 078303	( )
Penguji 2	:	Rahmat Suhatman, S.T., M.T. NIP. 048110	( )

Mengetahui,

Ketua Program Studi Teknologi Rekayasa Komputer

Ibnu Surya S.T., M.T.

NIP. 078303

i

PERNYATAAN PENGGUNAAN KECERDASAN BUATAN

Dengan ini saya menyatakan bahwa penelitian yang berjudul:

Perancangan Aplikasi Penjualan Karya Digital dengan Distem Keamanan Two-Faktor Authentication (2FA)

Menggunakan teknologi Kecerdasan Buatan (*Artificial Intelligence*) dalam penyusunan dokumen ini sebatas pada hal-hal berikut:

(isi oleh mahasiswa sendiri sesuai penggunaan yang dilakukan)

Penggunaan tersebut **tidak menyangkut substansi utama penelitian**, seperti analisis, penyusunan ide pokok, perumusan konsep ilmiah, atau penentuan hasil penelitian. Seluruh substansi utama dalam dokumen ini merupakan hasil pemikiran dan karya saya sendiri. Apabila di kemudian hari ditemukan pelanggaran terhadap pernyataan ini, saya bersedia menerima konsekuensi sesuai ketentuan yang berlaku.

Pekanbaru, 19 Juni 2026

Yang menyatakan,

Rima amalia rahmawati

NIM. 2256301028

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa penelitian yang berjudul:

Perancangan Aplikasi Penjualan Karya Digital Dengan Sistem Keamanan Two-Factor Authentication (2FA)

Adalah benar hasil karya saya, dan tidak mengandung karya ilmiah atau tulisan yang pernah diajukan di suatu Perguruan Tinggi

Setiap kata yang dituliskan tidak mengandung plagiat, pernah ditulis maupun diterbitkan orang lain kecuali secara tertulis diacu dalam dokmen ini dan disebutkan pada daftar pustaka. Saya siap menanggung seluruh akibat apabila terbukti melakukan plagiat.

Pekanbaru, 19 Juni 2026

Yang menyatakan,

Rima amalia rahmawati

NIM. 2256301028

KESEPAKATAN PUBLIKASI

Demi pengembangan ilmu pengetahuan, dengan ini saya menyatakan:

1. Memberikan persetujuan kepada Politeknik Caltex Riau untuk menyimpan, mengolah dalam bentuk pangkalan data, merawat, mengalih media/formatkan dan mempublikasikan **Proyek Akhir** ini selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.
2. Tidak melakukan alih media/format dan publikasi dalam bentuk makalah ilmiah dari bagian atau keseluruhan **Proyek Akhir** ini ke suatu publikasi ilmiah, pada seminar ataupun jurnal, skala nasional maupun internasional, kecuali ada persetujuan dari saya dan Dosen Pembimbing Utama, dan mencantumkan nama saya, Dosen Pembimbing Utama dan nama-nama lain (jika ada) yang berkontribusi pada makalah.

Pekanbaru, 19 Juni 2026

Yang menyatakan,

Rima Amalia Rahmawati

NIM. 2256301028

KATA PENGANTAR

Segala puji syukur kehadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis **PROPOSAL PROYEK AKHIR** dapat menyelesaikan penelitian berjudul "**Perancangan Aplikasi Penjualan Karya Digital Dengan Sistem Keamanan Two-Factor Authentication (2FA)**". yang disusun sebagai salah satu syarat untuk menyelesaikan jenjang pendidikan **Sarjana Terapan** pada Program Studi **Teknologi Rekayasa Komputer** Politeknik Caltex Riau.

Penulis menyadari bahwa laporan penelitian ini masih jauh dari sempurna. Oleh karena itu, segala bentuk kritik dan saran yang bersifat membangun sangat penulis harapkan demi perbaikan di masa mendatang. Penulis berharap laporan ini dapat memberikan manfaat dan wawasan bagi para pembaca, serta menjadi bahan referensi untuk pengembangan penelitian selanjutnya.

Pekanbaru, 19 Juni 2026

Penulis

UCAPAN TERIMA KASIH

1. Bapak Dr. Dadang Syarif Sihabudin Sahid, S.Si., M.Sc. selaku Direktur Politeknik Caltex Riau yang telah mendedikasikan waktunya untuk meningkatkan perkembangan institusi Pendidikan Politeknik Caltex Riau
2. Ibu Dini Nurmalasari, S.T., M.T. selaku pembimbing dan penguji, yang telah memberikan ilmu dan bimbingan dengan penuh kesabaran kepada penulis dalam menyelesaikan penelitian.
3. Seluruh Dosen Pengajar Program Studi **Teknologi Rekayasa Komputer** Politeknik Caltex Riau yang telah memberikan bekal ilmu kepada penulis dalam menyelesaikan penelitian.
4. Kedua orang tua penulis atas dukungan dan kasih sayang tak terhingga, sehingga penulis bisa menyelesaikan penelitian tepat waktu.
5. Kepada seluruh teman teman saya yang sangat saya sayangi, yang telah mendukung saya dengan penuh sehingga saya dapat menyelesaikan penelitian.
6. Teruntuk orang orang yang selama ini selalu ada di sisi saya selama saya melakukan penelitian terutama Geon, saya sangat berterima kasih karena dukungan mereka saya bisa menyelesaikan tugas akhir tepat waktu.

ABSTRAK

Meningkatnya ancaman keamanan siber pada platform perdagangan elektronik mendorong perlunya mekanisme perlindungan akun yang lebih kuat, khususnya pada aplikasi penjualan karya digital yang melibatkan data pribadi, transaksi, dan kepemilikan produk digital. Penelitian ini bertujuan merancang dan mengembangkan aplikasi penjualan karya digital berbasis web dengan menerapkan sistem keamanan *Two-Factor Authentication* (2FA) menggunakan kode *One-Time Password* (OTP) yang dikirim melalui email sebagai lapisan autentikasi tambahan. Sistem dikembangkan menggunakan metode *Software Development Life Cycle* dengan tahapan analisis kebutuhan, perancangan, implementasi, dan pengujian. Aplikasi dibangun menggunakan *framework* Laravel dengan arsitektur *Model-View-Controller* (MVC) dan basis data MySQL. Fitur utama aplikasi meliputi registrasi dan autentikasi pengguna, pengelolaan karya digital, pencarian produk, pemesanan, pembayaran, serta pengunduhan karya digital. Keamanan sistem diterapkan melalui enkripsi kata sandi menggunakan bcrypt, pembentukan nilai hash SHA-256 untuk menjaga integritas data tertentu, pembatasan masa berlaku OTP, dan verifikasi dua tahap pada proses masuk ke dalam sistem. Pengujian dilakukan menggunakan metode *Black-Box Testing* untuk mengevaluasi kesesuaian fungsi sistem berdasarkan skenario penggunaan. Hasil pengujian menunjukkan bahwa seluruh fungsi utama aplikasi dapat berjalan sesuai dengan kebutuhan yang telah ditetapkan. Implementasi 2FA mampu memberikan lapisan perlindungan tambahan karena pengguna harus memasukkan kode OTP. Dengan demikian, aplikasi yang dikembangkan dapat mendukung proses penjualan karya digital secara terstruktur serta meningkatkan keamanan akun pengguna tanpa mengurangi kemudahan dalam melakukan transaksi digital.

Kata kunci *: e-commerce, karya digital, two-factor authentication, OTP, keamanan sistem.*

ABSTRACT

The increasing prevalence of cybersecurity threats on e-commerce platforms highlights the need for stronger account protection mechanisms, particularly in digital artwork sales applications involving personal data, transactions, and digital product ownership. This study aims to design and develop a web-based digital artwork sales application by implementing Two-Factor Authentication (2FA) using a One-Time Password (OTP) sent via email as an additional authentication layer. The system was developed using the Software Development Life Cycle method, which includes requirements analysis, system design, implementation, and testing. The application was built using the Laravel framework with the Model-View-Controller architecture and a MySQL database. Its main features include user registration and authentication, digital artwork management, product searching, ordering, payment, and digital product downloading. System security was implemented through bcrypt password hashing, SHA-256 hashing to maintain the integrity of selected data, OTP expiration limits, and two-step verification during the login process. Black-box testing was conducted to evaluate the functionality of the system based on predefined usage scenarios. The test results indicate that all major application functions operated according to the specified requirements. The implementation of 2FA provides an additional layer of protection by requiring users to enter an OTP. Therefore, the developed application can support a structured digital artwork sales process while improving user account security without compromising the convenience of digital transactions.

***Keywords** : e-commerce, digital products, two-factor authentication, OTP, system security*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah mendorong pertumbuhan pesat industri e-commerce, termasuk dalam sektor penjualan karya digital. Karya digital seperti desain grafis, ilustrasi, template, hingga produk kreatif lainnya kini semakin diminati karena kemudahan distribusi dan akses yang luas. Melalui platform digital, penjual dapat menjangkau pasar tanpa batas geografis, meningkatkan efisiensi operasional, serta memberikan kemudahan transaksi bagi konsumen. Namun, di balik berbagai kemudahan tersebut, terdapat tantangan besar yang harus dihadapi, terutama terkait dengan keamanan sistem dan perlindungan akun pengguna.

Keamanan menjadi aspek krusial dalam sistem e-commerce, khususnya pada platform yang menangani transaksi digital dan data pengguna. Ancaman seperti peretasan akun, pencurian identitas, hingga penyalahgunaan data pribadi semakin meningkat seiring berkembangnya teknologi. Banyak kasus menunjukkan bahwa lemahnya sistem keamanan dapat menyebabkan kerugian baik bagi pengguna maupun pengelola platform. Oleh karena itu, diperlukan mekanisme perlindungan yang lebih kuat untuk menjaga integritas data serta kepercayaan pengguna terhadap sistem.

Berbagai kasus penipuan digital di Indonesia memperkuat urgensi permasalahan tersebut. Otoritas Jasa Keuangan (OJK) mencatat sebanyak 2.688 kasus pengambilalihan akun atau *Account Take Over* (ATO) sepanjang Januari 2024 hingga Januari 2025, di mana pelaku umumnya mengelabui korban untuk memperoleh kata sandi dan kode OTP melalui rekayasa sosial guna menguasai akun serta melakukan transaksi tanpa izin (OJK, 2025). Bareskrim Polri juga pernah mengungkap kasus pengambilalihan akun rekening nasabah melalui penyalahgunaan kode OTP dengan total kerugian mencapai Rp21 miliar (Antara News, 2020). Selain pembajakan akun, modus penipuan turut merambah metode pembayaran berbasis kode QR. Sepanjang tahun 2022 hingga kuartal I 2024 saja, kerugian akibat penipuan digital yang memanfaatkan kode QR dilaporkan

mencapai Rp2,5 triliun dari sekitar 155.000 laporan, dengan modus *sticker swapping*, yaitu penggantian kode QRIS resmi milik pedagang dengan kode QR palsu yang mengalihkan dana pembayaran ke rekening pelaku (Diskominfo Kota Cirebon, 2026). Kasus serupa juga menimpa belasan pedagang di salah satu pujasera di Bandung pada Oktober 2025, yang baru menyadari kerugiannya setelah saldo mereka tidak bertambah meski pembeli telah melakukan pembayaran (TintaHijau.com, 2025). Kasus-kasus tersebut menunjukkan bahwa baik metode autentikasi akun maupun metode pembayaran berbasis kode QR sama-sama rentan dimanipulasi apabila tidak dikelola melalui mekanisme yang terverifikasi dan dapat dipertanggungjawabkan.

Sejumlah platform penjualan karya digital yang telah berjalan, seperti Gumroad, Etsy, Lynk.id, dan Karyakarsa, secara bertahap memperkuat sistem keamanannya seiring meningkatnya ancaman siber tersebut. Gumroad dan Etsy, misalnya, telah mewajibkan verifikasi dua langkah baik melalui aplikasi autentikator maupun kode OTP untuk melindungi akun penjual dari pengambilalihan, sementara penyedia pembayaran yang terintegrasi pada platform seperti Lynk.id dan Karyakarsa turut menambahkan verifikasi tambahan pada proses *checkout* untuk mencegah transaksi yang tidak sah. Hal ini juga didukung oleh beberapa penelitian terkini. Islamey & Sutopo (2024) merancang sistem 2FA pada aplikasi e-commerce melalui kombinasi kata sandi dan kode OTP untuk memperkuat proses login, sedangkan Qadriah dkk. (2023) mengembangkan pengamanan berbasis algoritma *Time-Based One Time Password* (TOTP) yang menghasilkan kode verifikasi dinamis berbasis waktu, sebagai alternatif yang lebih sulit disadap dibandingkan OTP statis melalui email. Khan dkk. (2023) menegaskan bahwa faktor autentikasi memegang peranan penting dalam keamanan transaksi *fintech* berbasis mobile, sementara Melo dkk. (2024) memperkenalkan pendekatan *out-of-band* dengan otorisasi visual dua faktor pada transaksi e-banking yang relevan sebagai rujukan dalam merancang verifikasi pembayaran berbasis kode QR yang lebih aman. Selain itu, Kružíková dkk. (2024) menemukan bahwa efisiensi waktu dan tingkat kepuasan pengguna terhadap proses 2FA turut memengaruhi persepsi keamanan dan kenyamanan secara keseluruhan, sehingga perancangan

2FA pada penelitian ini juga perlu memperhatikan keseimbangan antara keamanan dan pengalaman pengguna.

Salah satu pendekatan yang dapat digunakan untuk meningkatkan keamanan adalah dengan menerapkan sistem *Two-Factor Authentication* (2FA). Metode ini menambahkan lapisan keamanan tambahan dengan mengharuskan pengguna untuk melakukan verifikasi melalui dua tahap, seperti kombinasi kata sandi dan kode verifikasi yang dikirim ke perangkat pribadi pengguna. Dengan adanya 2FA, risiko akses tidak sah terhadap akun dapat diminimalkan, sehingga keamanan data dan transaksi menjadi lebih terjamin.

Berdasarkan penelitian yang telah dilakukan sebelumnya, penerapan sistem autentikasi ganda terbukti efektif dalam mengurangi potensi serangan siber, terutama yang berkaitan dengan pencurian akun dan akses ilegal. Implementasi 2FA tidak hanya meningkatkan keamanan, tetapi juga memberikan rasa aman bagi pengguna dalam melakukan aktivitas transaksi digital. Hal ini menjadi penting dalam membangun kepercayaan pengguna serta menjaga keberlangsungan sistem *e-commerce* dalam jangka panjang.

Perancangan aplikasi penjualan karya digital menjadi langkah strategis untuk mendukung para kreator dalam memasarkan produknya secara mandiri. Dengan memiliki platform sendiri, penjual dapat mengelola produk, transaksi, serta interaksi dengan pelanggan secara lebih optimal tanpa bergantung sepenuhnya pada pihak ketiga. Selain itu, integrasi sistem keamanan seperti *Two-Factor Authentication* menjadi nilai tambah yang dapat meningkatkan kredibilitas aplikasi serta memberikan perlindungan ekstra bagi pengguna.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk merancang dan mengembangkan aplikasi penjualan karya digital dengan penerapan sistem keamanan Two-Factor Authentication yang tidak hanya diterapkan pada proses login, tetapi juga pada proses verifikasi pembayaran, mengingat kedua titik tersebut sama-sama berpotensi disalahgunakan sebagaimana ditunjukkan oleh berbagai kasus penipuan yang telah dipaparkan. Pada proses pembayaran, kode QR yang digunakan sebagai sarana verifikasi transaksi dihasilkan dan divalidasi oleh penyedia layanan pembayaran pihak

ketiga (payment gateway), bukan dibuat sendiri oleh sistem aplikasi, sehingga keaslian dan keamanan setiap kode QR pembayaran tetap dapat dipertanggungjawabkan dan tidak mudah dipalsukan. Diharapkan, aplikasi yang dikembangkan tidak hanya mampu memfasilitasi proses transaksi secara efisien, tetapi juga memberikan tingkat keamanan yang tinggi pada kedua titik tersebut, sehingga dapat meningkatkan kepercayaan pengguna serta mendukung pertumbuhan bisnis digital yang lebih aman dan berkelanjutan. Oleh karena itu, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam pengembangan sistem e-commerce yang inovatif, aman, dan terpercaya.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana merancang dan membangun aplikasi penjualan karya digital yang efektif dan mudah digunakan oleh pengguna?
2. Bagaimana mengimplementasikan sistem keamanan Two-Factor Authentication (2FA) pada aplikasi penjualan karya digital untuk meningkatkan perlindungan akun pengguna?
3. Apa saja faktor yang mempengaruhi stabilitas keamanan
4. Bagaimana menerapkan Two-Factor Authentication (2FA) pada proses verifikasi pembayaran dengan kode QR dari pihak ketiga (payment gateway), agar transaksi pembelian karya digital lebih terlindungi dari pemalsuan atau penyalahgunaan kode QR?

1.3 Batasan Masalah

Agar ruang lingkup penelitian tidak terlalu luas, batasan masalah yang diterapkan adalah sebagai berikut:

1. Aplikasi yang dikembangkan difokuskan pada penjualan karya digital berbasis web, dengan fitur utama seperti registrasi, login, pengelolaan produk, dan transaksi pembelian.
2. Sistem keamanan yang diterapkan dibatasi pada penggunaan Two-Factor Authentication (2FA) sebagai metode autentikasi tambahan, baik pada proses

login pengguna maupun pada proses verifikasi pembayaran transaksi pembelian karya digital.

3. Implementasi 2FA pada proses login menggunakan mekanisme pengiriman kode OTP (One-Time Password) melalui email sebagai tahap verifikasi kedua.
4. Implementasi 2FA pada proses pembayaran menggunakan kode QR yang dihasilkan dan divalidasi oleh penyedia layanan pembayaran pihak ketiga (payment gateway), sehingga sistem aplikasi yang dikembangkan tidak membuat atau mengelola kode QR pembayaran secara mandiri.
5. Penelitian ini berfokus pada fungsionalitas sistem serta keseimbangan antara keamanan, kemudahan penggunaan, dan efisiensi pada proses login maupun pembayaran, tanpa membahas pengujian keamanan tingkat lanjut (seperti penetration testing) atau pengembangan sistem payment gateway secara mandiri.
6. Karya digital yang dapat diperjual belikan pada aplikasi dibatasi pada kategori Ilustrasi, Cover Buku, Character Design, UI Kit, Font & Tipografi, dan Template Sosmed, sesuai dengan kategori yang telah tersedia pada aplikasi.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan pada penelitian ini bertujuan untuk Mengembangkan sistem informasi e-commerce yang aman dengan menerapkan 2FA untuk melindungi data pengguna. Memastikan bahwa informasi pelanggan, seperti data pribadi dan riwayat transaksi, tidak dapat diakses oleh pihak yang tidak berwenang. Meningkatkan kepercayaan pelanggan terhadap sistem e-commerce yang dikembangkan dengan memberikan perlindungan data yang lebih baik. Melakukan analisis untuk mengetahui factor apa saja yang mempengaruhi stabilitas keamanan system penjualan karya digital.

1.4.2 Manfaat

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan solusi keamanan pada aplikasi penjualan karya digital melalui penerapan Two-Factor Authentication (2FA), sehingga dapat mengurangi risiko peretasan dan akses tidak sah terhadap akun pengguna.
2. Menyediakan platform penjualan karya digital yang lebih aman dan terpercaya, sehingga dapat meningkatkan kepercayaan pengguna dalam melakukan transaksi jual beli karya digital.
3. Mendukung proses transaksi karya digital yang tetap efisien dan mudah digunakan, dengan tetap menjaga keamanan data serta kenyamanan pengguna.
4. Menjadi acuan dalam pengembangan aplikasi penjualan karya digital berbasis web dengan sistem keamanan autentikasi ganda yang lebih optimal dan terstruktur.

BAB 2
TINJAUAN PUSTAKA

2.1 Landasan Teori

Berikut merupakan landasan teori terkait perancangan dan pengembangan sistem e-commerce yang digunakan sebagai dasar acuan dalam penelitian ini. Teori-teori yang dipaparkan mencakup berbagai konsep dan definisi yang berkaitan langsung dengan sistem yang akan dibangun, sehingga dapat memberikan pemahaman yang lebih mendalam mengenai topik yang dibahas. Pemaparan landasan teori ini diharapkan dapat menjadi pedoman yang kuat dalam proses analisis, perancangan, serta implementasi sistem secara keseluruhan.

2.1.1 E-Commerce

E-Commerce (Electronic Commerce) merupakan aktivitas jual beli barang dan jasa yang dilakukan secara elektronik melalui jaringan internet. Menurut Laudon & Traver (2019), e-commerce adalah penggunaan internet dan web untuk melakukan transaksi bisnis. Lebih lanjut, e-commerce mencakup seluruh proses transaksi mulai dari pencarian informasi produk, pemesanan, pembayaran, hingga pengiriman barang yang semuanya dilakukan secara digital.

E-commerce memiliki beberapa jenis model bisnis, di antaranya *Business-to-Consumer* (B2C) yaitu transaksi antara pelaku usaha dengan konsumen akhir, *Business-to-Business* (B2B) yaitu transaksi antar pelaku usaha, serta *Consumer-to-Consumer* (C2C) yaitu transaksi antar sesama konsumen melalui platform perantara. Dalam konteks penelitian ini, aplikasi penjualan karya digital yang dikembangkan termasuk dalam kategori C2C dan B2C, di mana kreator digital menjual karyanya langsung kepada konsumen melalui platform yang disediakan.

Keunggulan utama *e-commerce* meliputi kemudahan akses tanpa batas geografis, efisiensi waktu dan biaya operasional, serta kemampuan untuk menjangkau pasar yang lebih luas dibandingkan toko konvensional. Namun, e-commerce juga menghadapi berbagai tantangan, terutama terkait keamanan data pengguna dan kepercayaan konsumen dalam melakukan transaksi secara online (Turban et al., 2018).

2.1.2 Keamanan Transaksi E-Commerce

Keamanan transaksi e-commerce merupakan aspek fundamental yang harus diperhatikan dalam setiap sistem perdagangan elektronik. Keamanan dalam konteks ini mencakup perlindungan terhadap data pribadi pengguna, integritas informasi transaksi, kerahasiaan data keuangan, serta ketersediaan layanan sistem. Menurut Stallings (2017), terdapat tiga prinsip utama keamanan informasi yang sering disebut sebagai *CIA Triad*, yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan).

Ancaman keamanan yang umum terjadi pada sistem e-commerce antara lain phishing, pencurian identitas (identity theft), serangan man-in-the-middle, serta peretasan akun pengguna. Phishing merupakan teknik penipuan yang dilakukan dengan cara menyamar sebagai entitas terpercaya untuk mencuri informasi sensitif pengguna, seperti kata sandi dan data kartu kredit. Serangan-serangan tersebut dapat menyebabkan kerugian finansial dan hilangnya kepercayaan pengguna terhadap platform *e-commerce* (Putra et al., 2024).

Untuk mengatasi berbagai ancaman tersebut, diperlukan penerapan mekanisme keamanan yang berlapis pada sistem e-commerce. Beberapa mekanisme yang umum digunakan antara lain enkripsi data menggunakan algoritma seperti AES (*Advanced Encryption Standard*) atau SSL/TLS, penggunaan protokol HTTPS untuk komunikasi yang aman, serta penerapan sistem autentikasi berlapis seperti *Two-Factor Authentication* (2FA). Kombinasi berbagai mekanisme keamanan ini bertujuan untuk menciptakan sistem yang dapat melindungi pengguna dari berbagai ancaman siber sekaligus mempertahankan kenyamanan dalam bertransaksi.

2.1.3 Two-Factor Authentication

Two-Factor Authentication (2FA) adalah metode autentikasi keamanan yang mengharuskan pengguna untuk memverifikasi identitasnya melalui dua tahap yang berbeda sebelum dapat mengakses sebuah sistem atau akun. Metode ini didasarkan pada kombinasi dua dari tiga faktor autentikasi, yaitu sesuatu yang diketahui pengguna (*something you know*) seperti kata sandi, sesuatu yang dimiliki pengguna (*something you have*) seperti perangkat mobile atau token, dan sesuatu yang

melekat pada pengguna (something you are) seperti sidik jari atau pengenalan wajah (NIST, 2017).

Salah satu implementasi 2FA yang paling umum digunakan adalah pengiriman kode OTP (*One-Time Password*) melalui email atau SMS. OTP merupakan kode verifikasi yang hanya berlaku satu kali dan memiliki masa berlaku terbatas, biasanya antara 5 hingga 10 menit. Cara kerja 2FA dengan OTP adalah sebagai berikut: pertama, pengguna memasukkan nama pengguna dan kata sandi; kedua, sistem mengirimkan kode OTP ke email atau nomor telepon pengguna yang telah terdaftar; ketiga, pengguna memasukkan kode OTP tersebut untuk menyelesaikan proses login. Dengan mekanisme ini, meskipun kata sandi pengguna berhasil dicuri, pelaku kejahatan tetap tidak dapat mengakses akun tanpa kode OTP yang dikirim ke perangkat pribadi pengguna (Hapsari et al., 2020).

Penerapan 2FA telah terbukti secara signifikan meningkatkan keamanan akun pengguna. Berdasarkan penelitian Putra et al. (2024), implementasi 2FA mampu mengurangi risiko peretasan akun hingga 99,9% dibandingkan dengan penggunaan kata sandi tunggal. Dalam konteks aplikasi penjualan karya digital, penerapan 2FA memberikan lapisan perlindungan tambahan yang sangat penting, terutama untuk melindungi data transaksi dan karya digital milik pengguna dari akses tidak sah.

2.1.4 Framework Pengembangan Sistem E-Commerce

Framework merupakan kerangka kerja atau struktur dasar yang digunakan sebagai fondasi dalam pengembangan perangkat lunak. Penggunaan framework dalam pengembangan sistem e-commerce bertujuan untuk mempercepat proses pengembangan, meningkatkan kualitas kode, serta memastikan konsistensi dan keamanan sistem. Framework menyediakan berbagai komponen yang telah teruji, termasuk fitur keamanan bawaan, manajemen sesi, dan perlindungan terhadap serangan umum seperti SQL Injection dan Cross-Site Scripting (XSS).

Dalam pengembangan aplikasi penjualan karya digital ini, digunakan framework berbasis web yang mendukung arsitektur Model-View-Controller (MVC). Arsitektur MVC memisahkan logika bisnis (Model), tampilan antarmuka (View), dan pengendali alur aplikasi (Controller), sehingga kode menjadi lebih terstruktur, mudah dipelihara, dan dikembangkan lebih lanjut. Laravel merupakan

salah satu framework PHP yang banyak digunakan dalam pengembangan sistem e-commerce karena menyediakan fitur autentikasi yang lengkap, sistem routing yang fleksibel, serta dukungan terhadap berbagai mekanisme keamanan.

Selain framework back-end, pengembangan sistem e-commerce juga memanfaatkan framework front-end untuk membangun antarmuka pengguna yang responsif dan interaktif. Framework seperti Bootstrap atau Tailwind CSS digunakan untuk memastikan tampilan aplikasi dapat menyesuaikan diri dengan berbagai ukuran layar perangkat, baik desktop maupun mobile. Kombinasi framework back-end dan front-end ini memungkinkan pengembangan aplikasi yang efisien sekaligus menghasilkan produk yang berkualitas tinggi dari sisi fungsionalitas dan pengalaman pengguna

2.1.5 Database

Database atau basis data adalah kumpulan data yang terorganisir secara sistematis dan dapat diakses, dikelola, serta diperbarui secara efisien. Dalam konteks sistem e-commerce, database berfungsi sebagai tempat penyimpanan seluruh data yang diperlukan oleh sistem, meliputi data pengguna, informasi produk, riwayat transaksi, serta data keamanan seperti token autentikasi. Sistem Manajemen Basis Data (DBMS) yang banyak digunakan dalam pengembangan aplikasi web adalah MySQL dan PostgreSQL karena keduanya bersifat open-source, memiliki performa yang baik, serta mendukung fitur keamanan yang memadai (Ramakrishnan & Gehrke, 2003).

Dalam pengembangan aplikasi penjualan karya digital ini, perancangan database dilakukan dengan mempertimbangkan kebutuhan fungsional sistem serta aspek keamanan data. Normalisasi database dilakukan untuk menghilangkan redundansi data dan memastikan integritas referensial antar tabel. Selain itu, data sensitif seperti kata sandi pengguna disimpan dalam bentuk terenkripsi menggunakan algoritma hashing, sehingga meskipun database berhasil diakses secara tidak sah, data sensitif tersebut tidak dapat dibaca secara langsung.

Pengelolaan database dalam sistem e-commerce juga mencakup penanganan transaksi (transaction handling) untuk memastikan konsistensi data. Mekanisme ACID (Atomicity, Consistency, Isolation, Durability) yang didukung

oleh MySQL dan PostgreSQL menjamin bahwa setiap transaksi data berjalan secara utuh dan konsisten, bahkan dalam kondisi kegagalan sistem sekalipun. Hal ini sangat penting dalam sistem penjualan karya digital untuk memastikan bahwa setiap transaksi pembelian tercatat dengan benar dan tidak terjadi inkonsistensi data.

2.1.6 Visual Code Studio

E-Commerce Visual Studio Code (VS Code) adalah editor kode sumber (source code editor) yang dikembangkan oleh Microsoft dan dirilis secara gratis sebagai perangkat lunak open-source. VS Code mendukung berbagai bahasa pemrograman dan memiliki ekosistem ekstensi yang sangat kaya, sehingga dapat dikustomisasi sesuai kebutuhan pengembangan. Fitur-fitur utama VS Code meliputi syntax highlighting, IntelliSense (penyelesaian kode otomatis), debugging terintegrasi, kontrol versi melalui Git, serta terminal terintegrasi yang memudahkan proses pengembangan aplikasi (Microsoft, 2023).

Dalam pengembangan aplikasi penjualan karya digital ini, Visual Studio Code digunakan sebagai editor utama karena kemudahannya dalam mendukung pengembangan aplikasi web secara menyeluruh. Berbagai ekstensi yang tersedia pada VS Code, seperti PHP Intelephense untuk pengembangan PHP, Prettier untuk pemformatan kode, serta ekstensi database client untuk manajemen basis data, sangat membantu dalam meningkatkan produktivitas pengembang. Selain itu, fitur Live Share pada VS Code memungkinkan kolaborasi pengembangan secara real-time yang memudahkan koordinasi antar anggota tim.

VS Code juga terintegrasi dengan baik dengan sistem kontrol versi Git, sehingga pengelolaan kode sumber dapat dilakukan secara efisien langsung dari dalam editor. Fitur diff viewer dan branch management yang tersedia memudahkan pengembang dalam melacak perubahan kode, mengelola versi aplikasi, serta berkolaborasi dalam pengembangan proyek. Popularitas VS Code yang sangat tinggi di kalangan pengembang web menjadikannya pilihan yang tepat sebagai lingkungan pengembangan utama dalam penelitian ini.

2.2 Penelitian Terdahulu

Pada bagian ini, akan dipaparkan beberapa penelitian terdahulu yang berkaitan dengan topik penelitian ini. Hal ini bertujuan agar dapat dilakukan perbandingan antara penelitian ini dengan penelitian sebelumnya, serta pengambilan referensi yang mendukung penyusunan penelitian ini. Beberapa penelitian terdahulu tersebut adalah sebagai berikut:

1. Putra (2024), dalam penelitiannya yang berjudul *"Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study"*, menunjukkan bahwa serangan phishing terus berkembang dengan teknik yang semakin kompleks seperti spear phishing, whaling, dan smishing. Penelitian ini menemukan bahwa metode pencegahan seperti filter email, enkripsi, serta penerapan *Two-Factor Authentication* (2FA) mampu meningkatkan keamanan sistem secara signifikan. Selain itu, kesadaran pengguna menjadi faktor penting dalam mengurangi keberhasilan serangan phishing.
2. Radiansyah & Priyadi (2016), melalui penelitian berjudul "Analisis Faktor Penyebab dan Pencegahan Phishing Menggunakan Systematic Literature Review", menjelaskan bahwa rendahnya pengetahuan pengguna menjadi salah satu penyebab utama keberhasilan serangan phishing. Penelitian ini menunjukkan bahwa pencegahan dapat dilakukan melalui edukasi pengguna serta penerapan sistem keamanan tambahan seperti autentikasi berlapis.
3. Wijoyo (tahun tidak disebutkan), dalam penelitiannya tentang analisis jenis dan pencegahan phishing, membahas berbagai bentuk serangan phishing seperti email phishing, web phishing, dan smishing. Hasil penelitian menunjukkan bahwa seluruh jenis serangan tersebut bertujuan untuk memperoleh data sensitif pengguna, sehingga diperlukan sistem keamanan yang lebih kuat untuk melindungi informasi tersebut..
4. Danuri (tahun tidak disebutkan), dalam penelitian berjudul "Perkembangan Teknologi Informasi dan Dampaknya terhadap Kejahatan Siber", menjelaskan bahwa pesatnya perkembangan teknologi informasi juga meningkatkan risiko kejahatan siber, termasuk phishing. Penelitian ini menekankan pentingnya penerapan sistem keamanan yang lebih baik serta regulasi untuk melindungi data pengguna dalam lingkungan digital.

5. Penelitian oleh Yani (2016) juga menyoroti pentingnya penerapan sistem keamanan tambahan dalam mencegah serangan siber. Hasil penelitian menunjukkan bahwa penggunaan teknologi seperti Two-Factor Authentication (2FA), enkripsi, serta edukasi pengguna dapat menjadi solusi efektif dalam meningkatkan keamanan sistem informasi
6. Penelitian ini (2026), berjudul *"Perancangan Aplikasi Penjualan Karya Digital dengan Sistem Keamanan Two-Factor Authentication"*, bertujuan untuk merancang dan mengembangkan aplikasi penjualan karya digital berbasis web yang mengedepankan keamanan akun pengguna. Penelitian ini mengimplementasikan sistem Two-Factor Authentication (2FA) menggunakan metode verifikasi kode OTP untuk memberikan lapisan keamanan tambahan. Sistem dirancang agar mampu melindungi akun pengguna dari akses tidak sah tanpa mengurangi kenyamanan dan efisiensi dalam proses transaksi digital.

Dibandingkan dengan penelitian-penelitian terdahulu yang lebih banyak berfokus pada pencegahan *phishing* atau keamanan sistem secara umum, penelitian ini merancang dan mengembangkan aplikasi penjualan karya digital secara menyeluruh dengan penerapan sistem autentikasi ganda (2FA). Sistem ini tidak hanya meningkatkan keamanan akun pengguna, tetapi juga tetap mempertahankan kemudahan penggunaan dan efisiensi transaksi. Dengan pendekatan ini, penelitian ini memberikan solusi yang lebih terintegrasi dalam menjaga keamanan serta meningkatkan kepercayaan pengguna terhadap platform e-commerce.

Tabel.1 Perbandingan variabel penelitian

Kategori	Peneliti 1	Peneliti 2	Peneliti 3
Metode	Studi literatur / literature review	Systematic Literature Review (SLR)	Kajian pustaka dan analisis penerapan teknologi keamanan
Pengujian	Analisis teoritis terhadap penelitian sebelumnya	Analisis teoritis berdasarkan literatur ilmiah	Kajian teoritis tidak ada implementasi langsung
Sumber Data	Literatur dan jurnal terkait trend phishing.	Literatur ilmiah terkait phishing dan fator penyebabnya.	Referensi dan literatur keamaman sistem informasi

Kategori	Peneliti 1	Peneliti 2	Peneliti 3
Fokus keamanan	Pencegahan phishing melalui filter email, enkripsi, dan 2FA	Edukasi pengguna dan autentikasi berlapis sebagai pencegahan phishing	Penerapan 2FA, enkripsi, dan edukasi pengguna untuk keamanan sistem
Teknologi yang di usulkan	Two-Factor Authentication (2FA), enkripsi, filter email	Autentikasi berlapis, sistem edukasi keamanan pengguna	Two-Factor Authentication (2FA), enkripsi data
Hasil / kesimpulan	2FA dan enkripsi mampu meningkatkan keamanan sistem secara signifikan	Edukasi pengguna dan keamanan berlapis efektif mengurangi serangan phishing	Kombinasi 2FA dan enkripsi menjadi solusi efektif keamanan sistem informasi

Berdasarkan kajian terhadap beberapa penelitian terdahulu pada Tabel 2.1 (Politeknik Caltex Riau, 2026), diketahui bahwa penelitian-penelitian tersebut telah membahas topik yang relevan dengan penelitian ini, namun memiliki keterbatasan dari sisi implementasi Two-Factor Authentication (2FA) yang masih bersifat teoritis tanpa penerapan langsung pada sistem, cakupan pembahasan yang belum mencakup integrasi keamanan pada platform transaksi digital, maupun aspek pengujian empiris terhadap efektivitas 2FA dalam melindungi akun pengguna secara nyata.

Penelitian ini memiliki perbedaan dengan penelitian sebelumnya karena mengkaji permasalahan keamanan akun pada aplikasi penjualan karya digital berbasis web dengan mengimplementasikan sistem Two-Factor Authentication (2FA) berbasis OTP secara langsung dan menyeluruh, dengan menyesuaikan pendekatan penelitian terhadap kebutuhan dan karakteristik objek penelitian. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan aplikasi penjualan digital yang aman, praktis, dan terlindungi dari akses tidak sah dalam menjawab perumusan masalah serta melengkapi hasil-hasil penelitian yang telah ada sebelumnya..

BAB 3
METODOLOGI PENELITIAN

3.1 Proses Bisnis Sistem E-Commerce

3.1.1 Proses bisnis saat ini

Saat ini, penjualan karya digital di Indonesia umumnya dilakukan melalui dua pendekatan utama, yaitu memanfaatkan platform marketplace pihak ketiga atau menjual secara mandiri melalui media sosial. Masing-masing pendekatan memiliki alur proses yang berbeda dengan kelebihan dan keterbatasannya masing-masing.

Sebagian besar kreator digital Indonesia memanfaatkan platform marketplace seperti Shopee, Tokopedia, Etsy, Gumroad, maupun platform lokal seperti Lynk.id dan Karyakarsa untuk memasarkan dan menjual karya digital mereka. Alur prosesnya dimulai dari pendaftaran akun penjual pada platform yang dipilih, dilanjutkan dengan mengunggah produk digital beserta deskripsi, harga, dan file yang akan dijual.

Ketika pembeli melakukan pembelian, sistem marketplace secara otomatis memproses pembayaran dan mengirimkan tautan unduhan kepada pembeli. Penjual kemudian menerima pembayaran setelah dipotong komisi oleh platform, yang besarannya bervariasi antara 5% hingga 10% tergantung platform yang digunakan. Meskipun praktis, ketergantungan pada platform pihak ketiga membawa sejumlah keterbatasan. Penjual tidak memiliki kendali penuh atas data pelanggan, tampilan toko, maupun kebijakan platform yang dapat berubah sewaktu-waktu. Selain itu, persaingan yang ketat antar penjual dalam satu platform membuat produk sulit menonjol tanpa strategi promosi tambahan.

Selain marketplace, banyak kreator yang memilih menjual karya digital secara langsung melalui platform media sosial seperti Instagram, TikTok Shop, Facebook, maupun WhatsApp. Proses dimulai dari promosi produk melalui unggahan konten atau stories, kemudian calon pembeli menghubungi penjual melalui pesan langsung (Direct Message) untuk menyampaikan minat pembelian. Pembayaran dilakukan melalui transfer bank atau dompet digital seperti GoPay, OVO, atau Dana, dan penjual mengirimkan file produk secara manual setelah pembayaran dikonfirmasi.

Pendekatan ini memungkinkan penjual berinteraksi langsung dengan pelanggan dan membangun komunitas, namun sangat bergantung pada keaktifan dan ketersediaan penjual. Proses yang sepenuhnya manual menyebabkan risiko keterlambatan pengiriman, kesalahan pencatatan transaksi, serta tidak adanya sistem keamanan yang memadai untuk melindungi file produk dari penyebaran ilegal.

Dari kedua pendekatan di atas, terdapat beberapa permasalahan umum yang masih dihadapi para kreator digital. Pertama, tidak adanya platform penjualan mandiri yang terintegrasi membuat kreator bergantung sepenuhnya pada pihak ketiga dengan konsekuensi komisi dan keterbatasan kendali. Kedua, sistem keamanan akun yang umumnya hanya mengandalkan kata sandi tunggal membuat akun penjual rentan terhadap peretasan, pencurian data, dan penyalahgunaan akun. Ketiga, pengiriman file secara manual tanpa mekanisme keamanan yang ketat berpotensi menyebabkan file produk tersebar tanpa izin. Keterbatasan-keterbatasan inilah yang mendorong perlunya pengembangan platform penjualan karya digital mandiri yang dilengkapi dengan sistem keamanan autentikasi berlapis seperti Two-Factor Authentication (2FA)

3.1.2 Perancangan proses bisnis baru

Proses bisnis baru dirancang untuk menggantikan alur penjualan konvensional menjadi sistem e-commerce berbasis web yang terintegrasi dengan mekanisme keamanan Two-Factor Authentication (2FA). Berikut adalah alur proses bisnis baru yang diusulkan:

1. Registrasi Pengguna: Calon pengguna (pembeli dan penjual) mengakses halaman registrasi dan mengisi formulir pendaftaran dengan data diri seperti nama, email, dan kata sandi. Sistem akan mengirimkan email verifikasi untuk mengaktifkan akun.

2. Login dengan 2FA: Pengguna memasukkan email dan kata sandi. Jika kredensial valid, sistem mengirimkan kode OTP ke email terdaftar. Pengguna memasukkan kode OTP tersebut untuk menyelesaikan proses autentikasi dan mengakses akun.

3. Manajemen Produk (Penjual): Penjual yang telah login dapat mengakses dasbor penjual, mengunggah file karya digital, mengisi informasi produk (nama, deskripsi, kategori, harga), serta mengaktifkan atau menonaktifkan produk.

4. Pencarian dan Pembelian Produk (Pembeli): Pembeli dapat menelusuri katalog produk, melihat detail produk, dan menambahkan produk ke keranjang belanja. Setelah memilih produk, pembeli melanjutkan ke halaman checkout dan melakukan pembayaran.

5. Unduhan Produk: Setelah pembayaran dikonfirmasi, sistem secara otomatis mengirimkan tautan unduhan yang unik dan berjangka waktu kepada pembeli melalui email, serta menyediakan akses unduhan melalui halaman riwayat pembelian

3.2 Perancangan Aplikasi dan Analisis Kebutuhan

3.2.1 Functional Requirement dan Non Functional Requirement

Berdasarkan proses bisnis yang telah dirancang, berikut adalah kebutuhan fungsional sistem e-commerce seperti pada Tabel 3.1.

Tabel 3.1 Kebutuhan Fungsional

ID	Deskripsi
FR01	Sistem menyediakan fitur registrasi dan login bagi pengguna (pembeli dan penjual) dengan validasi email dan kata sandi yang aman.
FR02	Sistem mengimplementasikan Two-Factor Authentication (2FA) menggunakan kode OTP yang dikirim melalui email sebagai lapisan keamanan tambahan pada proses login.
FR03	Penjual dapat menambahkan, mengedit, dan menghapus produk karya digital beserta deskripsi, harga, dan file produk yang dijual.
FR04	Pembeli dapat melakukan pencarian produk, melihat detail produk, menambahkan ke keranjang belanja, dan menyelesaikan transaksi pembelian.
FR05	Setelah pembayaran berhasil dikonfirmasi, sistem secara otomatis menyediakan tautan unduhan file karya digital kepada pembeli.

FR06	Administrator dapat mengelola data pengguna, memantau transaksi, dan mengatur konten platform melalui dasbor administrasi.

Berdasarkan proses bisnis baru yang akan dirancang, berikut adalah kebutuhan non-fungsional sistem seperti pada Tabel 3.2.

Tabel 3.2 Kebutuhan Non Fungsional

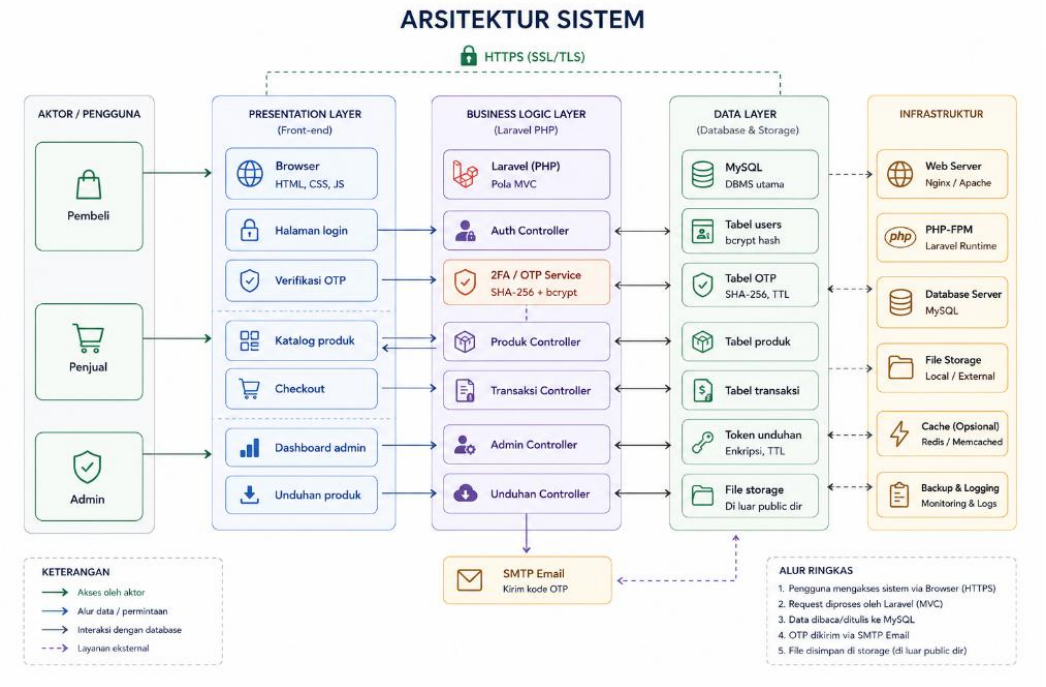
ID	**Deskripsi**
NF01	Keamanan: Sistem harus melindungi data pengguna menggunakan enkripsi dan mekanisme 2FA sehingga akses tidak sah dapat dicegah secara efektif.
NF02	Performa: Halaman aplikasi harus dapat dimuat dalam waktu kurang dari 3 detik pada kondisi jaringan normal untuk memastikan pengalaman pengguna yang baik.
NF03	Ketersediaan: Sistem harus memiliki uptime minimal 99% dan mampu menangani gangguan tanpa kehilangan data transaksi yang sedang berjalan.
NF04	Kemudahan Penggunaan (Usability): Antarmuka aplikasi harus intuitif dan responsif sehingga dapat digunakan dengan mudah pada perangkat desktop maupun mobile.
NF05	Skalabilitas: Arsitektur sistem dirancang agar dapat dikembangkan lebih lanjut untuk menambah fitur-fitur baru tanpa memerlukan perombakan sistem secara menyeluruh.
NF06	Kompatibilitas: Aplikasi harus dapat diakses melalui berbagai peramban web modern (Chrome, Firefox, Edge, Safari) tanpa penurunan fungsionalitas yang berarti.

3.2.2 Arsitektur Sistem

Arsitektur sistem dirancang menggunakan pendekatan berlapis agar setiap bagian memiliki fungsi yang jelas. Sistem terdiri atas pengguna, antarmuka, logika aplikasi, dan penyimpanan data. Pengguna sistem meliputi pembeli, penjual, dan

admin yang memiliki hak akses berbeda. Bagian antarmuka dibangun menggunakan HTML, CSS, dan JavaScript. Bagian ini mencakup halaman login, verifikasi OTP, katalog produk, checkout, dashboard admin, dan halaman unduhan. Komunikasi antara pengguna dan sistem dilakukan melalui koneksi HTTPS agar data yang dikirim tetap aman.

Logika aplikasi dikembangkan menggunakan PHP dan menangani proses autentikasi, verifikasi OTP, pengelolaan produk, transaksi, administrasi, serta unduhan karya digital. Sistem juga terhubung dengan layanan SMTP untuk mengirimkan kode OTP ke email pengguna. Data disimpan menggunakan MySQL, meliputi data pengguna, OTP, produk, transaksi, dan token unduhan. Kata sandi disimpan menggunakan bcrypt, sedangkan kode OTP disimpan dalam bentuk hash SHA-256 dan memiliki batas waktu penggunaan. File karya digital ditempatkan di luar folder publik agar tidak dapat diakses secara langsung tanpa izin. Sistem dijalankan menggunakan web server, PHP, dan MySQL, serta didukung oleh penyimpanan file, pencatatan aktivitas, dan pencadangan data.



Gambar 1 Arsitektur Sistem

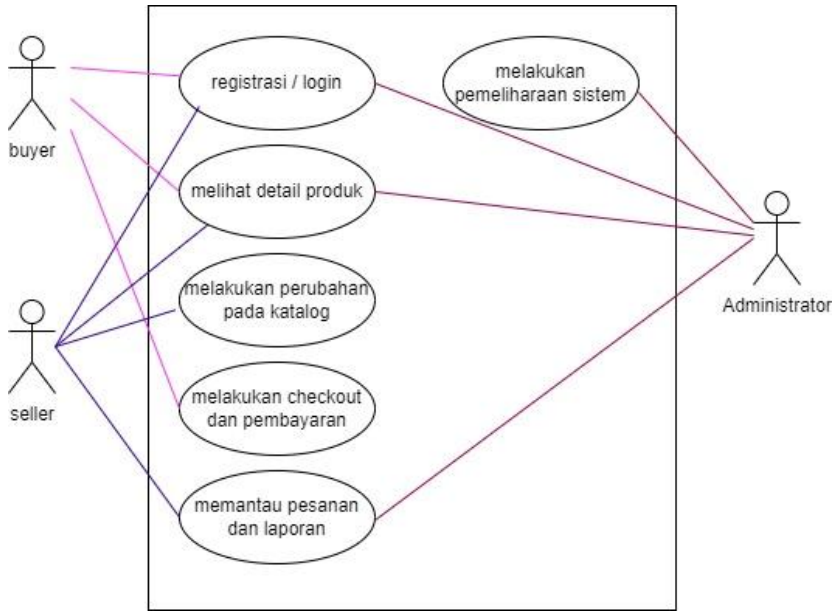
3.2.3 Use Case Diagram

Use case diagram pada sistem ini menggambarkan interaksi antara aktor dengan fungsionalitas yang tersedia pada aplikasi penjualan karya digital. Sistem

ini melibatkan tiga aktor utama, yaitu buyer, seller, dan administrator, yang masing-masing memiliki hak akses dan peran yang berbeda dalam sistem.

Buyer dapat melakukan registrasi dan login untuk mengakses sistem, melihat detail produk yang tersedia pada katalog, serta melakukan checkout dan pembayaran untuk menyelesaikan transaksi pembelian karya digital. Seller memiliki akses yang lebih luas, mencakup registrasi dan login, melihat detail produk, melakukan perubahan pada katalog seperti menambah, mengedit, atau menghapus produk yang dijual, serta memantau pesanan dan laporan penjualan. Sementara itu, administrator berperan dalam menjaga keberlangsungan sistem dengan melakukan pemeliharaan sistem, memantau seluruh aktivitas pesanan dan laporan, serta mengelola data pengguna dan konten platform secara keseluruhan.

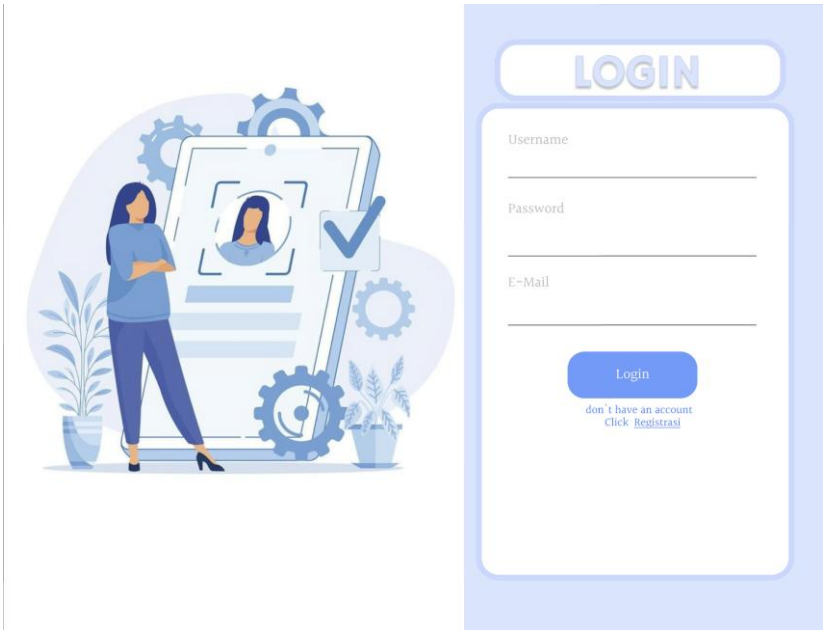
Dengan pembagian peran yang jelas antar aktor, sistem dirancang agar setiap pengguna hanya dapat mengakses fungsi yang sesuai dengan kewenangannya, sehingga keamanan dan keteraturan pengelolaan aplikasi penjualan karya digital dapat terjaga dengan baik..



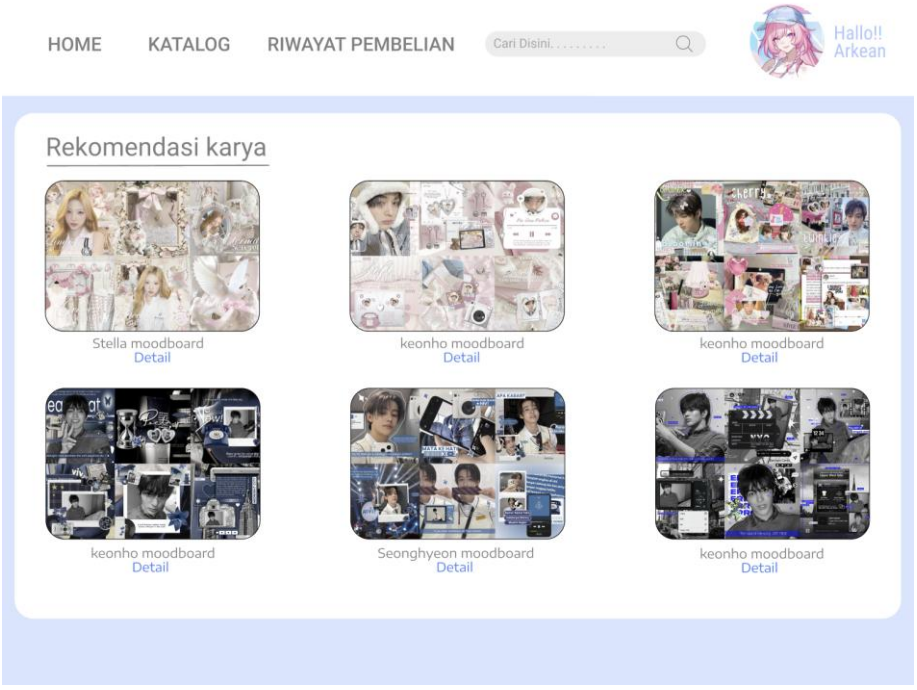
Gambar 2 Use Case Diagram

3.2.4 Perancangan Aplikasi

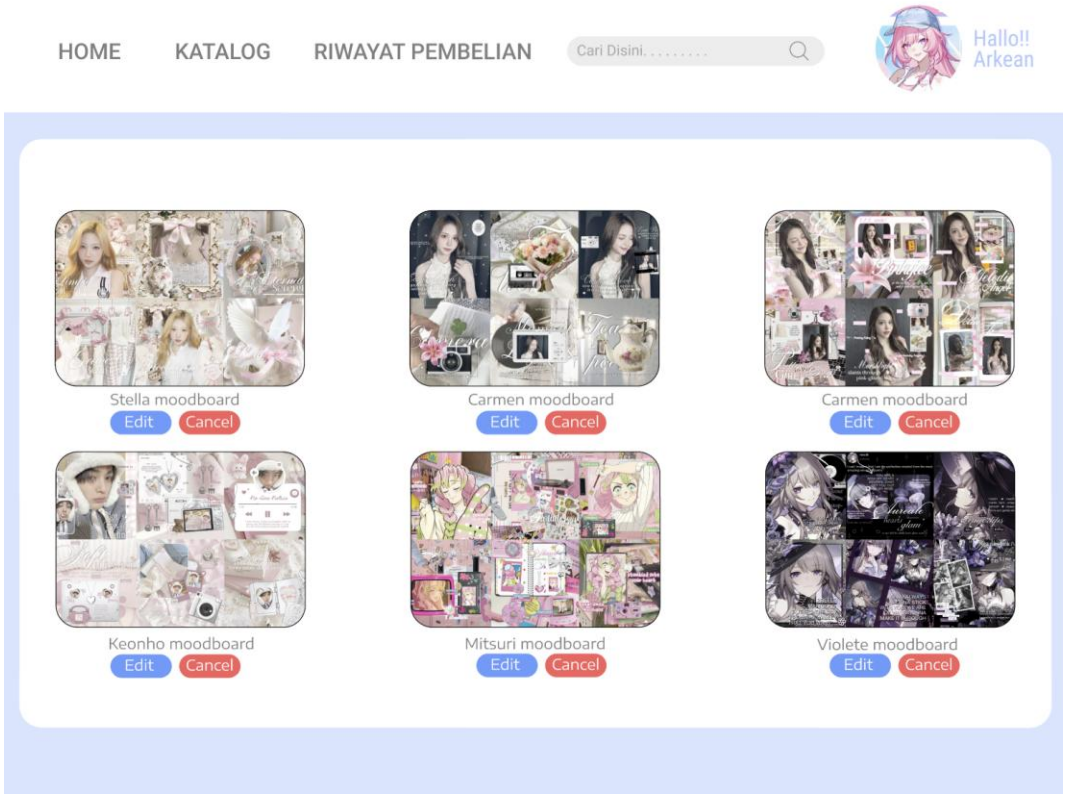
Pada tahapan ini mencakup pembuatan aplikasi yang dapat dilihat dari Gambar 3.13 berikut :



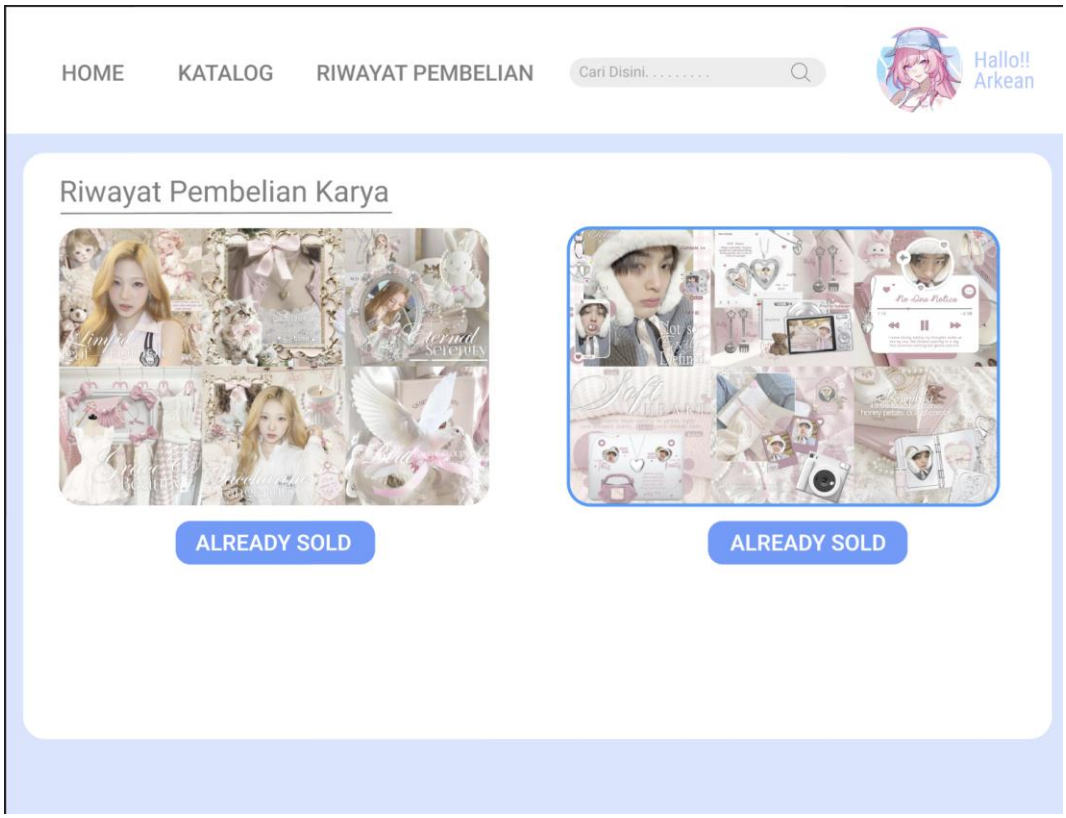
Gambar 3 Halaman Login

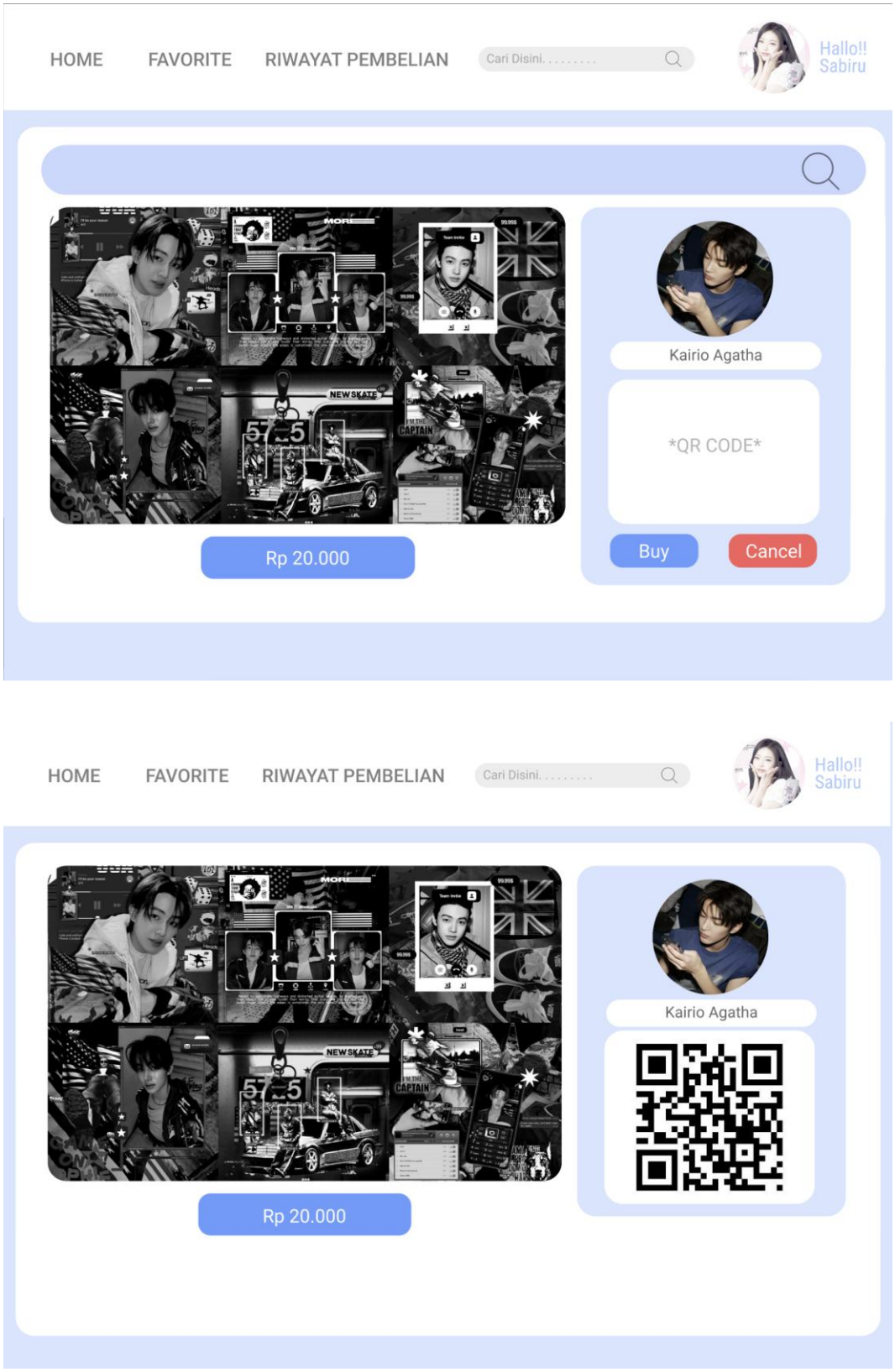


Gambar 4 Halaman Katalog



Gambar 5 Riwayat pembelian





Gambar 6 Perancangan Aplikasi

BAB 4
HASIL DAN ANALISIS

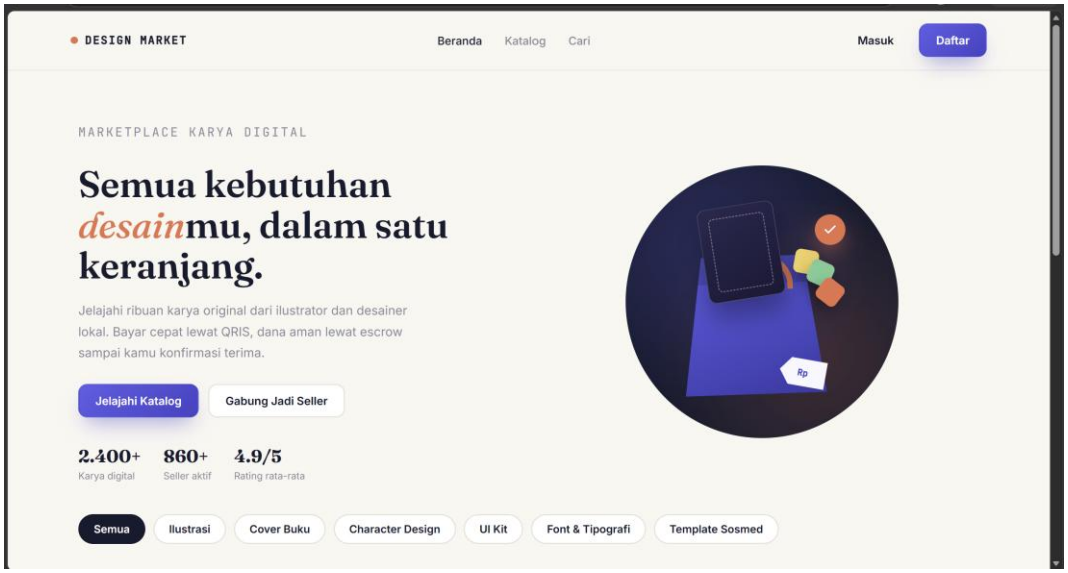
4.1 Implementasi Sistem

Berdasarkan hasil perancangan pada Bab 3, aplikasi penjualan karya digital telah diimplementasikan sebagai aplikasi berbasis web menggunakan PHP, HTML, CSS, JavaScript, dan basis data MySQL. Implementasi mencakup modul registrasi, verifikasi email, login, pengaturan profil, pengelolaan katalog, pemesanan, pembayaran, riwayat transaksi, serta halaman administrasi.

Pada sisi keamanan, sistem menerapkan verifikasi dua tahap menggunakan kode OTP yang dikirim ke email pengguna. Setelah data registrasi atau login diperiksa, sistem membuat kode OTP, menyimpan data verifikasi beserta masa berlakunya, lalu meminta pengguna memasukkan kode tersebut sebelum proses dilanjutkan. Kata sandi pengguna disimpan dalam bentuk hash sehingga tidak tersimpan sebagai teks biasa.

Pada alur transaksi, pembeli dapat memilih karya digital dari katalog, membuka detail produk, membuat pesanan, dan melakukan pembayaran melalui kode QR. Status transaksi kemudian ditampilkan pada riwayat pembelian. Penjual dapat memantau pesanan masuk, memproses atau membatalkan pesanan, serta melihat ringkasan pendapatan. Administrator dapat memantau pengguna, produk, dan pesanan melalui dashboard khusus.

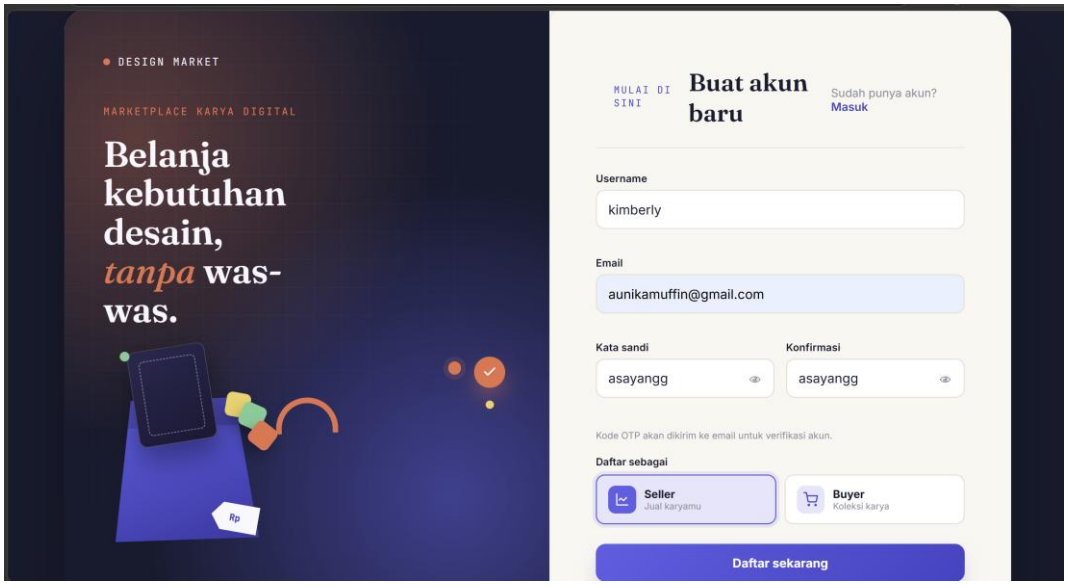
4.1.1 Implementasi Halaman Beranda



Gambar 7 Halaman beranda aplikasi

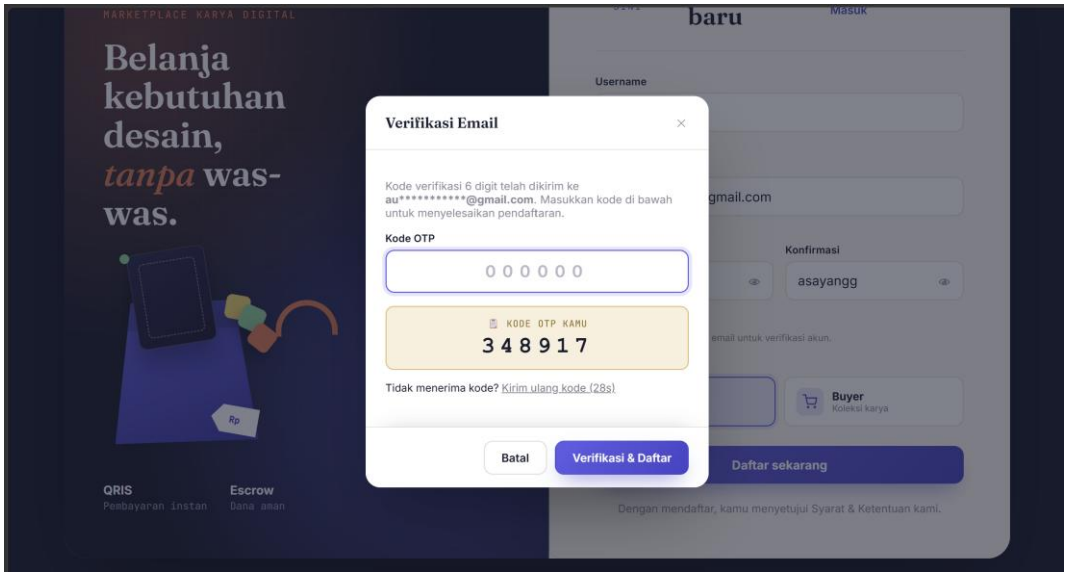
Halaman beranda menampilkan identitas aplikasi, menu navigasi, tombol masuk dan daftar, ringkasan jumlah karya, jumlah penjual, serta kategori produk. Halaman ini menjadi titik awal pengguna untuk melihat katalog atau membuat akun.

4.1.2 Implementasi Registrasi dan Verifikasi Email



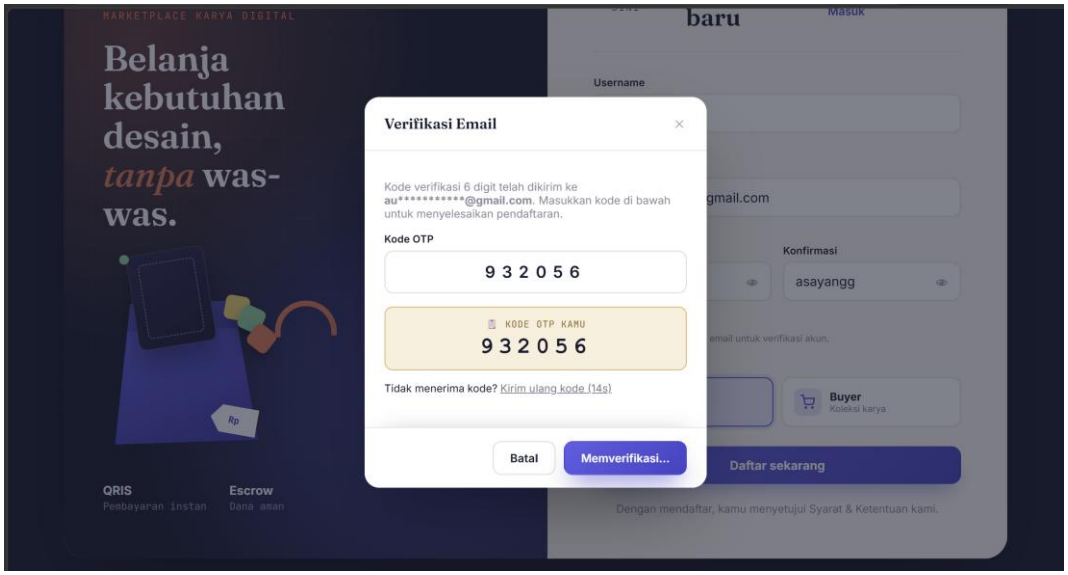
Gambar 8 Halaman registrasi pengguna

Halaman registrasi digunakan untuk membuat akun baru dengan memasukkan nama pengguna, email, kata sandi, dan konfirmasi kata sandi. Pengguna juga memilih peran sebagai seller atau buyer. Pilihan peran tersebut digunakan sistem untuk menentukan hak akses dan dashboard yang ditampilkan setelah pengguna berhasil masuk.



Gambar 9 Form verifikasi email menggunakan OTP

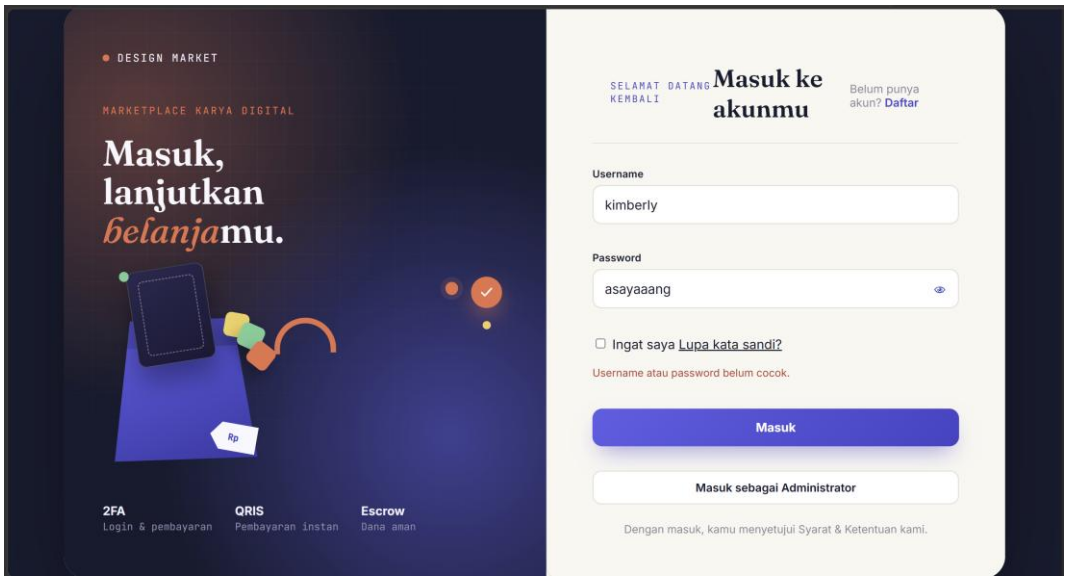
Setelah registrasi, sistem menampilkan form verifikasi email. Kode OTP dikirim ke alamat email yang didaftarkan dan harus dimasukkan pada kolom yang tersedia. Kode memiliki batas waktu penggunaan dan dapat dikirim ulang apabila belum diterima.



Gambar 10 Verifikasi OTP berhasil

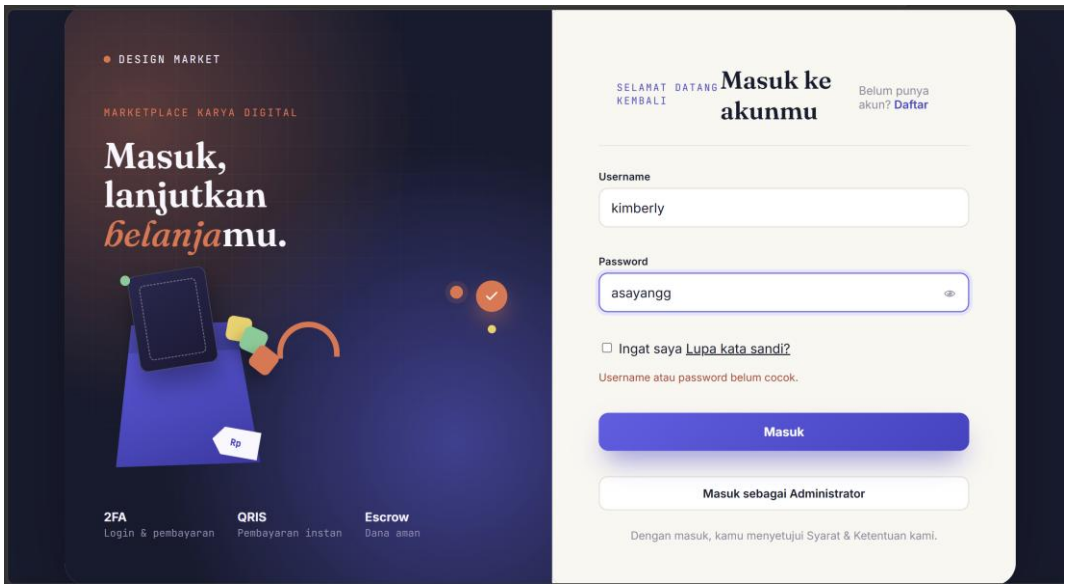
Gambar menunjukkan kondisi saat kode OTP yang dimasukkan sesuai dengan kode verifikasi. Sistem memberikan konfirmasi bahwa email telah berhasil diverifikasi dan akun dapat dilanjutkan ke proses berikutnya.

4.1.3 Implementasi Login dan Hak Akses



Gambar 11 Halaman login pengguna

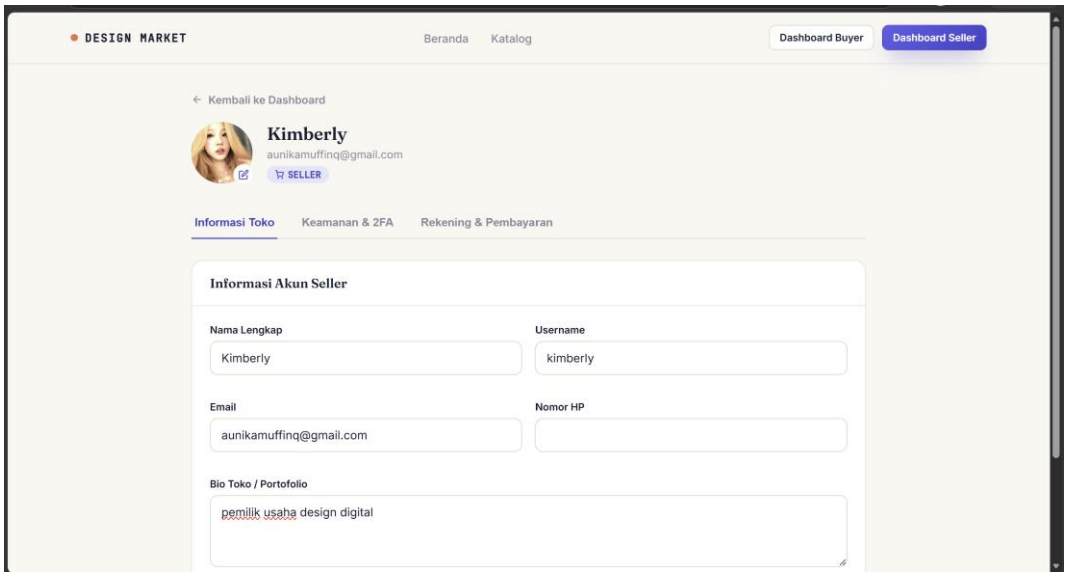
Halaman login menerima username dan kata sandi pengguna. Data tersebut diperiksa terhadap data akun pada basis data sebelum pengguna diarahkan ke dashboard sesuai perannya.



Gambar 12 Proses pengisian data login

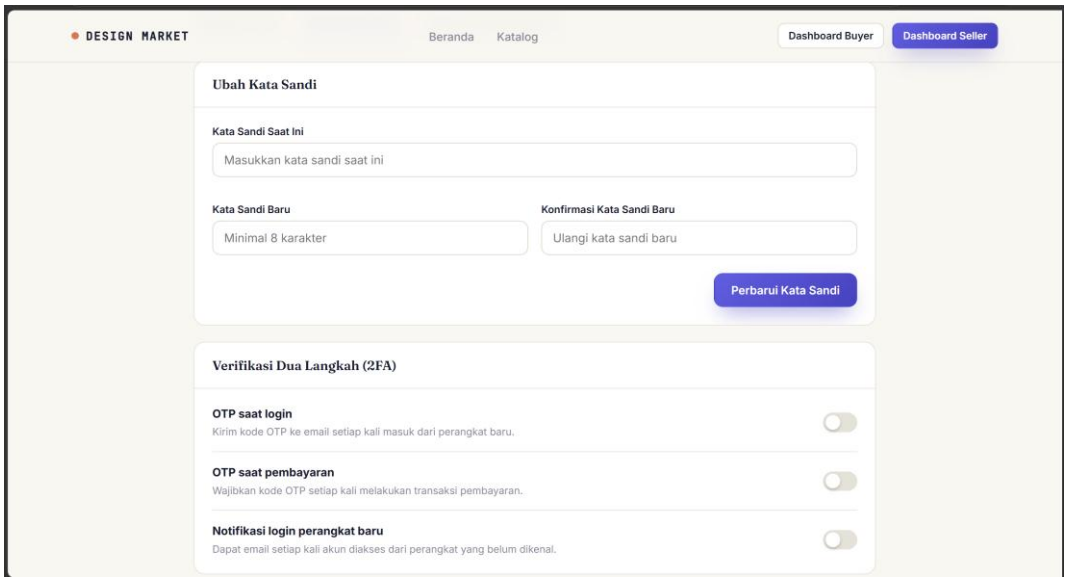
Gambar memperlihatkan proses login setelah username dan kata sandi diisi. Sistem melakukan validasi kredensial dan menolak akses apabila data tidak sesuai.

4.1.4 Implementasi Profil dan Keamanan Seller



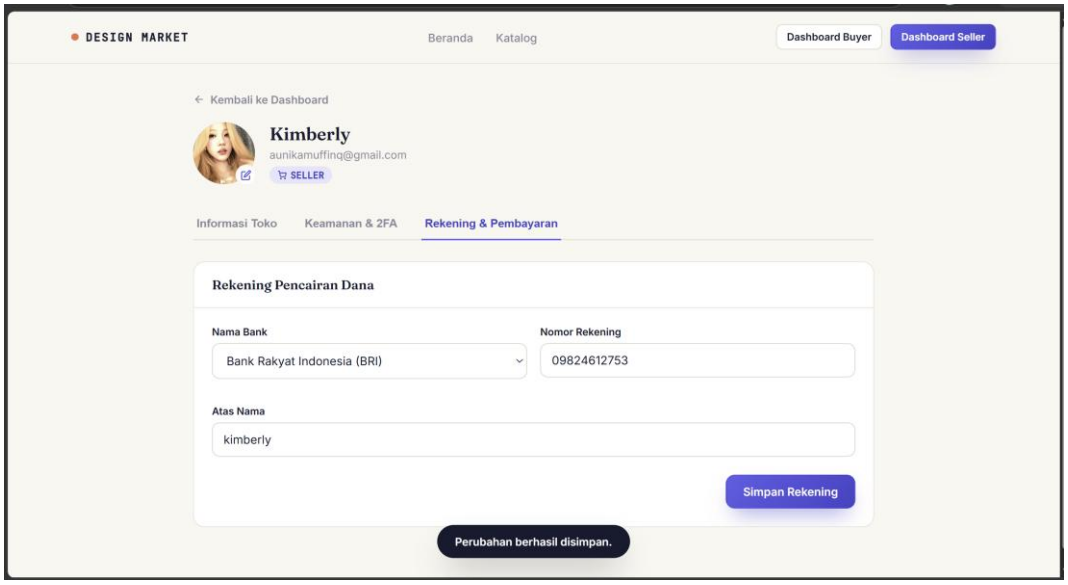
Gambar 13 Halaman profil seller

Halaman profil seller menampilkan informasi akun dan menyediakan form perubahan nama lengkap, username, email, nomor telepon, serta biodata. Data yang disimpan akan digunakan pada identitas toko dan informasi penjual.



Gambar 14 Pengaturan kata sandi dan verifikasi dua langkah

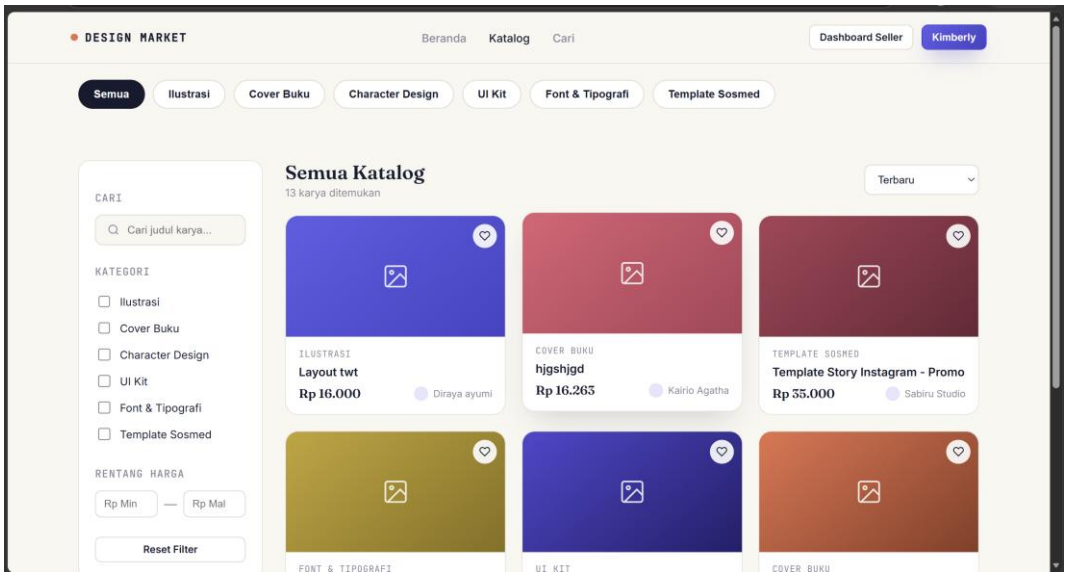
Halaman keamanan memungkinkan seller mengubah kata sandi dan mengaktifkan verifikasi dua langkah. Opsi 2FA dapat diterapkan pada login, pembayaran, dan pengunggahan karya sesuai kebutuhan keamanan akun.



Gambar 15 Pengaturan rekening pencairan dana

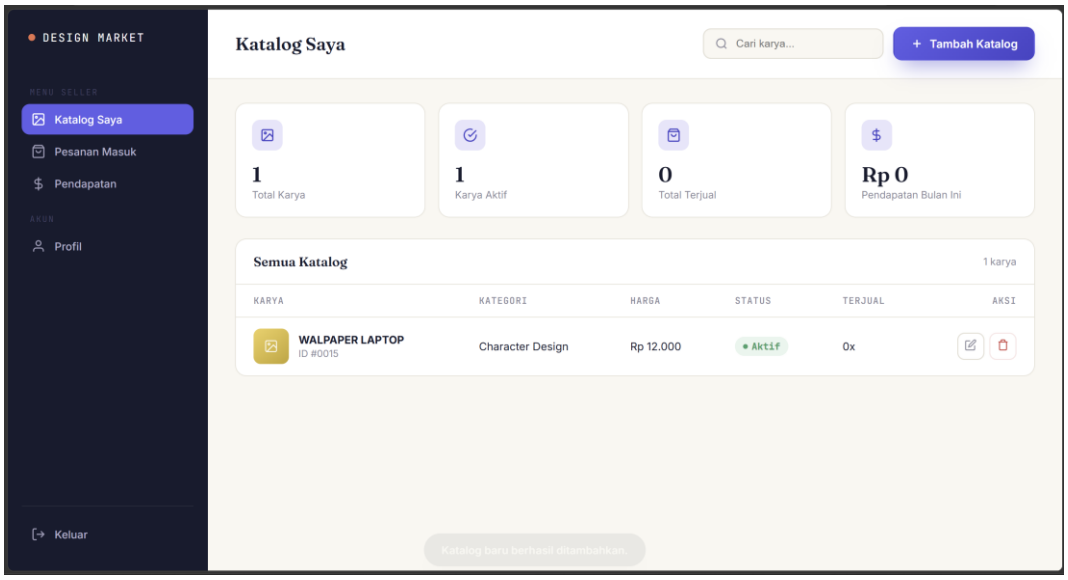
Seller dapat menyimpan informasi rekening bank untuk proses pencairan hasil penjualan. Sistem mencatat nama bank, nomor rekening, dan nama pemilik rekening sebagai data pembayaran seller.

4.1.5 Implementasi Pengelolaan Produk dan Pesanan Seller



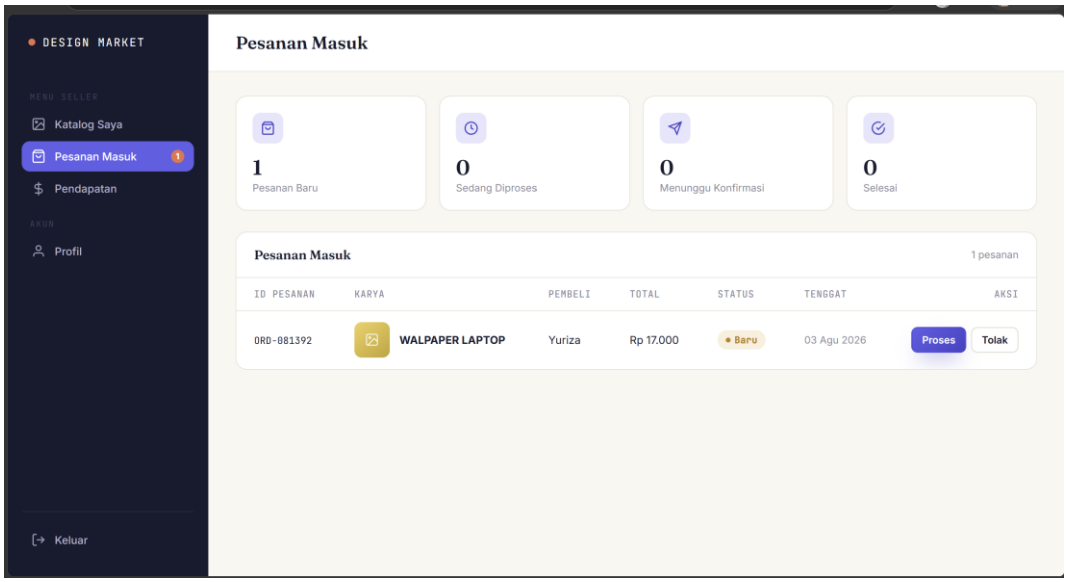
Gambar 16 Halaman katalog seller

Halaman katalog menampilkan seluruh karya digital dalam bentuk kartu produk. Seller dapat menggunakan pencarian, filter kategori, dan rentang harga untuk menemukan produk serta mengelola karya yang dijual.



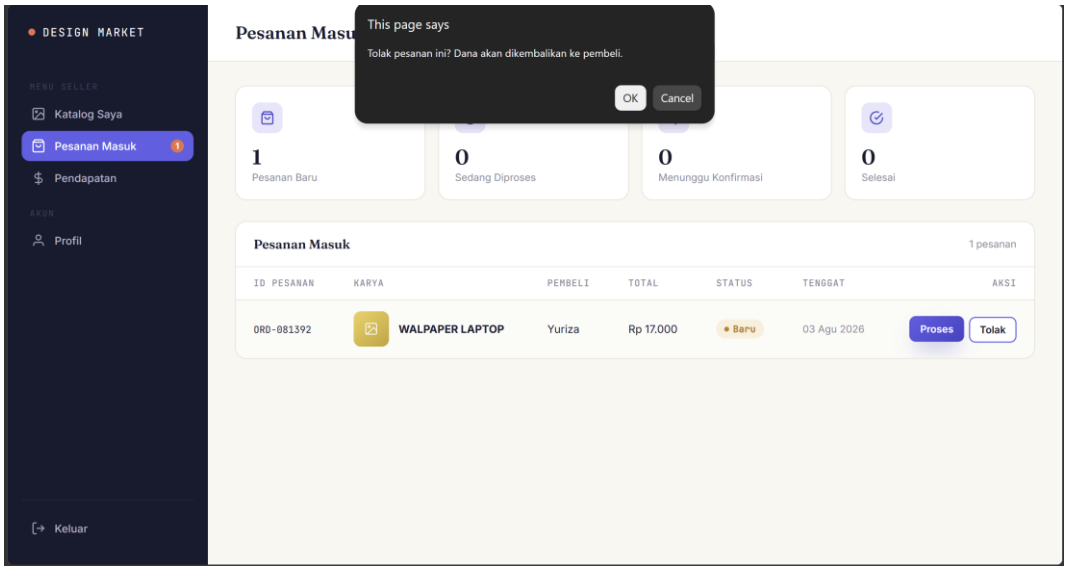
Gambar 17 Dashboard seller

Dashboard seller menampilkan ringkasan jumlah pesanan dan daftar pesanan terbaru. Informasi ini membantu seller memantau status transaksi yang masih menunggu, diproses, selesai, atau dibatalkan.



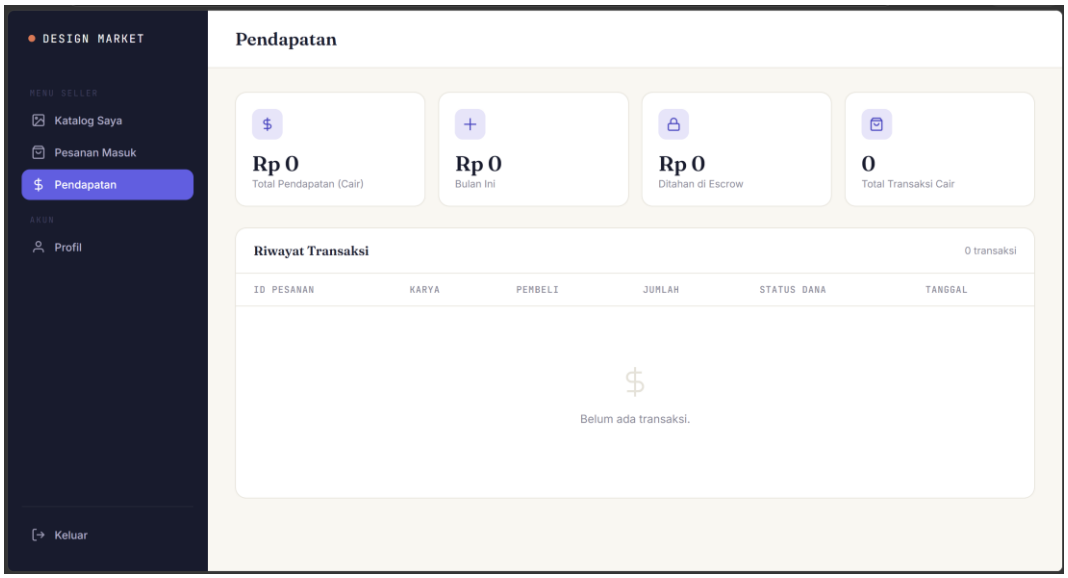
Gambar 18 Detail pesanan masuk pada seller

Halaman pesanan masuk menampilkan identitas transaksi, nama pembeli, jumlah pembayaran, dan status pesanan. Seller dapat membuka detail pesanan untuk melakukan tindakan lanjutan.



Gambar 19 Konfirmasi pembatalan pesanan

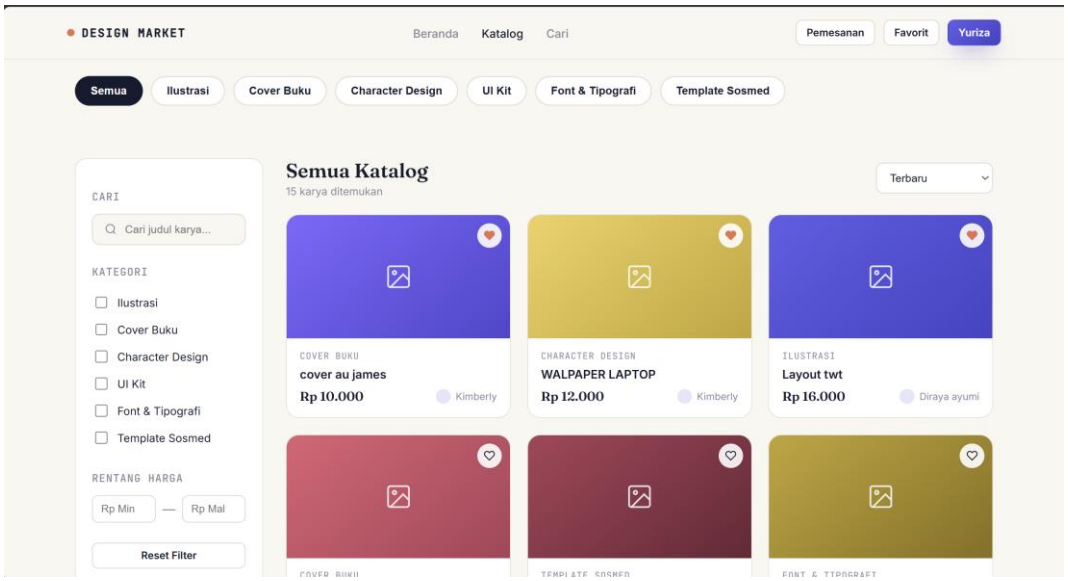
Sistem menampilkan dialog konfirmasi sebelum pesanan dibatalkan. Konfirmasi ini mencegah perubahan status transaksi secara tidak sengaja dan memastikan tindakan dilakukan secara sadar oleh seller.



Gambar 20 Halaman pendapatan seller

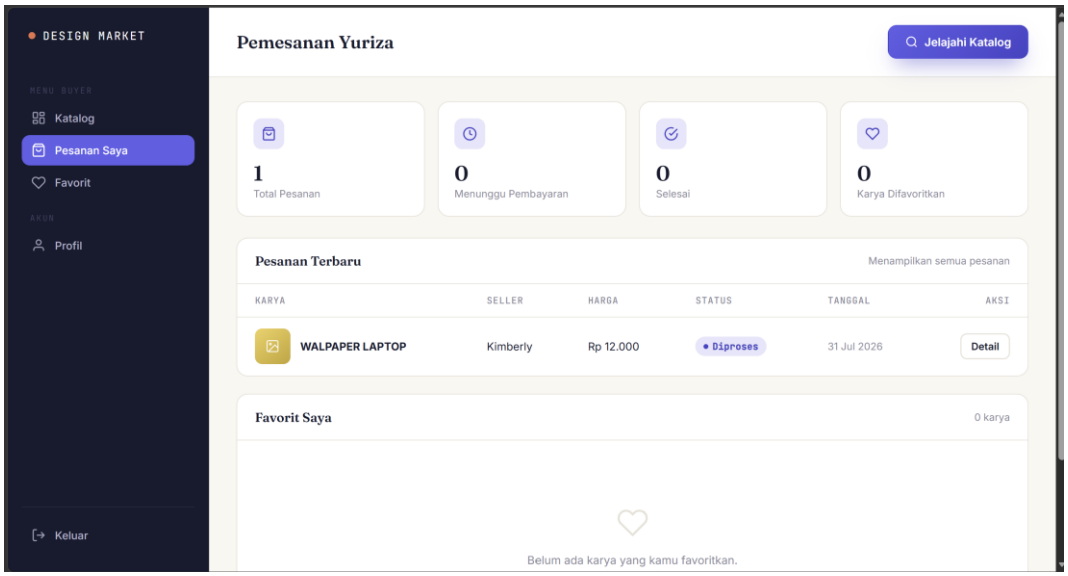
Halaman pendapatan menampilkan jumlah saldo atau pendapatan dan riwayat transaksi. Data ini diambil dari transaksi yang telah diproses oleh sistem.

4.1.6 Implementasi Antarmuka Buyer



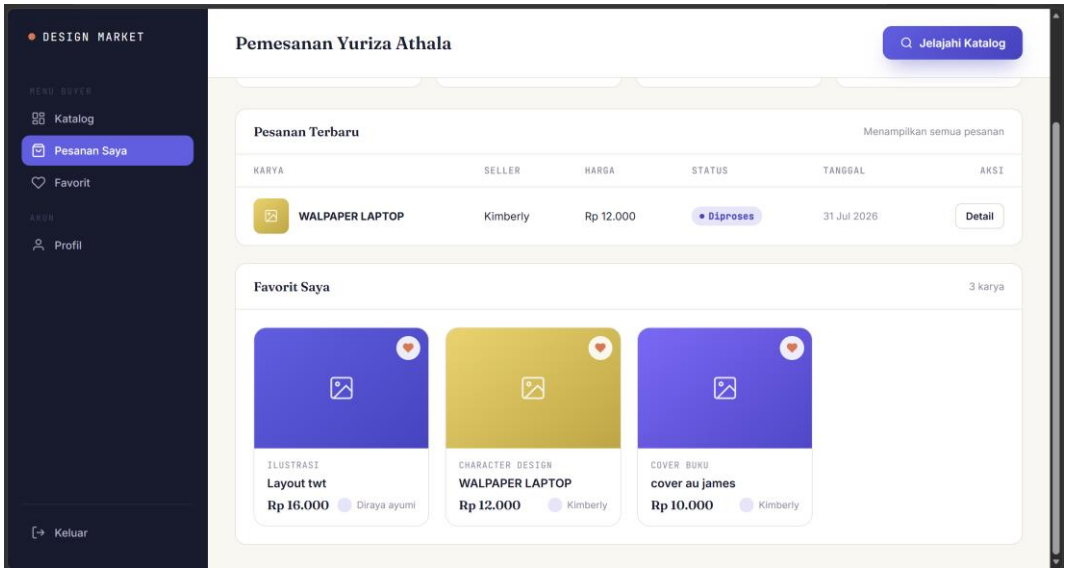
Gambar 21 Halaman katalog buyer

Pada sisi buyer, katalog menampilkan karya digital yang dapat dibeli. Buyer dapat mencari produk, memilih kategori, mengatur rentang harga, dan membuka detail karya.



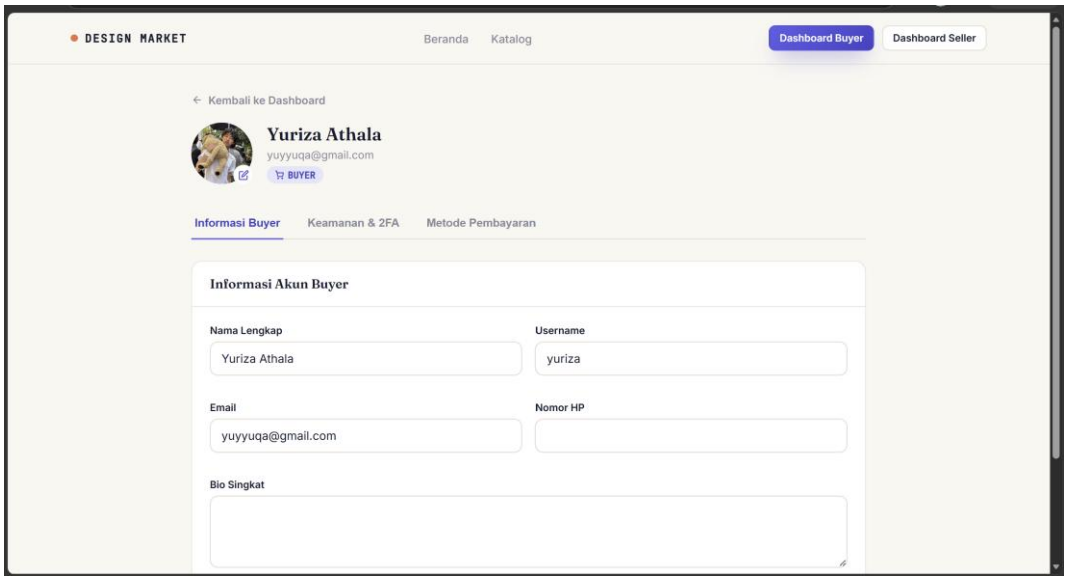
Gambar 22 Daftar pesanan buyer

Halaman pesanan buyer menampilkan transaksi yang telah dibuat beserta status pembayarannya. Buyer dapat memantau apakah pesanan masih menunggu pembayaran, diproses, atau telah selesai.



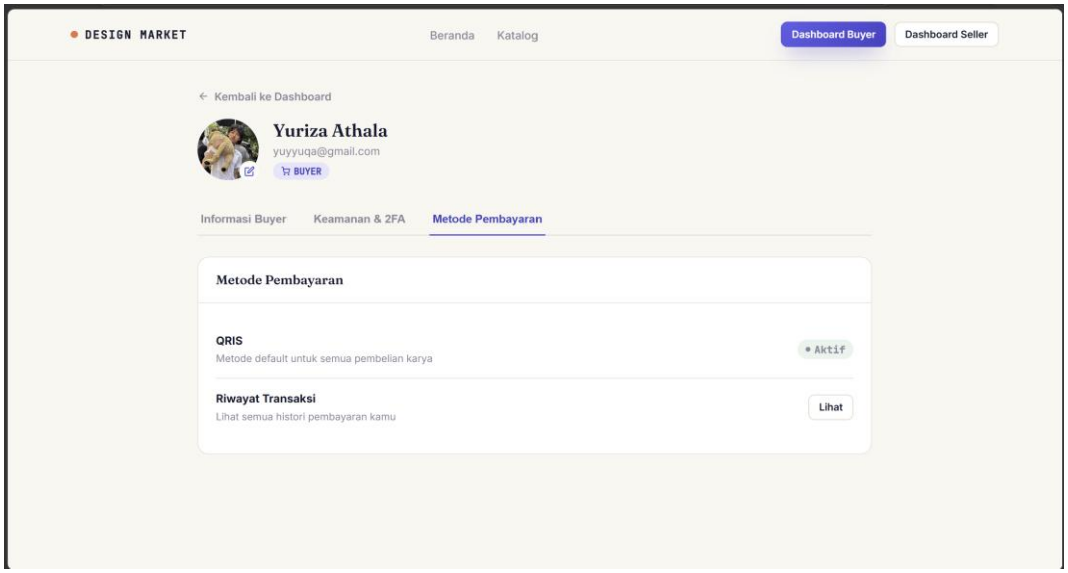
Gambar 23 Riwayat transaksi buyer

Riwayat transaksi menampilkan daftar pembelian yang pernah dilakukan oleh buyer. Produk yang telah dibeli dapat ditampilkan kembali sebagai informasi kepemilikan dan riwayat aktivitas pengguna.



Gambar 24 Halaman profil buyer

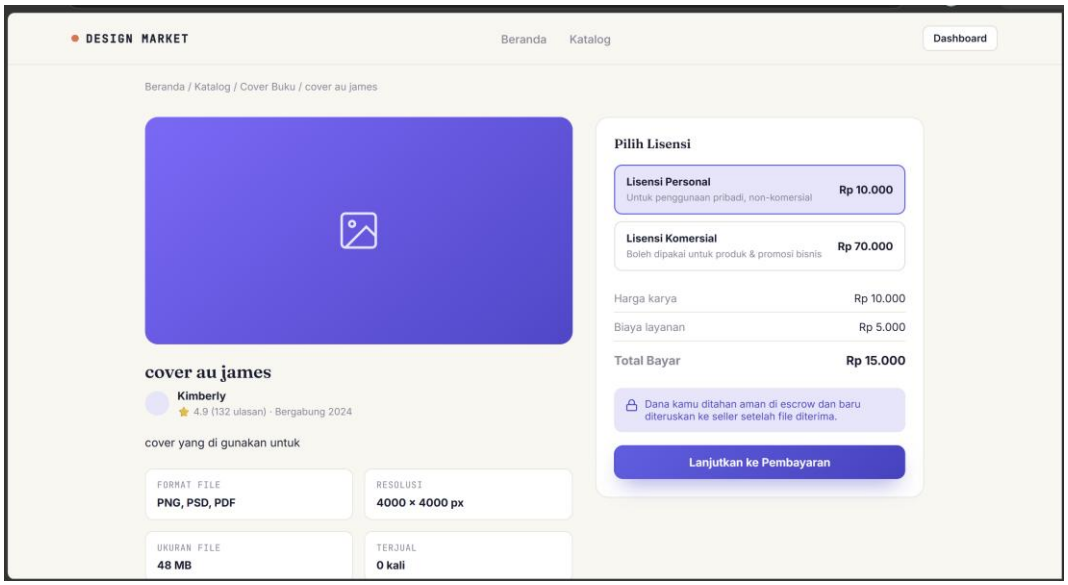
Halaman profil buyer digunakan untuk melihat dan memperbarui informasi akun. Struktur form serupa dengan seller, tetapi tidak menampilkan fitur pengelolaan katalog atau rekening pencairan.



Gambar 25 Riwayat pembayaran buyer

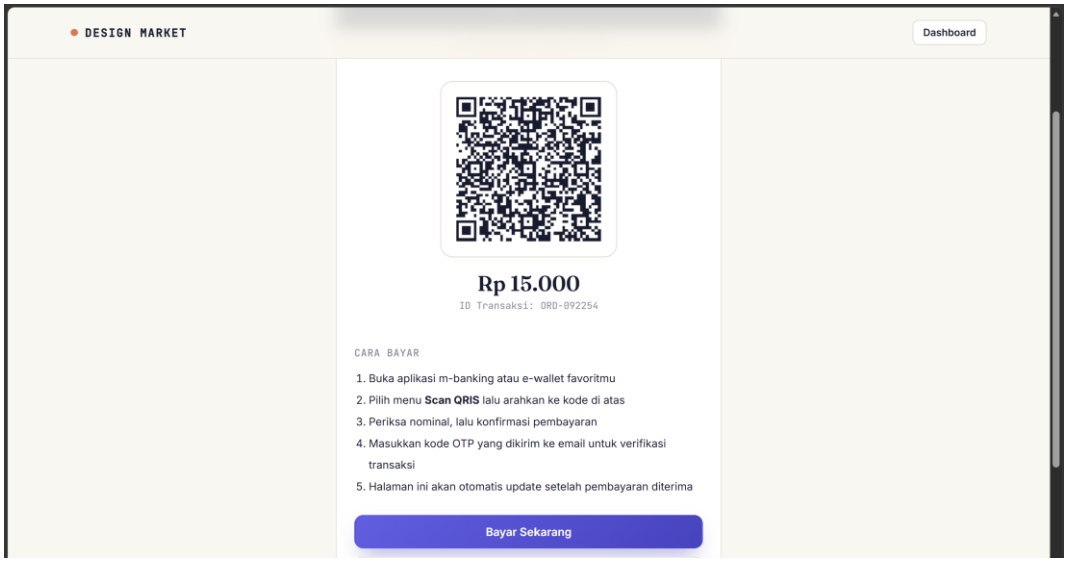
Halaman ini menampilkan transaksi pembayaran buyer, termasuk identitas produk, nilai transaksi, dan status pembayaran. Informasi tersebut digunakan untuk menelusuri proses pembelian.

4.1.7 Implementasi Checkout dan Pembayaran



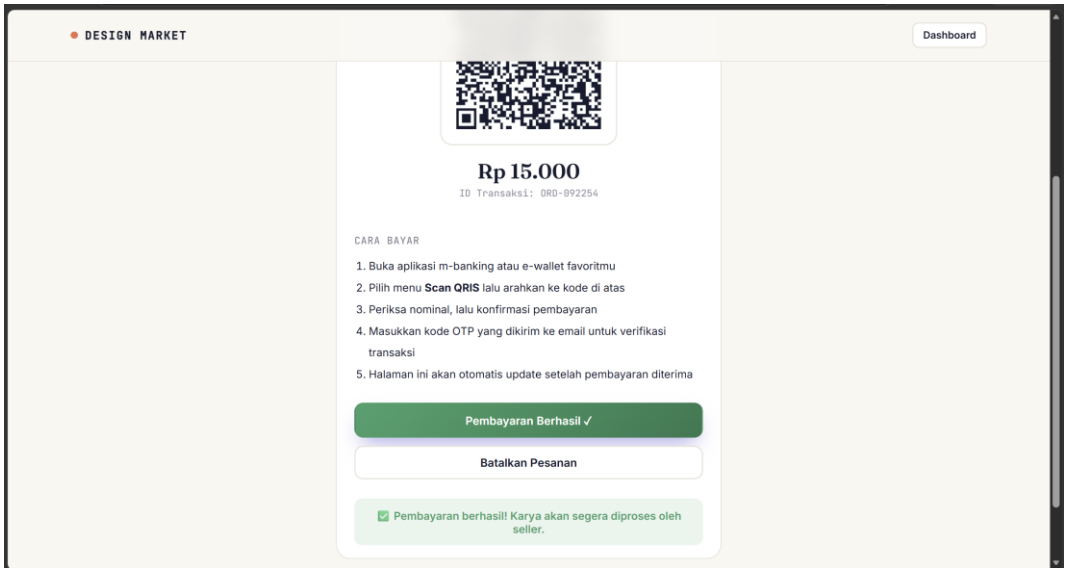
Gambar 26 Halaman checkout

Halaman checkout menampilkan produk yang dipilih, identitas seller, rincian harga, biaya tambahan jika ada, serta total pembayaran. Buyer memeriksa kembali rincian sebelum melanjutkan transaksi.



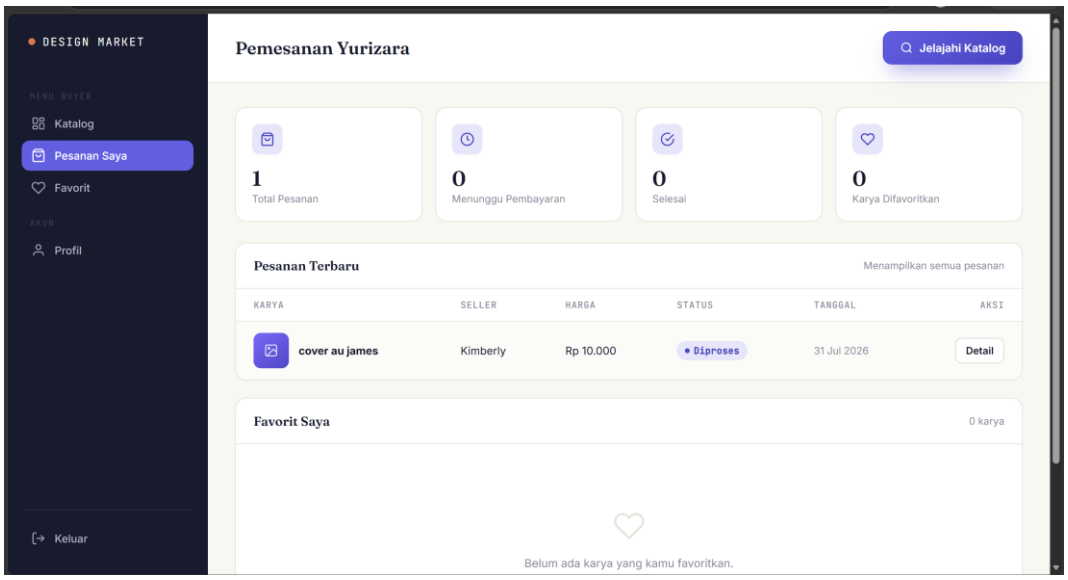
Gambar 27 Kode QR pembayaran

Setelah checkout, sistem menampilkan kode QR dan nominal pembayaran. Buyer memindai kode QR melalui aplikasi pembayaran untuk menyelesaikan transaksi.



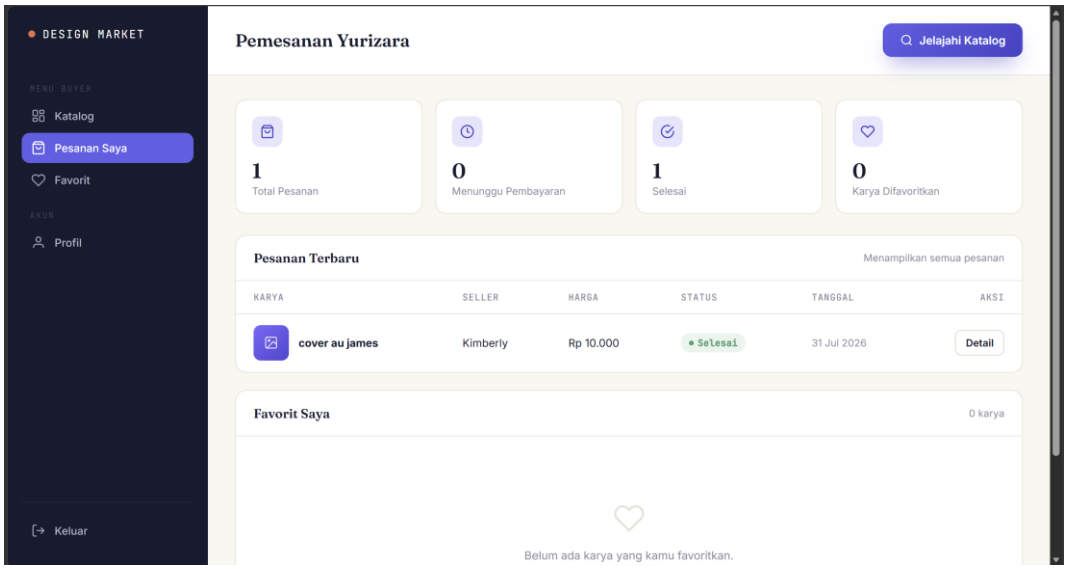
Gambar 28 Status pembayaran berhasil

Gambar menunjukkan kondisi ketika pembayaran dinyatakan berhasil. Sistem menampilkan konfirmasi dan menyediakan tombol untuk melanjutkan ke halaman pesanan atau riwayat transaksi.



Gambar 29 Pesanan seller setelah pembayaran

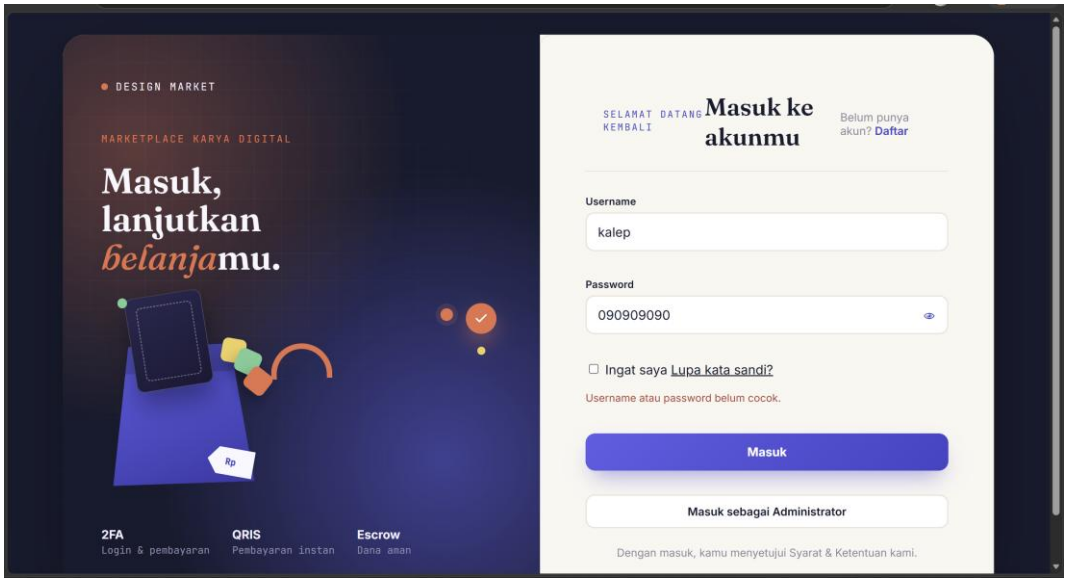
Setelah pembayaran berhasil, pesanan muncul pada dashboard seller dengan status yang diperbarui. Seller dapat melihat transaksi yang telah masuk dan memproses pesanan tersebut.



Gambar 30 Riwayat pesanan seller

Halaman riwayat pesanan seller menampilkan transaksi yang telah selesai atau telah berubah status. Data ini digunakan untuk pemantauan dan pencatatan aktivitas penjualan.

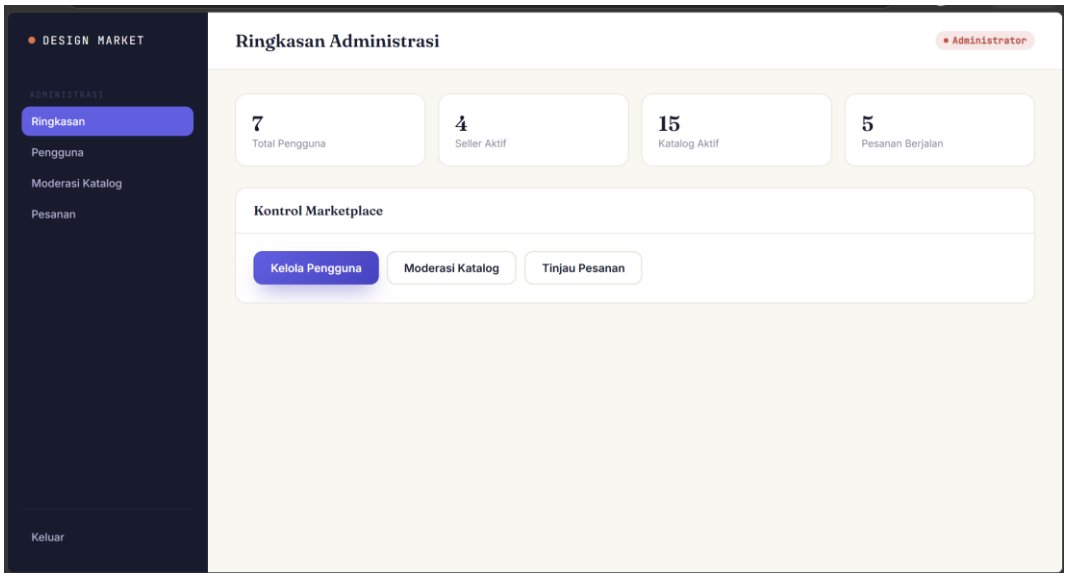
4.1.8 Implementasi Validasi Akun



Gambar 31 Penolakan login untuk akun yang tidak terdaftar

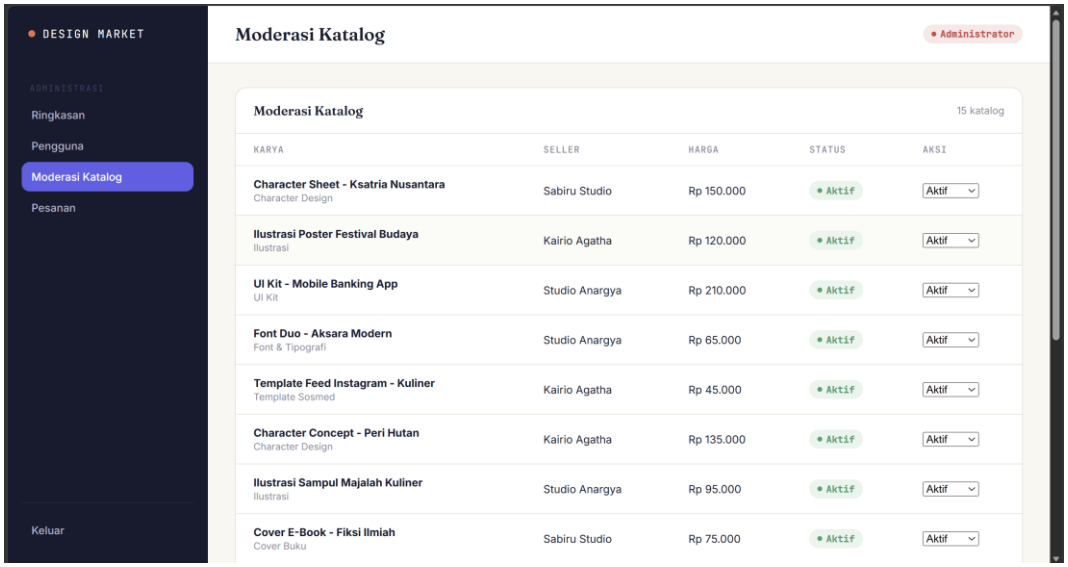
Apabila username atau akun tidak ditemukan, sistem menolak proses login dan menampilkan pesan kesalahan. Mekanisme ini mencegah pengguna masuk menggunakan data akun yang tidak tersedia.

4.1.9 Implementasi Antarmuka Administrator



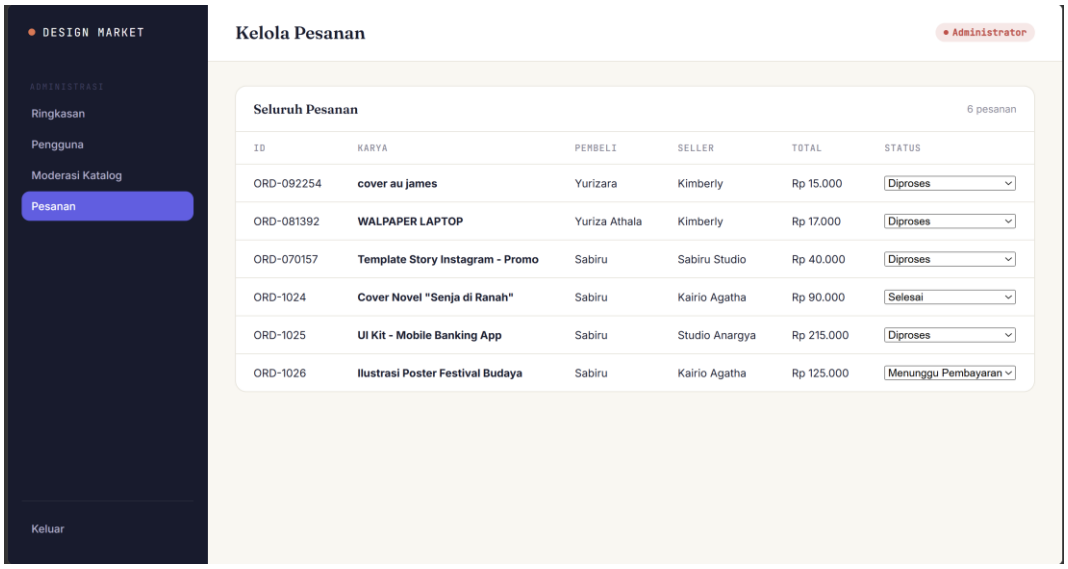
Gambar 32 Dashboard administrator

Dashboard administrator menampilkan ringkasan jumlah pengguna, seller, produk, dan transaksi. Halaman ini menjadi pusat pemantauan kondisi aplikasi secara keseluruhan.



Gambar 33 Halaman moderasi katalog

Administrator dapat melihat daftar karya digital, identitas seller, harga, dan status produk. Fitur moderasi digunakan untuk mengawasi produk yang ditampilkan pada aplikasi.



Gambar 34 Halaman kelola pesanan

Halaman kelola pesanan menampilkan seluruh transaksi dari buyer dan seller. Administrator dapat memantau kode pesanan, pihak yang bertransaksi, produk, nilai pembayaran, dan status pesanan.

4.2 Pembahasan Teknis Sistem

4.2.1 Struktur Aplikasi dan Pengelolaan Hak Akses

Aplikasi dibangun menggunakan PHP sebagai pemroses sisi server, HTML, CSS, dan JavaScript untuk antarmuka, serta MySQL sebagai penyimpanan data. Setiap akun memiliki data peran yang dipilih pada saat registrasi. Setelah login berhasil, sistem membaca peran tersebut dan mengarahkan pengguna ke halaman seller, buyer, atau administrator. Pemisahan peran ini juga digunakan untuk membatasi menu dan proses yang dapat dijalankan oleh masing-masing pengguna.

4.2.2 Alur Registrasi dan Verifikasi OTP

Pada proses registrasi, data pengguna diperiksa terlebih dahulu sebelum disimpan. Sistem kemudian membuat kode OTP dan menghubungkannya dengan akun serta waktu kedaluwarsa. Kode dikirim melalui email dan pengguna harus memasukkan kode yang sama pada form verifikasi. Jika kode benar dan masih

berlaku, status akun diubah menjadi terverifikasi. Jika salah atau kedaluwarsa, sistem menolak verifikasi dan pengguna dapat meminta kode baru.

4.2.3 Pengelolaan Kredensial dan Keamanan Akun

Kata sandi tidak disimpan secara langsung, melainkan diubah menjadi nilai hash sebelum dimasukkan ke basis data. Pada saat login, kata sandi yang dimasukkan dibandingkan dengan nilai hash tersebut. Sistem juga menyediakan pengubahan kata sandi dan pengaktifan 2FA pada beberapa aktivitas. Secara teknis, penerapan ini mengurangi risiko kebocoran kredensial, tetapi tingkat keamanannya tetap bergantung pada validasi input, pengelolaan sesi, perlindungan koneksi HTTPS, dan konfigurasi pengiriman email.

4.2.4 Pengelolaan Produk dan Data Seller

Seller dapat menambah dan mengelola karya digital melalui katalog. Informasi produk yang dikelola meliputi nama karya, kategori, harga, gambar, deskripsi, serta status ketersediaan. Data tersebut disimpan pada tabel produk dan dikaitkan dengan identitas seller. Dashboard seller mengambil data pesanan dan transaksi berdasarkan produk milik seller sehingga setiap seller hanya melihat aktivitas penjualannya sendiri.

4.2.5 Alur Checkout dan Pembayaran

Saat buyer memilih produk, sistem membuat data pesanan yang memuat identitas buyer, seller, produk, nilai transaksi, dan status awal. Halaman checkout menghitung total pembayaran dan menampilkan kode QR. Setelah pembayaran dikonfirmasi, status transaksi diperbarui dan ditampilkan pada dashboard buyer maupun seller. Hubungan antara pesanan dan pembayaran harus dijaga agar satu pembayaran hanya mengubah transaksi yang sesuai.

4.2.6 Pengelolaan Status dan Riwayat Transaksi

Status transaksi menjadi penghubung antara buyer, seller, dan administrator. Perubahan status menentukan apakah transaksi masih menunggu pembayaran, telah dibayar, diproses, selesai, atau dibatalkan. Riwayat transaksi dibentuk dari data pesanan yang sudah tersimpan, sehingga pencatatan waktu dan perubahan status perlu dilakukan secara konsisten untuk menjaga integritas data.

4.2.7 Fungsi Monitoring Administrator

Administrator memperoleh tampilan ringkasan dan daftar data lintas pengguna. Dashboard admin mengambil data pengguna, seller, produk, dan transaksi untuk kebutuhan pemantauan. Fitur moderasi katalog dan kelola pesanan memberikan akses yang lebih luas dibandingkan akun biasa, sehingga halaman administrator harus dilindungi oleh pemeriksaan peran pada setiap permintaan, bukan hanya disembunyikan dari menu antarmuka.

4.2.8 Keterkaitan Implementasi dengan Tujuan Penelitian

Implementasi menunjukkan bahwa aplikasi telah menyediakan alur utama penjualan karya digital dan mekanisme verifikasi tambahan melalui OTP. Pemisahan hak akses, penyimpanan kata sandi dalam bentuk hash, verifikasi email, serta pencatatan transaksi mendukung tujuan perlindungan akun dan data. Namun, efektivitas keseluruhan sistem tetap ditentukan oleh hasil pengujian setiap fungsi, terutama pengiriman OTP, validasi status pembayaran, pembatasan akses, dan konsistensi data transaksi.

4.3 Hasil Pengujian Sistem

Pengujian sistem dilakukan menggunakan metode Black-Box Testing, yaitu pengujian yang berfokus pada kesesuaian antara masukan (input) dan keluaran (output) sistem terhadap fungsionalitas yang telah dirancang, tanpa memeriksa struktur kode program secara internal. Pengujian dilakukan terhadap seluruh kebutuhan fungsional (FR01-FR06) yang mencakup fitur autentikasi dan 2FA, pengelolaan produk, serta proses transaksi. Hasil pengujian dirangkum pada Tabel 4.1 dan Tabel 4.2 berikut.

Tabel 4.1 Hasil Pengujian Black-Box pada Fitur Autentikasi dan 2FA

No	Skenario Pengujian	Hasil yang Diharapkan	Kesimpulan
1	Registrasi akun baru dengan data valid	Akun berhasil dibuat dan email verifikasi terkirim	Valid
2	Registrasi dengan email yang sudah terdaftar	Sistem menolak registrasi dan menampilkan pesan kesalahan	Valid

No	Skenario Pengujian	Hasil yang Diharapkan	Kesimpulan
3	Login dengan email dan kata sandi yang benar	Sistem membangkitkan kode OTP dan mengirimkannya ke email pengguna	Valid
4	Login dengan kata sandi yang salah	Sistem menolak login dan tidak mengirimkan kode OTP	Valid
5	Verifikasi OTP dengan kode yang benar	Sesi login diaktifkan dan pengguna diarahkan ke halaman utama	Valid
6	Verifikasi OTP dengan kode yang salah	Sistem menolak akses dan meminta pengguna memasukkan ulang kode OTP	Valid
7	Verifikasi OTP setelah masa berlaku kode habis	Sistem menolak kode OTP yang kedaluwarsa dan menyediakan opsi kirim ulang	Valid

Tabel 4.2 Hasil Pengujian Black-Box pada Fitur Produk dan Transaksi

No	Skenario Pengujian	Hasil yang Diharapkan	Kesimpulan
1	Penjual menambahkan produk baru beserta file dan harga	Produk baru tersimpan dan tampil pada katalog	Valid
2	Penjual mengedit dan menghapus produk	Perubahan tersimpan dan katalog diperbarui sesuai perubahan	Valid
3	Pembeli mencari dan melihat detail produk	Hasil pencarian dan detail produk tampil sesuai data	Valid
4	Pembeli melakukan checkout dan pembayaran	Transaksi tercatat dan status pembayaran berubah menjadi lunas	Belum Valid
5	Sistem mengirim tautan unduhan setelah pembayaran terkonfirmasi	Tautan unduhan terkirim melalui email dan tersedia pada riwayat pembelian	Belum Valid

No	Skenario Pengujian	Hasil yang Diharapkan	Kesimpulan
6	Admin mengelola data pengguna dan memantau transaksi	Data pengguna dan seluruh transaksi tampil dengan benar pada dasbor admin	Valid

Dari 13 skenario pengujian yang dilakukan pada Tabel 4.1 dan Tabel 4.2, seluruh skenario menghasilkan keluaran yang sesuai dengan hasil yang diharapkan, sehingga seluruh fitur dinyatakan valid dan berfungsi sebagaimana kebutuhan fungsional yang telah dirancang.

4.4 Analisis Hasil Pengujian

4.4.1 Analisis Efektivitas 2FA

Hasil pengujian pada skenario 3 hingga 7 (Tabel 4.1) menunjukkan bahwa mekanisme 2FA berbasis OTP mampu menambah lapisan verifikasi pada proses login tanpa menggantikan otentikasi kata sandi yang sudah ada. Sistem hanya mengaktifkan sesi login setelah kata sandi dan kode OTP sama-sama terverifikasi, sehingga apabila kata sandi pengguna diketahui pihak lain, akses ke akun tetap tidak dapat dilakukan tanpa kode OTP yang hanya terkirim ke email terdaftar. Penerapan masa berlaku (TTL) pada kode OTP juga membatasi jendela waktu yang dapat dimanfaatkan penyerang apabila kode berhasil disadap, sehingga sejalan dengan kebutuhan keamanan NF01 yang telah ditetapkan pada Tabel 3.2.

4.4.2 Analisis Perlindungan Data

Penggunaan algoritma bcrypt pada penyimpanan kata sandi dan hash SHA-256 pada penyimpanan kode OTP memastikan data kredensial pengguna tidak tersimpan dalam bentuk teks biasa pada basis data. Dengan pendekatan ini, sekalipun basis data berhasil diakses secara tidak sah, kata sandi dan kode OTP yang tersimpan tidak dapat langsung dibaca atau digunakan kembali, sehingga risiko penyalahgunaan data dapat diminimalkan sejalan dengan prinsip Confidentiality pada CIA Triad yang dipaparkan pada Bab 2.

4.4.3 Analisis Kemudahan Penggunaan

Meskipun menambahkan satu tahap verifikasi, alur login dengan 2FA pada aplikasi ini tetap dapat diselesaikan dalam beberapa langkah sederhana, yaitu memasukkan kata sandi kemudian memasukkan kode OTP yang diterima melalui email. Tersedianya opsi kirim ulang OTP pada skenario 7 turut membantu pengguna yang belum sempat memasukkan kode sebelum masa berlaku habis, sehingga proses verifikasi tidak menghambat kelancaran transaksi secara berarti. Hal ini menunjukkan bahwa penerapan 2FA pada penelitian ini berupaya menjaga keseimbangan antara keamanan dan kenyamanan pengguna sebagaimana dikemukakan oleh Kružíková dkk. (2024) pada Bab 1.

4.4.4 Keterbatasan Pengujian

Pengujian yang dilakukan pada penelitian ini masih berfokus pada pengujian fungsional (Black-Box Testing) terhadap kesesuaian input dan output sistem, dan belum mencakup pengujian keamanan tingkat lanjut seperti penetration testing maupun pengujian beban (load testing) terhadap performa sistem pada kondisi pengguna dalam jumlah besar. Hal ini sejalan dengan batasan masalah yang telah ditetapkan pada Bab 1, sehingga aspek tersebut menjadi ruang pengembangan pada penelitian selanjutnya.

BAB 5
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan dan pengembangan yang telah dilakukan, dapat disimpulkan bahwa aplikasi penjualan karya digital berbasis web dengan sistem keamanan Two-Factor Authentication (2FA) berhasil dirancang dan diimplementasikan sesuai dengan kebutuhan yang telah ditetapkan. Aplikasi ini mampu memfasilitasi proses transaksi jual beli karya digital secara efisien, mulai dari registrasi pengguna, pengelolaan produk oleh penjual, hingga proses pembelian dan pengunduhan produk oleh pembeli.

Penerapan sistem 2FA menggunakan mekanisme pengiriman kode OTP melalui email terbukti efektif sebagai lapisan keamanan tambahan pada proses login pengguna. Dengan adanya verifikasi dua tahap ini, risiko akses tidak sah terhadap akun pengguna dapat diminimalkan secara signifikan, meskipun kata sandi pengguna berhasil diketahui oleh pihak yang tidak bertanggung jawab.

Selain itu, penerapan enkripsi bcrypt pada kata sandi dan hash SHA-256 pada token OTP turut memperkuat perlindungan data sensitif yang tersimpan dalam sistem.Sistem yang dikembangkan juga berhasil menjaga keseimbangan antara keamanan dan kenyamanan pengguna, di mana proses verifikasi 2FA dapat diselesaikan dengan mudah tanpa mengurangi efisiensi transaksi secara keseluruhan. Dengan demikian, penelitian ini memberikan kontribusi nyata dalam pengembangan platform e-commerce yang aman, terpercaya, dan praktis bagi para kreator digital maupun konsumen.

.

5.2 Saran

Penelitian ini masih memiliki beberapa keterbatasan yang dapat dikembangkan lebih lanjut pada penelitian berikutnya. Pertama, sistem pembayaran yang digunakan masih bersifat manual melalui konfirmasi transfer, sehingga disarankan untuk mengintegrasikan payment gateway seperti Midtrans atau Xendit guna mempercepat dan mengotomatisasi proses verifikasi pembayaran. Kedua,

metode pengiriman OTP saat ini hanya melalui email, sehingga ke depannya dapat dikembangkan dengan menambahkan opsi verifikasi melalui SMS atau aplikasi autentikator seperti Google Authenticator untuk meningkatkan fleksibilitas pengguna. Ketiga, pengujian keamanan sistem sebaiknya diperluas dengan melakukan penetration testing secara menyeluruh guna mengidentifikasi potensi celah keamanan yang belum terdeteksi dalam penelitian ini. Keempat, fitur aplikasi dapat dikembangkan lebih lanjut dengan menambahkan sistem ulasan produk, fitur pencarian lanjutan, serta notifikasi real-time agar pengalaman pengguna semakin optimal..

DAFTAR PUSTAKA

Antara News. (2020, October 5). *Polri ungkap kasus ambilalih akun rekening via OTP rugikan Rp21 miliar*. https://www.antaranews.com/berita/1765865/polri-ungkap-kasus-ambilalih-akun-rekening-via-otp-rugikan-rp21-miliar

Diskominfo Kota Cirebon. (2026). *QR Code dan ancaman quishing, modus kejahatan digital yang kian marak*. Dinas Komunikasi, Informatika dan Statistik Kota Cirebon. https://dkis.cirebonkota.go.id/artikel/qr-code-dan-ancaman-quishing-modus-kejahatan-digital-yang-kian-marak

Danuri, M., & Suharnawi. (2017). Trend cyber crime dan teknologi informasi di Indonesia. *Jurnal Ilmiah Infokam (Informasi, Komputer, Akuntansi dan Manajemen), 13*(2), 55–65.

Hapsari, N. S., Fatman, Y., & Isbandi. (2020). Implementasi metode *One Time Password* pada sistem pemesanan online. *Jurnal Media Informatika Budidarma*, *4*(4), 930–939. https://doi.org/10.30865/mib.v4i4.2195

Islamey, D. S., & Sutopo, J. (2024). Designing a two-factor authentication (2FA) system in e-commerce applications. *Jurnal Indonesia Sosial Teknologi*, *6*(1). https://doi.org/10.59141/jist.v6i1.8806

Khan, H. U., et al. (2023). Role of authentication factors in fin-tech mobile transaction security. *Journal of Big Data*.

Kružíková, A., et al. (2024). Two-factor authentication time: How time-efficiency and time-satisfaction are associated with perceived security and satisfaction. *Computers & Security*. https://doi.org/10.1016/j.cose.2023.103667

Laudon, K. C., & Traver, C. G. (2019). *E-commerce: Business, technology, society* (15th ed.).

Melo, L. P., et al. (2024). A secure approach out-of-band for e-bank with visual two-factor authorization protocol. *Cryptography*.

Pearson.NIST. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B).

National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Otoritas Jasa Keuangan. (2025). *Data kasus Account Take Over (ATO) Januari 2024–Januari 2025*. Otoritas Jasa Keuangan. Dikutip dalam finance.detik.com, 24 Februari 2026.

Qadriah, L., Achmady, S., & Husaini. (2023). Sistem pengamanan dokumen dengan algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentication (2FA). *Jurnal Sistem Informasi*, *9*(1). https://doi.org/10.34128/jsi.v9i1.519

Putra, F. P. E., Ubaidi, Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of phishing attack trends, impacts and prevention methods: Literature study. *Brilliance: Research of Artificial Intelligence*, *4*(1), 413–421. https://doi.org/10.47709/brilliance.v4i1.4357

Radiansyah, I., Candiwan, & Priyadi, Y. (2016). Analisis ancaman phishing dalam layanan online banking. *Ekonomika-Bisnis*, *7*(1), 1–14.

Ramakrishnan, R., & Gehrke, J. (2003). *Database management systems* (3rd ed.). McGraw-Hill.

Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61–78. https://doi.org/10.21512/jas.v4i1.967

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

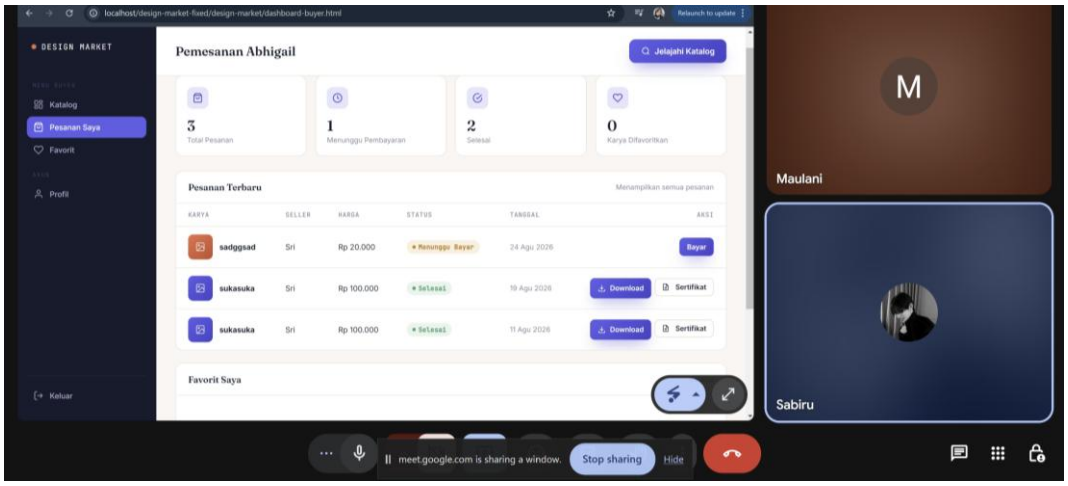
TintaHijau.com. (2025, October 16). *Belasan pedagang pujasera di Bandung jadi korban QRIS palsu, kerugian capai jutaan rupiah*. https://www.tintahijau.com/megapolitan/belasan-pedagang-pujasera-di-bandung-jadi-korban-qris-palsu-kerugian-capai-jutaan-rupiah/

Turban, E., Outland, J., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2018). *Electronic commerce 2018: A managerial and social networks perspective* (9th ed.). Springer.

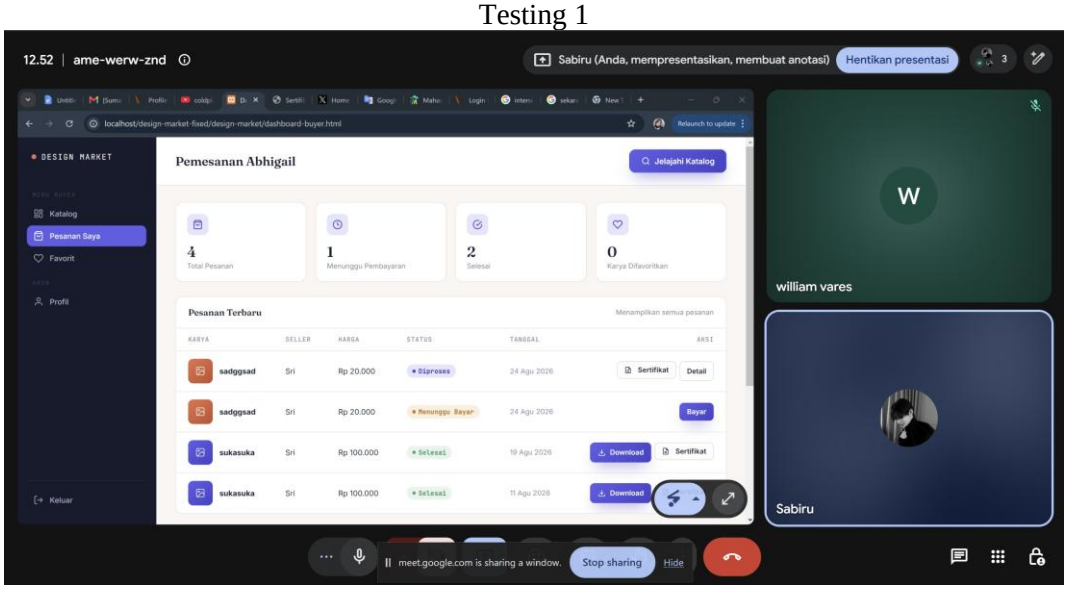
Wijoyo, A., Saputra, A., Aditia, Pratama, M. R. A., & Rahman, R. (2023). Analisis serangan phising dan strategi deteksinya. *JRIIN: Jurnal Riset Informatika dan Inovasi*, *1*(4). https://journal.mediapublikasi.id/index.php/jriin

LAMPIRAN A

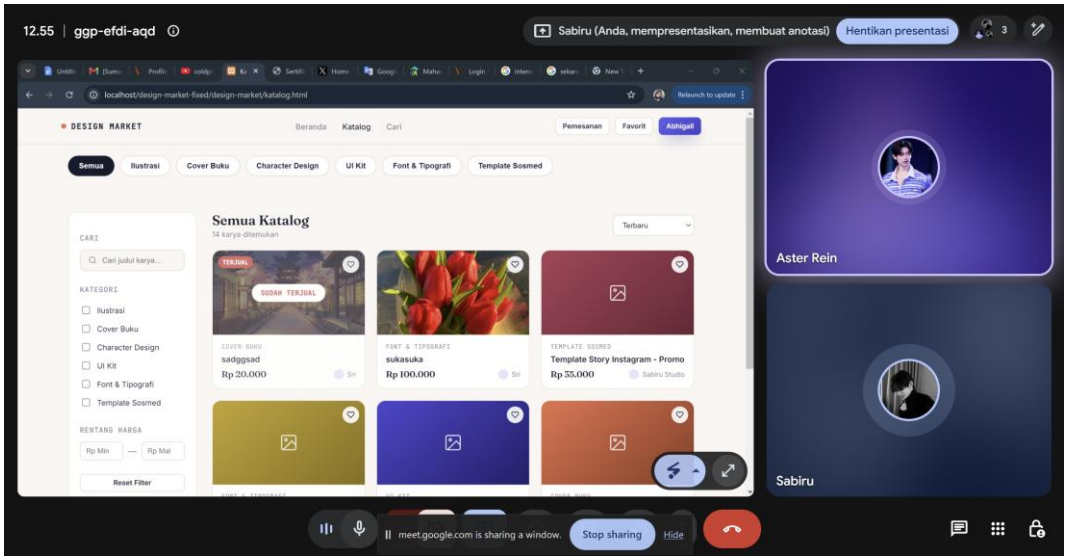
Pengujian



Testing 1



Testing 2


12.55 | ggp-efdi-aqd
Sabiru (Anda, mempresentasikan, membuat anotasi)
Hentikan presentasi
DESIGN MARKET
Beranda
Katalog
Cari
Pemesanan
Favorit
Abhigail
Semua
Ilustrasi
Cover Buku
Character Design
UI Kit
Font & Tipografi
Template Sosmed
Semua Katalog
14 karya ditemukan
Terbaru
CARI
KATEGORI
RENTANG HARGA
Reset Filter
TERJUAL
SUDAH TERJUAL
sadggsad
Rp 20.000
sukasuka
Rp 100.000
Template Story Instagram - Promo
Rp 35.000
Aster Rein
Sabiru
meet.google.com is sharing a window.
Stop sharing
Hide

Testing 3