TruckMotion Threat Model

Owner: DESOFS 3
Reviewer: DESOFS 3
Contributors: Nuno Marmeleiro, Rogério Sousa, Óscar Folha, Rafael Oliveira, Rafael Faísca
Date Generated: Sun Apr 07 2024

OWASP Threat Dragon

Executive Summary

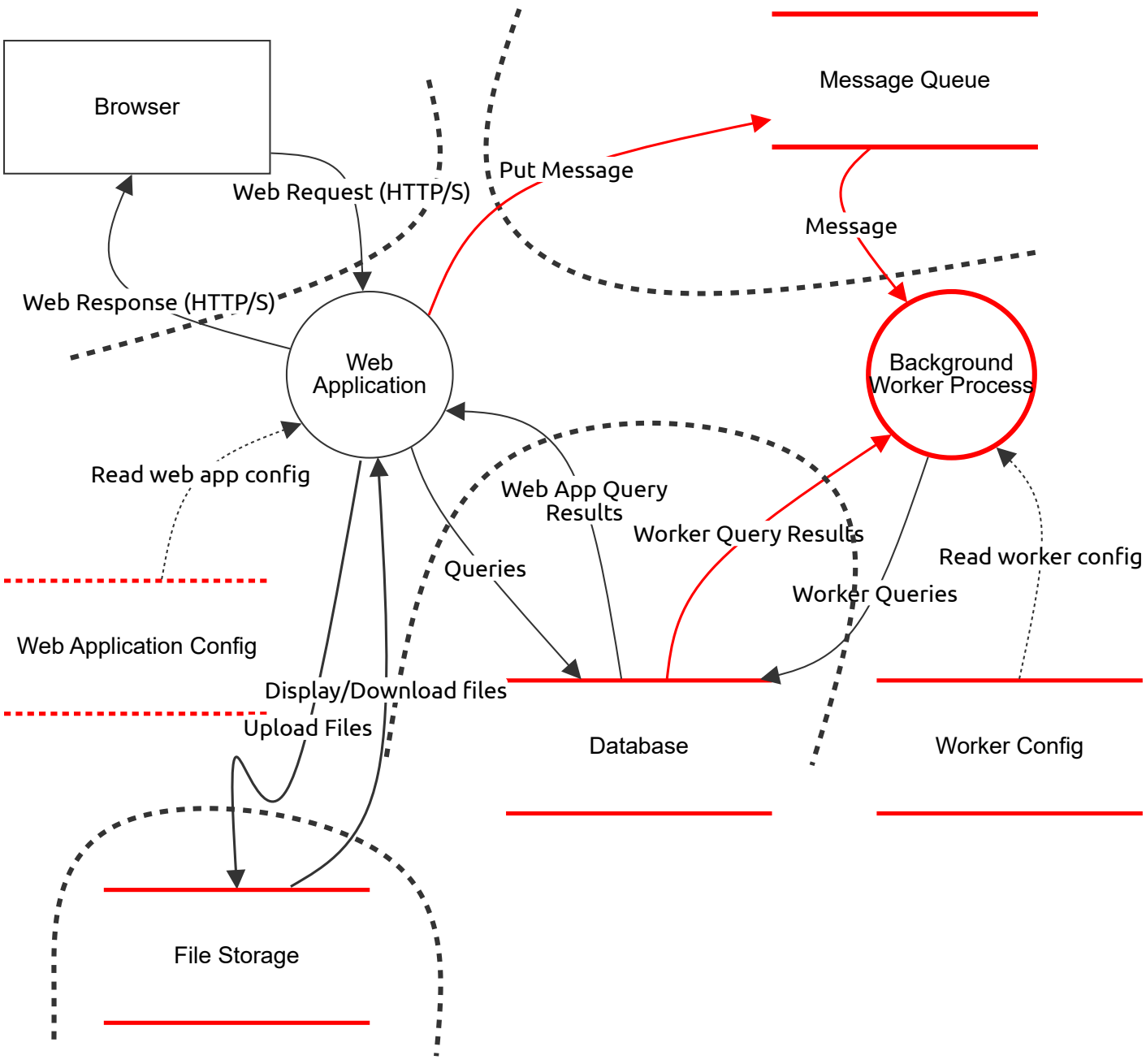
High level system description

Model for TruckMotion

Summary

Total Threats	15
Total Mitigated	4
Not Mitigated	11
Open / High Priority	5
Open / Medium Priority	4
Open / Low Priority	2
Open / Unknown Priority	0

Main Request Data Flow



Main Request Data Flow

Worker Config (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Accessing DB credentials	Information disclosure	High	Open		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.	Encrypt the DB credentials in the configuration file. Expire and replace the DB credentials regularly.

Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Unauthorised access	Information disclosure	High	Mitigated		An attacker could make an query call on the DB,	Require all queries to be authenticated.
	Credential theft	Information disclosure	Medium	Open		An attacker could obtain the DB credentials ans use them to make unauthorised queries.	Use a firewall to restrict access to the DB to only the Background Worker IP address.

Web Application Config (Store) - *Out of Scope*

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Credentials should be encrypted	Information disclosure	High	Open		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.	The Message Queue credentials should be encrypted.

Message Queue (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Message secrecy	Information disclosure	Low	Open		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.	Use message level encryption for high sensitivity data (e.g. security tokens) in messages.
	Message tampering	Tampering	Medium	Open		Messages on the queue could be tampered with, causing incorrect processing by the Background Worker.	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.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Fake messages could be placed on the queue	Spoofing	High	Mitigated		An attacker could put a fake message on queue, causing the Background Worker to do incorrect processing.	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)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Poison messages 1	Denial of service	Medium	Open		An attacker could generate a malicious message that the Background Worker cannot process.	Implement a poison message queue where messages are placed after a fixed number of retries.
	Poison messages 2	Denial of service	Medium	Open		An attacker could generate a malicious message that the Background Worker cannot process.	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)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Data flow should use HTTP/S	Information disclosure	High	Mitigated		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Put Message (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Data flow should use HTTP/S	Information disclosure	High	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Message (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Data flow should use HTTP/S	Information disclosure	High	Open		These requests are made over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Worker Query Results (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Man in the middle attack	Information disclosure	Low	Open		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).	Enforce an encrypted connection at the DB server

Web Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
	Data flow should use HTTP/S	Information disclosure	High	Mitigated		These responses are over the public internet and could be intercepted by an attacker.	The requests should require HTTP/S. This will provide confidentiality and integrity. HTTP should not be supported.

Read web app config (Data Flow) *- Out of Scope*

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Read worker config (Data Flow) *- Out of Scope*

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Queries (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web App Query Results (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Worker Queries (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Upload Files (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Display/Download files (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

File Storage (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Upload Malicious Files	Tampering	High	Open		By letting the application have a file upload system, the files need to be stored somewhere, in a physical system. This allows malicious users to upload files that are bad to tamper the server.	Provide remediation for this threat or a reason if status is N/A