Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Wed Oct 16 2024

Executive Summary

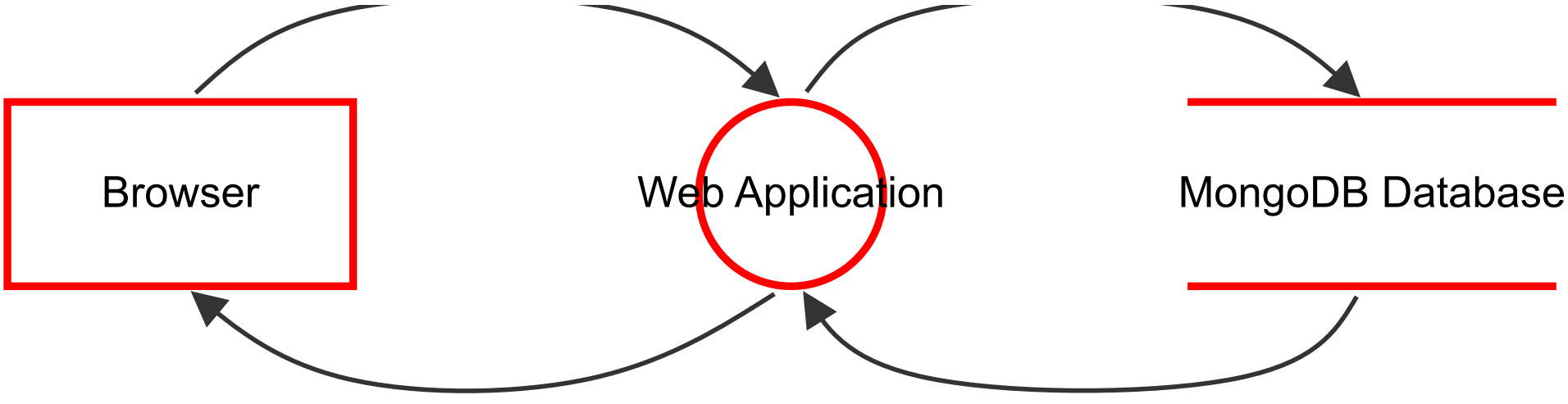
High level system description

Not provided

Summary

Total Threats	10
Total Mitigated	0
Not Mitigated	10
Open / High Priority	0
Open / Medium Priority	10
Open / Low Priority	0
Open / Unknown Priority	0

Waddle



Waddle

Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Зловмисник може отримати доступ до сеансу користувача через неправильний вихід із системи та тайм-аут	Spoofing	Medium	Open		Сеансові файли cookie — це ідентифікатор, за яким сервер дізнається особу поточного користувача для кожного вхідного запиту. Якщо зловмиснику вдасться викрасти маркер користувача, він зможе отримати доступ до всіх даних користувача та виконувати всі дії від імені користувача	Provide remediation for this threat or a reason if status is N/A

Web Application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Зловмисник може виконувати дії від імені іншого користувача через відсутність засобів контролю міждоменних запитів	Denial of service	Medium	Open		Неможливість обмежити запити, що надходять із доменів третіх сторін, може призвести до несанкціонованих дій або доступу до даних	Provide remediation for this threat or a reason if status is N/A
7	Зловмисник може змінити слабко зашифрований або хешований вміст	Information disclosure	Medium	Open		Зловмисник може змінити слабко зашифрований або хешований вміст	Provide remediation for this threat or a reason if status is N/A
8	Зловмисник викрадає повідомлення з мережі та відтворює їх, щоб викрасти сеанс користувача	Tampering	Medium	Open		Зловмисник викрадає повідомлення з мережі та відтворює їх, щоб викрасти сеанс користувача	Provide remediation for this threat or a reason if status is N/A
9	Зловмисник може отримати доступ до незамаскованих конфіденційних даних, таких як номери кредитних карток	Information disclosure	Medium	Open		Зловмисник може отримати доступ до незамаскованих конфіденційних даних, таких як номери кредитних карток	Provide remediation for this threat or a reason if status is N/A
10	Скомпрометований ключ доступу може надати зловмиснику більше доступу до екземпляра бази даних MongoDB, ніж це передбачено	Elevation of privilege	Medium	Open		Скомпрометований ключ доступу може дозволити зловмиснику отримати надто привілейований доступ до примірника бази даних MongoDB	Provide remediation for this threat or a reason if status is N/A
13	Зловмисник може підробити цільову веб-програму через незахищену конфігурацію сертифіката TLS	Spoofing	Medium	Open		Переконайтеся, що параметри сертифіката TLS налаштовані з правильними значеннями	Provide remediation for this threat or a reason if status is N/A

MongoDB Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
15	Зловмисник може заперечити зловмисну дію та видалити сліди атаки, що призводить до проблем із відмовою	Repudiation	Medium	Open		Правильна реєстрація всіх подій безпеки та дій користувача створює можливість відстеження в системі та усуває будь-які можливі проблеми відмови. За відсутності належного контролю аудиту та журналювання неможливо було б запровадити будь-яку підзвітність у системі	Provide remediation for this threat or a reason if status is N/A
16	Зловмисник може отримати доступ до конфіденційних даних, виконавши впровадження SQL через веб-додаток	Tampering	Medium	Open		SQL-ін’єкція – це атака, під час якої шкідливий код вставляється в рядки, які згодом передаються екземпляру SQL Server для аналізу та виконання. Основна форма SQL-ін’єкції полягає в прямому вставленні коду в змінні, що вводяться користувачем, які об’єднуються з командами SQL і виконуються. Менш пряма атака впроваджує шкідливий код у рядки, які призначені для зберігання в таблиці або як метадані. Коли збережені рядки згодом об’єднуються в динамічну команду SQL, виконується шкідливий код	Provide remediation for this threat or a reason if status is N/A
17	Зловмисник може отримати доступ до конфіденційних даних, що зберігаються у конфігураційних файлах веб-програми	Tampering	Medium	Open		Зловмисник може отримати доступ до конфігураційних файлів і якщо в ньому зберігаються конфіденційні дані, вони будуть скомпрометовані	Provide remediation for this threat or a reason if status is N/A

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations