Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Thu Oct 10 2024

Executive Summary

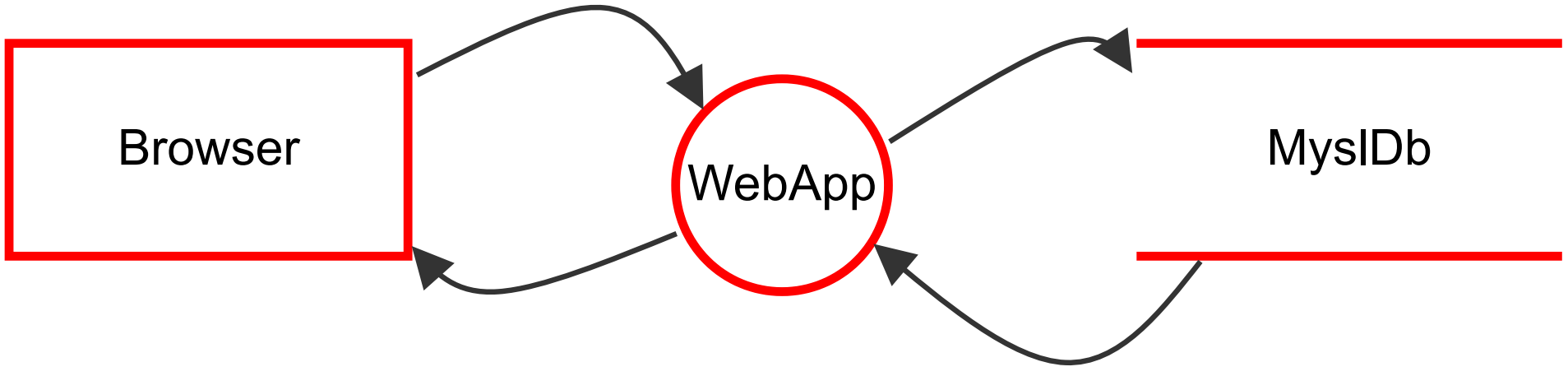
High level system description

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

cinemaworld



cinemaworld

MyslDb (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	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
2	Зловмисник може скрити 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
3	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
4	Зловмисник може використати відсутність систем моніторингу та викликати аномальний трафік до бази даних	Tampering	Medium	Open		Зловмисник може використати відсутність виявлення вторгнень і запобігання аномальній діяльності бази даних і викликати аномальний трафік до бази даних	Provide remediation for this threat or a reason if status is N/A

Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Зловмисник може отримати доступ до конфіденційної інформації через повідомлення про помилки	Spoofing	Medium	Open		Зловмисник може отримати доступ до таких конфіденційних даних, як наведені нижче, через докладні повідомлення про помилки - імена серверів - рядки підключення - імена користувачів - паролі - процедури SQL - подробиці динамічних помилок SQL - трасування стека та рядки коду - змінні, що зберігаються в пам'яті - диск і розташування папок - Точки встановлення програми - Параметри конфігурації хоста - Інші внутрішні деталі програми	Provide remediation for this threat or a reason if status is N/A

WebApp (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Зловмисник може отримати несанкціонований доступ до бази даних через відсутність захисту доступу до мережі	Elevation of privilege	Medium	Open		Якщо на рівні мережі чи брандмауера хоста немає обмежень для доступу до бази даних, будь-хто може спробувати підключитися до бази даних із неавторизованого місця	Provide remediation for this threat or a reason if status is N/A

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Зловмисник може обійти критичні кроки або виконати дії від імені інших користувачів (жертв) через неправильну логіку перевірки	Elevation of privilege	Medium	Open		Неможливість обмежити привілеї та права доступу до програми для осіб, яким потрібні привілеї чи права доступу, може призвести до несанкціонованого використання даних через неправильні налаштування прав і перевірку	Provide remediation for this threat or a reason if status is N/A
7	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
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 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

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations