Threat_Model_monlift

Owner: Romaric Sonkoue
Reviewer: Mouhamad Diack
Contributors:
Date Generated: Thu May 11 2023

OWASP Threat Dragon

Executive Summary

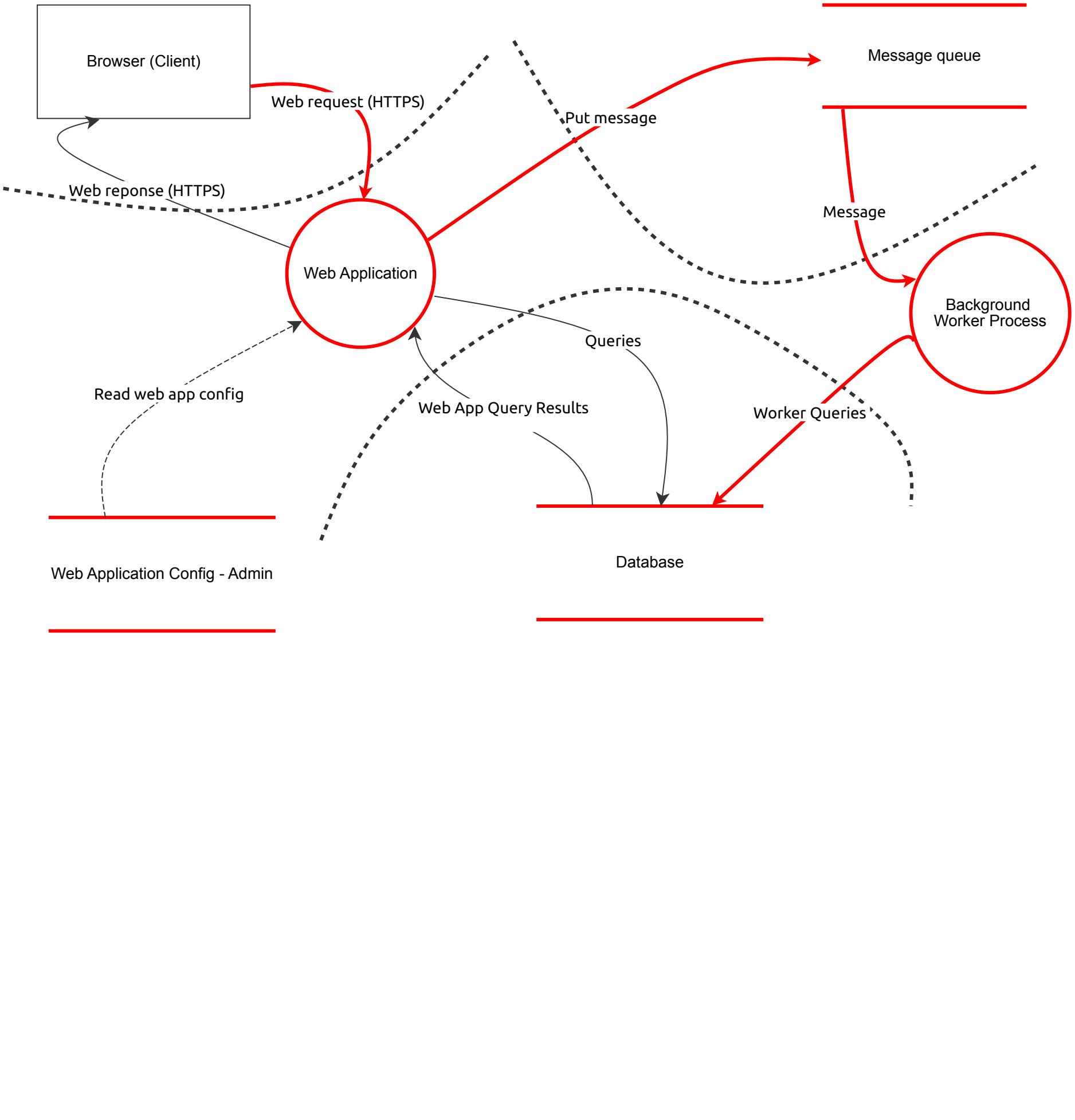
High level system description

Mon Lift est une plateforme de covoiturage au Canada disponible en version web et mobile . Elle permet aux conducteurs de proposer des trajets et aux passagers de réserver des places dans leur véhicule pour partager les frais de voyage. L'application offre également des fonctionnalités telles que la géolocalisation, la messagerie entre les utilisateurs et la notation des conducteurs et des passagers.

Summary

Total Threats	19
Total Mitigated	2
Not Mitigated	17
Open / High Priority	8
Open / Medium Priority	7
Open / Low Priority	2
Open / Unknown Priority	0

Monlift Diagram Threat



Monlift Diagram Threat

Web Application Config - Admin (Store)

Le web application config est un fichier de configuration qui permet de paramétrer différents aspects d'une application web.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Credentials should be encrypted	Information disclosure	High	Open		La configuration de l'application Web stocke les informations d'identification utilisées par l'application Web pour accéder à la file d'attente des messages. Ceux-ci pourraient être volés par un attaquant et utilisés pour lire des données confidentielles ou placer un message empoisonné dans la file d'attente.	Les informations d'identification de Message Queue doivent être chiffrées.

Database (Store)

C'est a ce niveau que sera stocker, organiser et gérer des données de manière structurée, afin de permettre leur accès et leur utilisation efficaces.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Unauthorised Access	Information disclosure	High	Open		Un attaquant pourrait effectuer un appel de requête sur la base de données	Exiger que toutes les requêtes soient authentifiées.
3	Credential theft	Information disclosure	Medium	Open		Un attaquant pourrait obtenir les informations d'identification de la base de données et les utiliser pour effectuer des requêtes non autorisées.	Utilisez un pare-feu pour limiter l'accès à la base de données à l'adresse IP du travailleur en arrière-plan uniquement.

Web Application (Process)

Cet partie est notre application logicielle proprement dit qui est accessible via un navigateur web.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
17	Perform regular penetration testing and security audits	Elevation of privilege	Medium	Open		Les tests de pénétration et les audits de sécurité réguliers permettent de détecter les vulnérabilités de sécurité avant qu'elles ne soient exploitées par des attaquants	Engager des experts en sécurité pour effectuer des tests de pénétration et des audits de sécurité
18	Regularly update the software	Information disclosure	Medium	Open			Il est important de maintenir Monlift à jour en appliquant les mises à jour et correctifs de sécurité publiés par les fournisseurs des paquets et des logiciels.

Message queue (Store)

Elle permet à notre application Monlift de communiquer de manière asynchrone en envoyant des messages à une file d'attente.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Message secrecy	Information disclosure	Low	Open		Le flux de données entre l'application Web et le travailleur d'arrière-plan n'est pas point à point et, par conséquent, le secret de bout en bout ne peut pas être fourni au niveau de la couche de transport. Les messages pourraient être lus par un attaquant au repos dans la file d'attente de messages.	Utilisez le chiffrement au niveau des messages pour les données à haute sensibilité (par exemple, les jetons de sécurité) dans les messages.
6	Message tampering	Tampering	Medium	Open		Les messages de la file d'attente pouvaient être falsifiés, ce qui entraînait un traitement incorrect par le travailleur en arrière-plan.	Signez tous les messages de la file d'attente sur le serveur Web. Validez la signature du message au niveau du Background Worker et rejetez tout message avec une signature manquante ou invalide. Enregistrez tous les messages ayant échoué.
7	Fake messages could be placed on the queue	Repudiation	High	Open		Un attaquant pourrait placer un faux message dans la file d'attente, ce qui obligerait le Background Worker à effectuer un traitement incorrect.	Limitez l'accès à la file d'attente aux adresses IP du serveur Web et du travailleur en arrière-plan. Implémentez l'authentification sur le point de terminaison de la file d'attente.

Background Worker Process (Process)

Ce processus s'exécutera en arrière-plan sans interférer avec l'exécution principale de l'application Monlift

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Poison messages 1	Denial of service	Medium	Open		Un attaquant pourrait générer un message malveillant que le Background Worker ne peut pas traiter.	Implémentez une file d'attente de messages incohérents dans laquelle les messages sont placés après un nombre fixe de tentatives.
10	Poison messages 2	Denial of service	Medium	Open		Un attaquant pourrait générer un message malveillant que le Background Worker ne peut pas traiter.	Validez le contenu de tous les messages, avant de les traiter. Rejetez tout message dont le contenu n'est pas valide et enregistrez le rejet. N'enregistrez pas le contenu malveillant - enregistrez plutôt une description de l'erreur.

Web request (HTTPS) (Data Flow)

Le client envoie des requêtes à l'application Monlift

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	Data flow should use HTTP/S	Information disclosure	High	Mitigated		Ces demandes sont faites sur le public Internet et pourrait être intercepté par un attaquant.	Les requêtes doivent nécessiter HTTP/S. Cela assurera la confidentialité et l'intégrité. HTTP ne doit pas être pris en charge.
13	Validate and filter user input	Denial of service	High	Open		Les attaques les plus courantes sur les applications web sont les injections de code, telles que les injections SQL et les injections de script entre autres.	Valider toutes les entrées utilisateur et filtrer les caractères spéciaux pour éviter que les attaquants ne puissent exploiter des vulnérabilités de sécurité.
14	Limit access permissions	Information disclosure	Medium	Open		Les attaquants peuvent utiliser l’accès non contrôlés pour initier des attaques sur l’application	Les autorisations d'accès doivent être limitées aux utilisateurs autorisés pour éviter les accès non autorisés et les fuites d'informations sensibles.
15	Manage user sessions	Information disclosure	High	Open		Les sessions utilisateur doivent être gérées de manière à éviter les attaques de vol de session.	Les techniques courantes pour cela incluent l'utilisation de cookies sécurisés et de jetons de session avec des délais d'expiration courts.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	Multi-Factor Authentification	Information disclosure	High	Open		MFA est une méthode d'authentification qui utilise plusieurs facteurs pour vérifier l'identité d'un utilisateur.	L'utilisateur doit généralement fournir son mot de passe ainsi que l'un des autres facteurs d'authentification. Par exemple, un utilisateur peut être invité à entrer son mot de passe, puis à saisir un code envoyé par SMS sur son téléphone portable.

Put message (Data Flow)

L'application transmet la requête a la fil d'attente

Number	Title	Type	Priority	Status	Score	Description	Mitigations
19	Data ow should use HTTP/S	Information disclosure	High	Open		Ces demandes sont faites sur l'Internet public et pourraient être interceptées par un attaquant.	Les requêtes doivent nécessiter HTTP/S. Cela assurera la confidentialité et l'intégrité. HTTP ne doit pas être pris en charge.

Message (Data Flow)

Le message est transmit au processus chargé de la gestion des process en arrière plan

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Data ow should use HTTP/S	Information disclosure	High	Open		Ces demandes sont faites sur l'Internet public et pourraient être interceptées par un attaquant.	Les requêtes doivent nécessiter HTTP/S. Cela assurera la confidentialité et l'intégrité. HTTP ne doit pas être pris en charge.

Web reponse (HTTPS) (Data Flow)

L’application Monlift répond a la requête du client

Number	Title	Type	Priority	Status	Score	Description	Mitigations
22	Data flow should use HTTP/S	Information disclosure	High	Mitigated		Ces réponses sont diffusées sur l'Internet public et pourraient être interceptées par un attaquant.	Les requêtes doivent nécessiter HTTP/S. Cela assurera la confidentialité et l'intégrité. HTTP ne doit pas être pris en charge.

Worker Queries (Data Flow)

La requête est envoyé du process de travailleur en arrière-plan vers la base de données

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	Man in the middle attack	Information disclosure	Low	Open		Un attaquant pourrait intercepter les requêtes de la base de données en transit et obtenir des informations sensibles, telles que les informations d'identification de la base de données, les paramètres de la requête ou les résultats de la requête.	Appliquer une connexion chiffrée au serveur de base de données