Online Payments Processing Platform

Owner: A development team
Reviewer: A security architect
Contributors: development engineers, product managers, security architects
Date Generated: Tue Oct 07 2025

Executive Summary

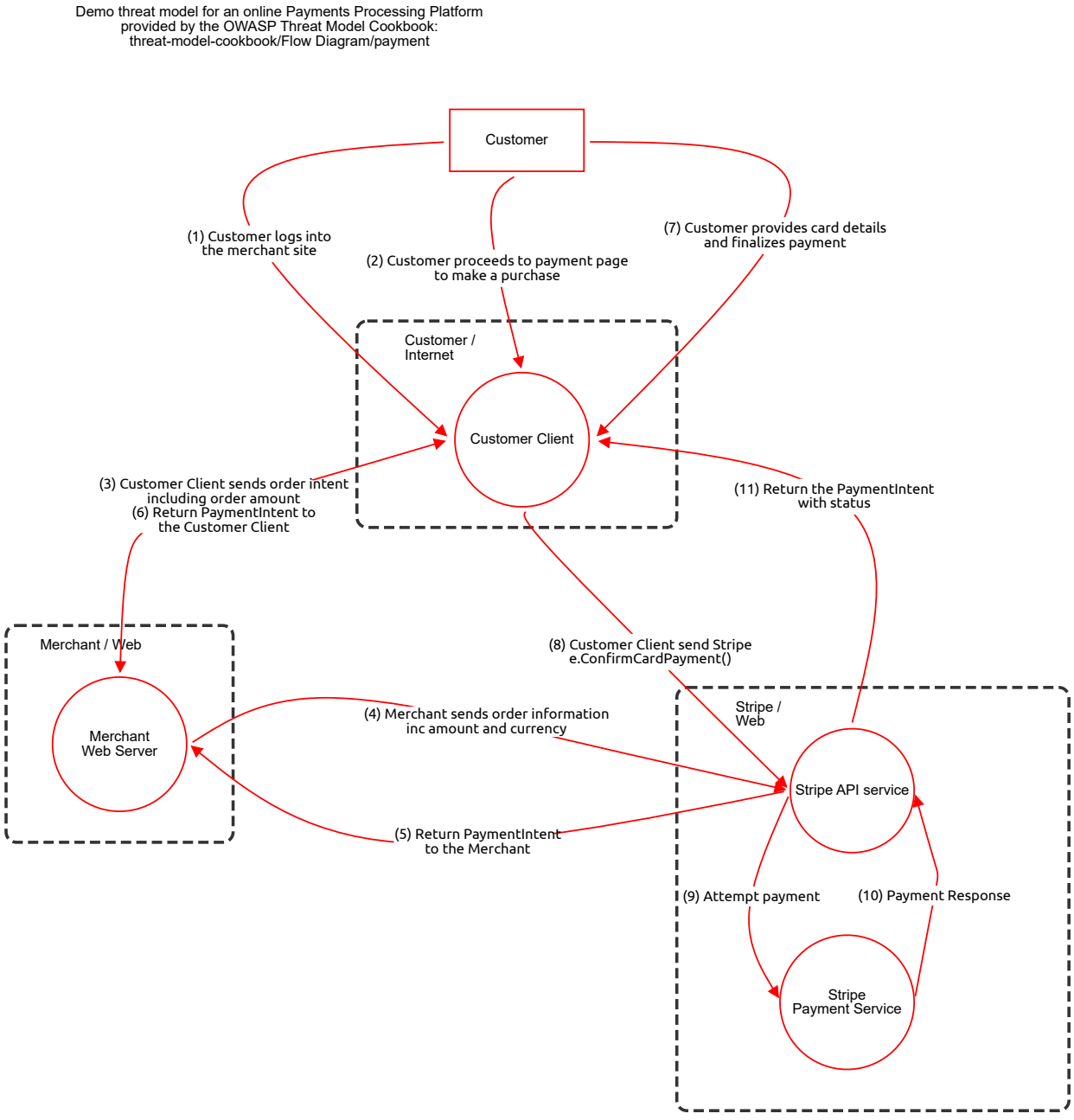
High level system description

This threat model has been provided by the OWASP Threat Model Cookbook:
threat-model-cookbook/Flow Diagram/payment

Summary

Total Threats	20
Total Mitigated	0
Total Open	20
Open / Critical Severity	0
Open / High Severity	15
Open / Medium Severity	5
Open / Low Severity	0

Payment


Demo threat model for an online Payments Processing Platform
provided by the OWASP Threat Model Cookbook:
threat-model-cookbook/Flow Diagram/payment
Customer
(1) Customer logs into
the merchant site
(2) Customer proceeds to payment page
to make a purchase
(7) Customer provides card details
and finalizes payment
Customer /
Internet
Customer Client
(3) Customer Client sends order intent
including order amount
(6) Return PaymentIntent to
the Customer Client
(11) Return the PaymentIntent
with status
Merchant / Web
Merchant
Web Server
(8) Customer Client send Stripe
e.ConfirmCardPayment()
(4) Merchant sends order information
inc amount and currency
(5) Return PaymentIntent
to the Merchant
Stripe /
Web
Stripe API service
(9) Attempt payment
(10) Payment Response
Stripe
Payment Service

Payment

Customer (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Authentication Data Intercepted	Spoofing	High	Open		Customer actor provides authentication credentials over potentially unencrypted channels to the Customer Client. This can lead to spoofing if intercepted.	Enforce end-to-end encryption (e.g., HTTPS/TLS 1.3) for all authentication flows and implement multi-factor authentication (MFA).
	Sensitive Data Exposure	Information Disclosure	High	Open		Customer actor communicates with Customer Client over public networks without encryption, exposing sensitive data to potential disclosure.	Ensure all communication between Customer and Customer Client is encrypted using strong protocols like TLS 1.3.

Customer Client (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Communication with External Services	Tampering	High	Open		Customer Client communicates with external services (Stripe) without encryption, increasing risk of data tampering or interception.	Enforce TLS 1.2+ for all external API communications and validate server certificates.
	Lack of Non-Repudiation Controls	Repudiation	Medium	Open		Customer Client handles payment-related data but lacks sufficient logging or audit capabilities, enabling repudiation of actions.	Implement comprehensive audit logging for all payment-related operations and ensure logs are immutable and centrally stored.

(1) Customer logs into the merchant site (Data Flow)

Description: OAuth

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Authentication Flow	Information Disclosure	High	Open		Flow from Customer to Customer Client for login is not encrypted, exposing credentials to interception on public or untrusted networks.	Enforce HTTPS/TLS 1.3 for all authentication flows and implement certificate pinning where applicable.

(2) Customer proceeds to payment page to make a purchase (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Payment Initiation Flow	Information Disclosure	High	Open		Flow from Customer to Customer Client for payment initiation is not encrypted, exposing transaction details to interception.	Enforce HTTPS/TLS 1.3 for all transaction-related flows and implement secure session management.

(7) Customer provides card details and finalizes payment (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Card Details Entry	Information Disclosure	High	Open		Flow from Customer to Customer Client for card details entry is not encrypted, exposing sensitive payment data.	Enforce HTTPS/TLS 1.3 and use secure input fields with client-side validation and masking.

(3) Customer Client sends order intent including order amount (6) Return PaymentIntent to the Customer Client (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Order Intent Exchange	Information Disclosure	High	Open		Bidirectional flow between Customer Client and Merchant Web Server lacks encryption, exposing order data to interception.	Enforce mutual TLS (mTLS) authentication and encryption for all internal API communications.

(9) Attempt payment (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Payment Attempt Flow	Information Disclosure	High	Open		Flow from Customer Client to Stripe API service for payment attempt is not encrypted, exposing transaction data.	Enforce HTTPS/TLS 1.3 for all payment processing communications and validate API responses.

(10) Payment Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Payment Response Flow	Information Disclosure	Medium	Open		Flow from Stripe Payment Service to Stripe API service for payment response is not encrypted, exposing transaction status.	Enforce HTTPS/TLS 1.3 for all internal service communications and implement message authentication codes (MACs).

(11) Return the PaymentIntent with status (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Payment Status Return	Information Disclosure	High	Open		Flow from Stripe API service to Customer Client for payment status is not encrypted, exposing sensitive transaction data.	Enforce HTTPS/TLS 1.3 for all client-facing communications and implement secure session tokens.

(8) Customer Client send Stripe e.ConfirmCardPayment() (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Card Confirmation Flow	Information Disclosure	High	Open		Flow from Customer Client to Stripe API service for card confirmation is not encrypted, exposing payment credentials.	Enforce HTTPS/TLS 1.3 and use secure tokenization for card data handling.

(5) Return PaymentIntent to the Merchant (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Payment Intent Return	Information Disclosure	High	Open		Flow from Stripe API service to Merchant Web Server for payment intent return is not encrypted, exposing transaction data.	Enforce HTTPS/TLS 1.3 for all merchant-facing communications and implement secure session tokens.

(4) Merchant sends order information inc amount and currency (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Order Information Flow	Information Disclosure	High	Open		Flow from Merchant Web Server to Stripe API service for order information is not encrypted, exposing transaction data.	Enforce HTTPS/TLS 1.3 for all merchant-to-payment service communications and implement secure session tokens.

Merchant Web Server (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Communication with External Services	Tampering	High	Open		Merchant Web Server communicates with external services without encryption, increasing risk of data tampering or interception.	Enforce TLS 1.2+ for all external API communications and validate server certificates.
	Lack of Non-Repudiation Controls	Repudiation	Medium	Open		Merchant Web Server handles payment-related data but lacks sufficient logging or audit capabilities, enabling repudiation of actions.	Implement comprehensive audit logging for all payment-related operations and ensure logs are immutable and centrally stored.

Stripe API service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Communication with External Clients	Tampering	High	Open		Stripe API service communicates with external clients without encryption, increasing risk of data tampering or interception.	Enforce TLS 1.2+ for all external API communications and validate client certificates.
	Lack of Non-Repudiation Controls	Repudiation	Medium	Open		Stripe API service handles payment-related data but lacks sufficient logging or audit capabilities, enabling repudiation of actions.	Implement comprehensive audit logging for all payment-related operations and ensure logs are immutable and centrally stored.

Stripe Payment Service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	Unencrypted Communication with External Services	Tampering	High	Open		Stripe Payment Service communicates with external services without encryption, increasing risk of data tampering or interception.	Enforce TLS 1.2+ for all external API communications and validate server certificates.
	Lack of Non-Repudiation Controls	Repudiation	Medium	Open		Stripe Payment Service handles payment-related data but lacks sufficient logging or audit capabilities, enabling repudiation of actions.	Implement comprehensive audit logging for all payment-related operations and ensure logs are immutable and centrally stored.