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

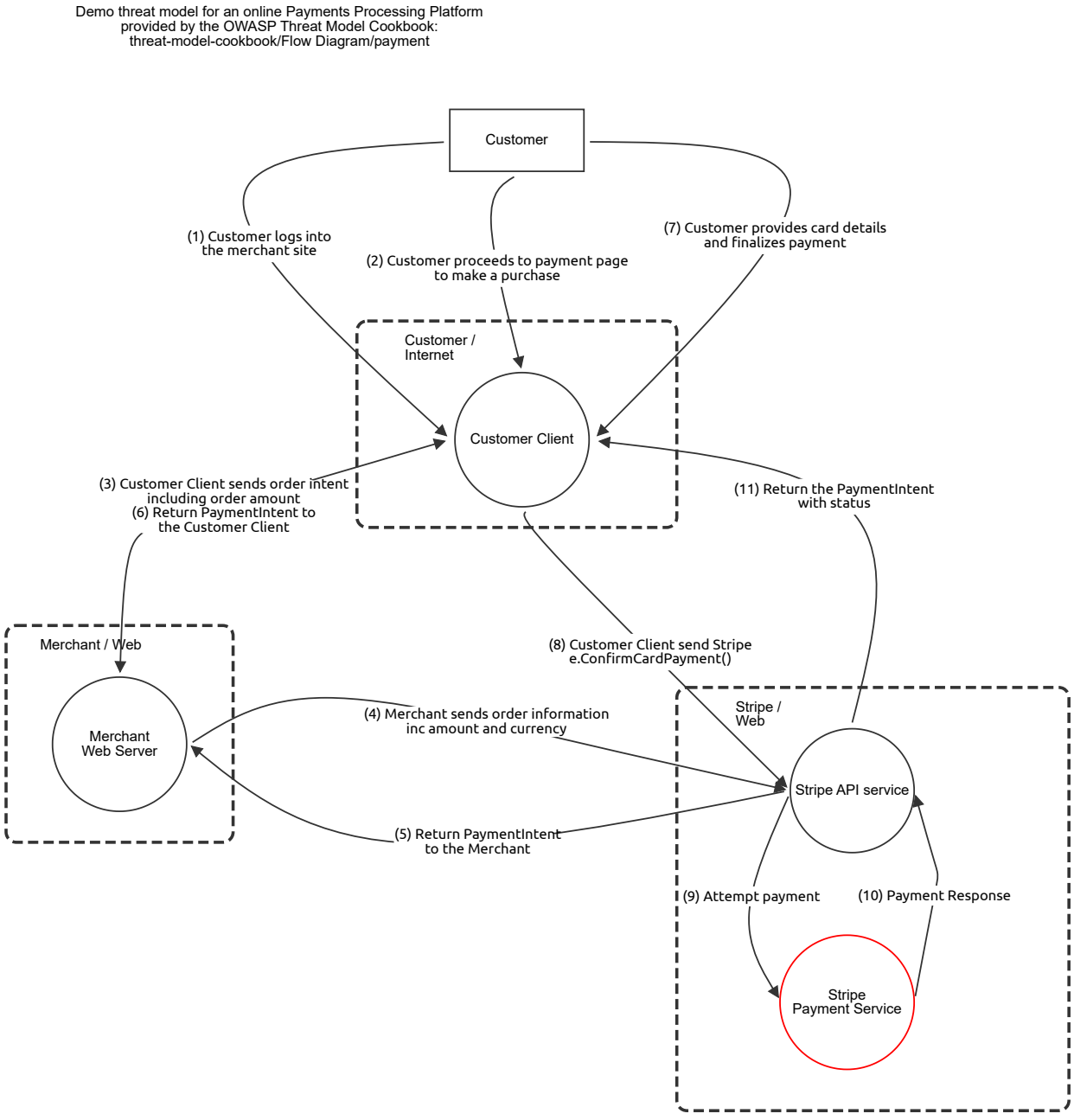
High level system description

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

Summary

Total Threats	1
Total Mitigated	0
Total Open	1
Open / Critical Severity	0
Open / High Severity	1
Open / Medium Severity	0
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

Customer Client (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

Description: OAuth

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations

(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

(9) Attempt payment (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

(10) Payment Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations

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

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Merchant Web Server (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Stripe API service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Stripe Payment Service (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
	External Data Exposure via Unencrypted Flow	Information Disclosure	High	Open		The Stripe Payment Service (id: 91a72b16-b05b-463a-b0c6-62fa2dd0f72b) transmits sensitive payment data over an unencrypted public network (data.isPublicNetwork=true, data.isEncrypted=false), risking data interception and disclosure.	Implement TLS 1.2+ for all external data transmissions; enforce mTLS to secure external communications.