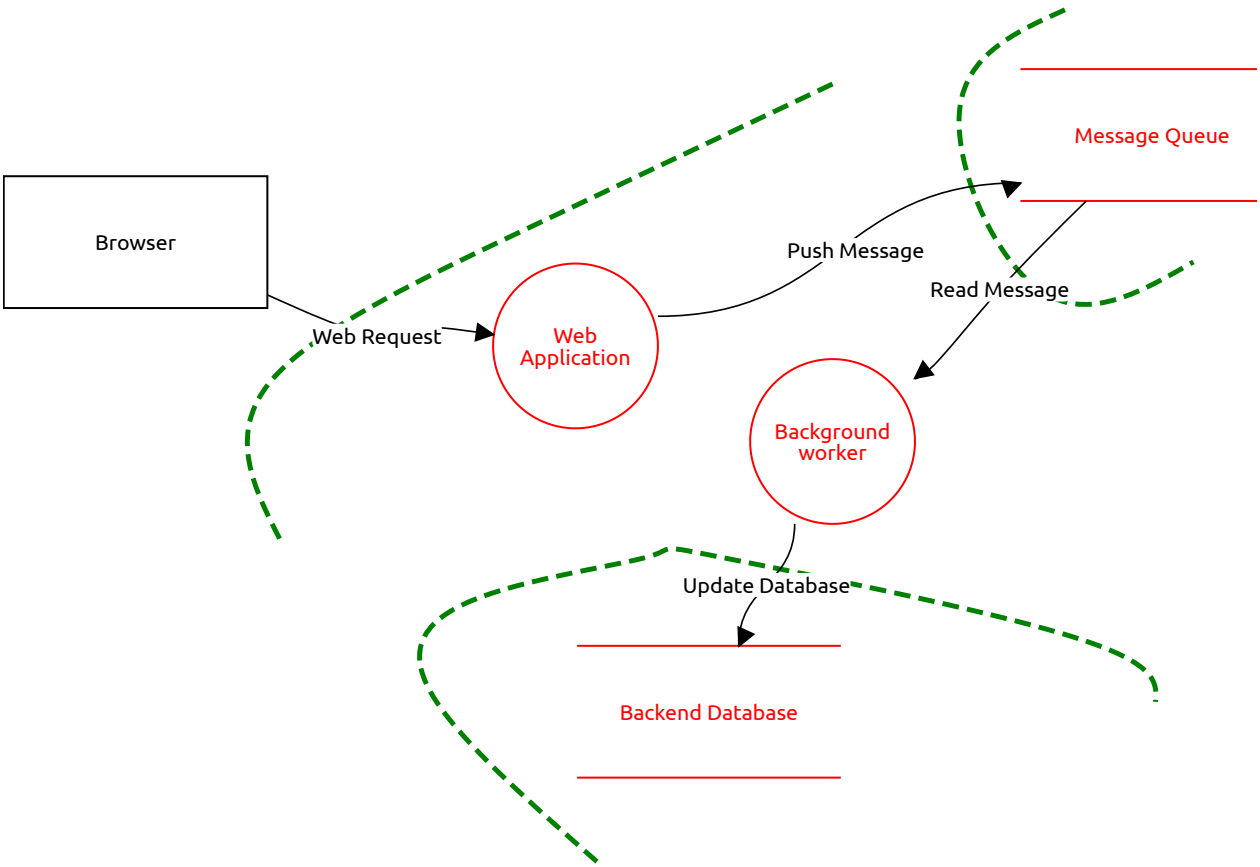
Threat model report for First Threat Model

Owner:
Pravin
Reviewer:
Pravin
Contributors:

High level system description

First Threat Model

Threat diagram



Browser (External Actor)

Description:

No threats listed.

Web Application (Process)

Description:

Comprimise user account

Spoofing, Open, High Severity

Description:
An attacker could send a request pretending to be another person and access that person’s data.

Mitigation:
Implement Multi-factor authentication.

Backend Database (Data Store)

Description:

Unauthorized access

Information disclosure, Open, High Severity

Description:
An attacker could make an query call on the DB to retrive data that is private, confidential & controlled data.

Mitigation:
Authenticate all queries & sanitize SQL injection payloads

Tampering Data In Use

Tampering, Open, Medium Severity

Description:
An attacker could modify an account number in the database to divert payment to their own account.

Mitigation:
Restrict access to the database using a firewall.

Covering the tracks

Repudiation, Open, Medium Severity

Description:
Attacker can cover the unauthorized actions

Mitigation:
Log all changes to bank account numbers and audit the changes.

Web Request (Data Flow)

Description:

No threats listed.

Background worker (Process)

Description:

Poison Message

Denial of service, Open, Medium Severity

Description:
An attacker could generate a malicious message that the Background Worker cannoy process.

Mitigation:
Maintain a retry count on message and discard them after three retries.

Message Queue (Data Store)

Description:

Message secrecy

Information disclosure, Open, Medium Severity

Description:
Messages could be read by an attacker at rest in the Message Queue.

Mitigation:
Use message level encryption for high sensitivity data (eg. security tokens) in messages.

Message Tampering

Tampering, Open, Medium Severity

Description:
Once Message on the queue are disclosed then attacker can tamper the messages on the queue.

Mitigation:
Digitally sign message on the queue and validate their signature before processing.

Push Message (Data Flow)

Description:

No threats listed.

Read Message (Data Flow)

Description:

No threats listed.

Update Database (Data Flow)

Description:

No threats listed.