Online Banking Application Threat Model

Owner: Andrew Morgan
Reviewer: Pluralsight viewers
Contributors:
Date Generated: Mon Jun 10 2024

Executive Summary

High level system description

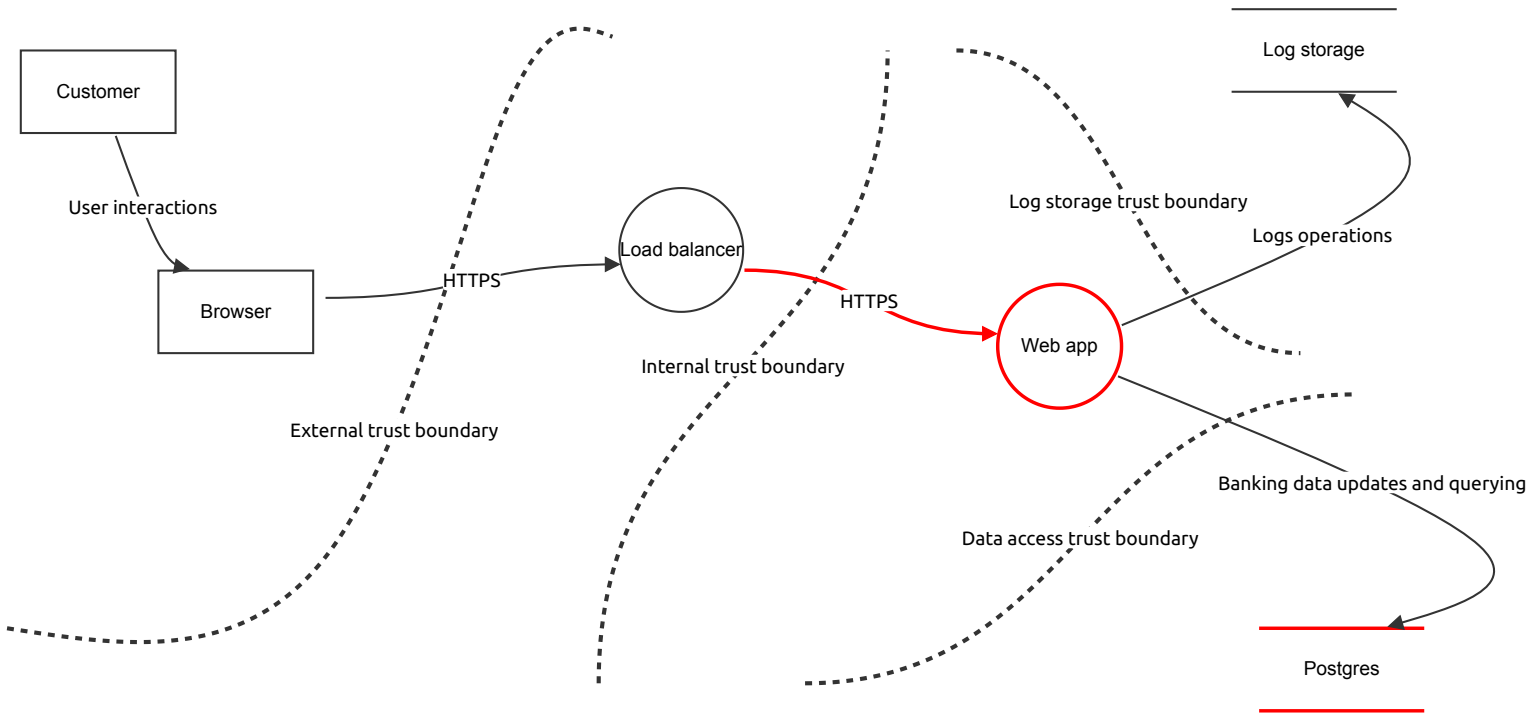
A Spring Boogt retail banking application.

Summary

Total Threats	10
Total Mitigated	3
Not Mitigated	7
Open / High Priority	1
Open / Medium Priority	6
Open / Low Priority	0
Open / Unknown Priority	0

High-level System Diagram

Overview of the key application components and data flow



High-level System Diagram

Web app (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	Load balancer bypassing	Spoofing	High	Open		Once inside the network, an attacker can call the web application directly, spoofing the load balancer and bypassing any security controls implemented within the load balancer.	- MTLS between the load balancer and the application.
14	Denying transactions	Repudiation	Medium	Open		The user denies having made a particular transaction.	Store all transaction date in logs.
15	Gains administrative access	Elevation of privilege	Medium	Open		An attacker exploits a vulnerability in the banking application to gain administrative access.	- Apply the least privilige principle to all authenticated users. - Implement strict role-based access control for all interactions with the system.
17	Compromised password	Spoofing	Medium	Open		Attacker logs in using another users leaked password	- MFA - Storing passwords securely with salts and expensive hashing algorithm - Testing passwords against known passwords

Postgres (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	Data breach of all user data	Information disclosure	Medium	Open		Bad actor accesses the database and is able to view all user data.	- Use encryption at rest - Regularly rotate encryption keys and set expiry - Strict access controls for data access

Customer (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User interactions (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Banking data updates and querying (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Logs operation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

HTTPS (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	MITM Attack Data Tampering	Tampering	High	Mitigated		MITM attacks could be used to intercept financial data coming or being return to the user.	Use HTTPS with a signed certificate in load balancer.
7	MITM Attack Data Viewing	Information disclosure	High	Mitigated		A MITM attack can be used to intercept private financial data.	Use HTTPS with a signed certificate in load balancer.

HTTPS (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	MITM Attack Data Tampering	Tampering	Medium	Open		MITM attacks could be used to modify financial data coming or being return to the user.	Re-encrypt HTTPS using a signed certificate between load balancer and application.
10	MITM Attack Data Viewing	Tampering	Medium	Open		A MITM attack can be used to view private financial data.	Re-encrypt HTTPS using a signed certificate between load balancer and application.

Load balancer (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	DDOS Attack	Denial of service	High	Mitigated		System unable to respond due to overwhelming number of requests	Use rate limiting solution offered by Cloud provider.

Log storage (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations