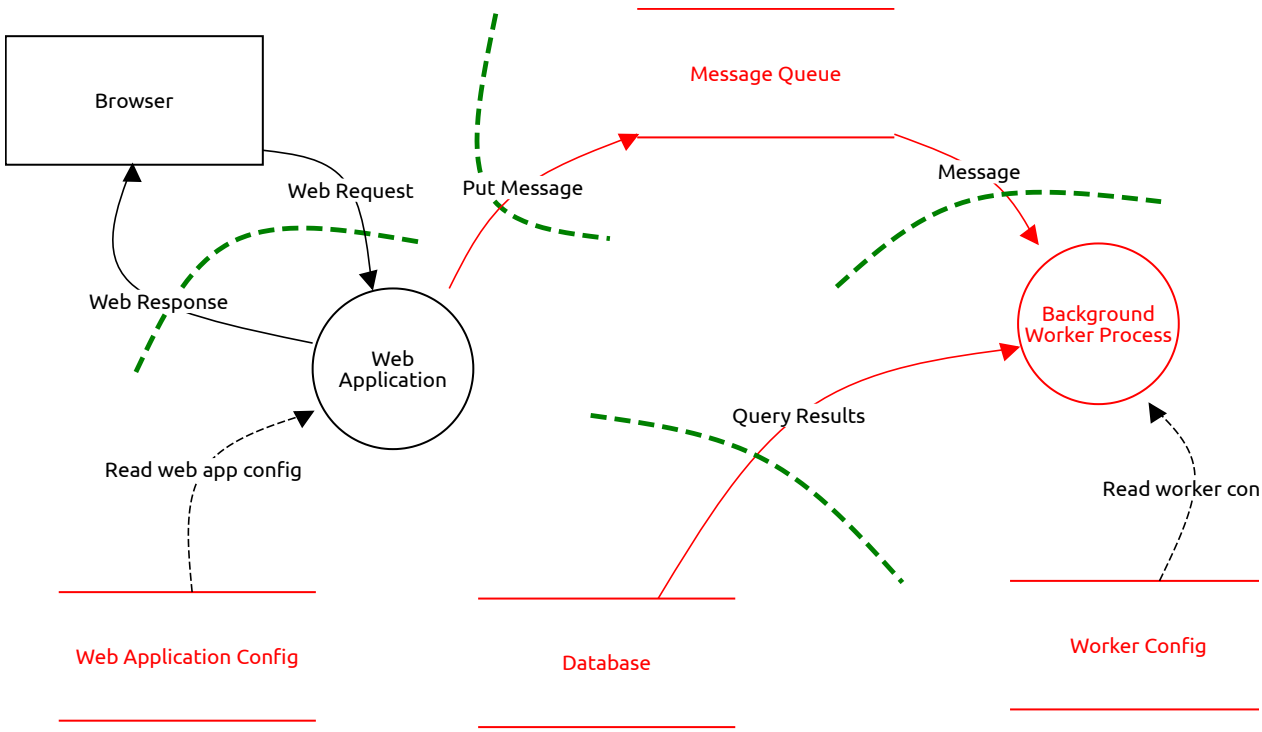
Threat model report for Demo Threat Model

Owner:
Mike Goodwin
Reviewer:
Jane Smith
Contributors:
Tom Brown

High level system description

A sample model of a web application, with a queue-decoupled background process.

Main Request Flow



Worker Config (Data Store)

Description:

Accessing DB credentials

Information disclosure, Open, High Severity

Description:
The Background Worker configuration stores the credentials used by the worker to access the DB. An attacker could compromise the Background Worker and get access to the DB credentials.

Mitigation:
Encrypt the DB credentials in the configuration file.

Expire and replace the DB credentials regularly.

Database (Data Store)

Description:

Unauthorised access

Information disclosure, Mitigated, High Severity

Description:
An attacker could make an query call on the DB,

Mitigation:
Require all queries to be authenticated.

Credential theft

Information disclosure, Open, Medium Severity

Description:
An attacker could obtain the DB credentials ans use them to make unauthorised queries.

Mitigation:
Use a firewall to restrict access to the DB to only the Background Worker IP address.

Web Application Config (Data Store)

Description:

Credentials should be encrypted

Information disclosure, Open, High Severity

Description:
The Web Application Config stores credentials used by the Web App to access the message queue. These could be stolen by an attacker and used to read confidential data or place poison message on the queue.

Mitigation:
The Message Queue credentials should be encrypted.

Message Queue (Data Store)

Description:

Message secrecy
Information disclosure, Open, Low Severity

Description:
The data flow between the Web Application and the Background Worker is not point-to-point and therefore end-to-end secrecy cannot be provided at the transport layer. Messages could be read by an attacker at rest in the Message Queue.

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

Message tampering
Tampering, Open, Medium Severity

Description:
Messages on the queue could be tampered with, causing incorrect processing by the Background Worker.

Mitigation:
Sign all queue messages at the Web Server. Validate the message signature at the Background Worker and reject any message with a missing or invalid signature. Log any failed messages.

Fake messages could be placed on the queue
Spoofing, Mitigated, High Severity

Description:

An attacker could put a fake message on queue, causing the Background Worker to do incorrect processing.

Mitigation:
Restrict access to the queue to the IP addresses of the Web Server and Background Worker.

Implement authentication on the queue endpoint.

Background Worker Process (Process)

Description:

Poison messages 1

Denial of service, Open, Medium Severity

Description:
An attacker could generate a malicious message that the Background Worker cannot process.

Mitigation:
Implement a poison message queue where messages are placed after a fixed number of retries.

Poison messages 2

Denial of service, Open, Medium Severity

Description:
An attacker could generate a malicious message that the Background Worker cannot process.

Mitigation:
Validate the content of all messages, before processing. Reject any message that have invalid content and log the rejection. Do not log the malicious content - instead log a description of the error.

Web Application (Process)

Description:

No threats listed.

Browser (External Actor)

Description:

No threats listed.

Web Request (Data Flow)

Description:

Data flow should use HTTP/S

Information disclosure, Mitigated, High Severity

Description:
These requests are made over the public internet and could be intercepted by an attacker.

Mitigation:
The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Put Message (Data Flow)

Description:

Data flow should use HTTP/S

Information disclosure, Open, High Severity

Description:
These requests are made over the public internet and could be intercepted by an attacker.

Mitigation:
The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Message (Data Flow)

Description:

Data flow should use HTTP/S

Information disclosure, Open, High Severity

Description:
These requests are made over the public internet and could be intercepted by an attacker.

Mitigation:
The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Query Results (Data Flow)

Description:

Man in the middle attack

Information disclosure, Open, Low Severity

Description:
An attacker could intercept the DB queries in transit and obtain sensitive information, such as DB credentials, query parameters or query results (is unlikely since the data flow is over a private network).

Mitigation:
Enforce an encrypted connection at the DB server

Web Response (Data Flow)

Description:

Data flow should use HTTP/S

Information disclosure, Mitigated, High Severity

Description:
These responses are over the public internet and could be intercepted by an attacker.

Mitigation:
The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Read web app config (out of scope Data Flow)

Description:

Out of scope reason:
This data flow represents a read from the file system

Read worker config (out of scope Data Flow)

Description:

Out of scope reason:
This data flow represents a read from the file system