Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Mon Oct 28 2024

Executive Summary

High level system description

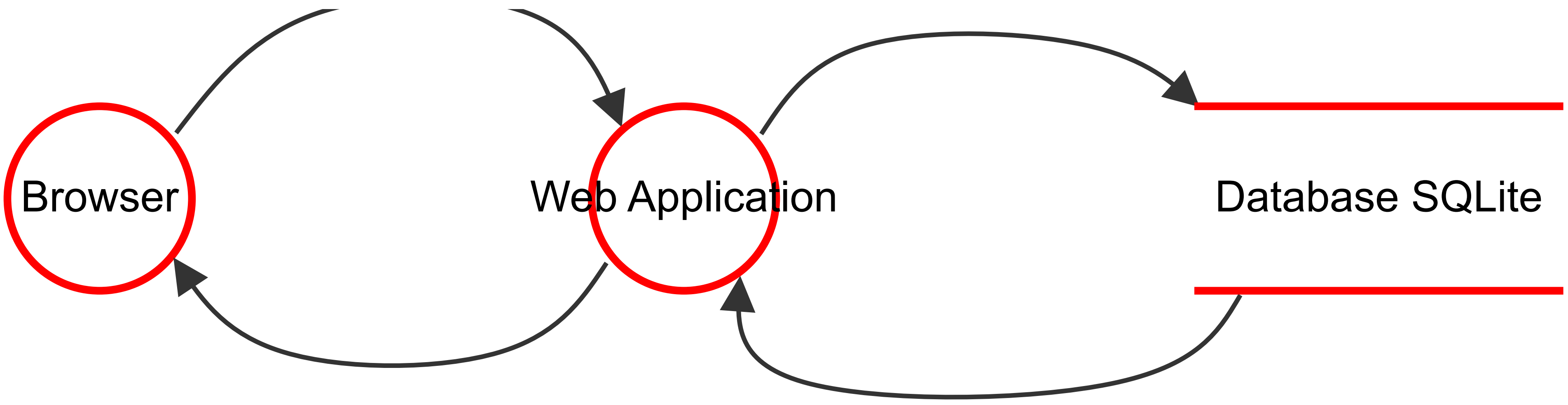
Not provided

Summary

Total Threats	11
Total Mitigated	0
Not Mitigated	11
Open / High Priority	0
Open / Medium Priority	11
Open / Low Priority	0
Open / Unknown Priority	0

Dragon_DFD

Smart Weather Hub



Dragon_DFD

Browser (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	An adversary can perform action on behalf of other user due to lack of controls against cross domain requests	Denial of service	Medium	Open		Failure to restrict requests originating from third party domains may result in unauthorized actions or access of data	Provide remediation for this threat or a reason if status is N/A
2	An adversary may bypass critical steps or perform actions on behalf of other users (victims) due to improper validation logic	Elevation of privilege	Medium	Open		Failure to restrict the privileges and access rights to the application to individuals who require the privileges or access rights may result into unauthorized use of data due to inappropriate rights settings and validation.	Provide remediation for this threat or a reason if status is N/A
3	An adversary can reverse weakly encrypted or hashed content	Information disclosure	Medium	Open		An adversary can reverse weakly encrypted or hashed content	Provide remediation for this threat or a reason if status is N/A
4	An adversary can steal sensitive data like user credentials	Spoofing	Medium	Open		Attackers can exploit weaknesses in system to steal user credentials. Downstream and upstream components are often accessed by using credentials stored in configuration stores. Attackers may steal the upstream or downstream component credentials. Attackers may steal credentials if; Credentials are stored and sent in clear text; Weak input validation coupled with dynamic sql queries; Password retrieval mechanism are poor;	Provide remediation for this threat or a reason if status is N/A
5	An attacker steals messages off the network and replays them in order to steal a user's session	Tampering	Medium	Open		An attacker steals messages off the network and replays them in order to steal a user's session	Provide remediation for this threat or a reason if status is N/A

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

(Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Database SQLite (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	An adversary can deny actions on database due to lack of auditing	Repudiation	Medium	Open		Proper logging of all security events and user actions builds traceability in a system and denies any possible repudiation issues. In the absence of proper auditing and logging controls; it would become impossible to implement any accountability in a system.	Provide remediation for this threat or a reason if status is N/A
8	An adversary may leverage the lack of monitoring systems and trigger anomalous traffic to database	Tampering	Medium	Open		An adversary may leverage the lack of intrusion detection and prevention of anomalous database activities and trigger anomalous traffic to database	Provide remediation for this threat or a reason if status is N/A
9	An adversary can reverse weakly encrypted or hashed content	Information disclosure	Medium	Open		An adversary can reverse weakly encrypted or hashed content	Provide remediation for this threat or a reason if status is N/A
10	New STRIDE threat	Denial of service	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Web Application (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	An adversary can gain unauthorized access to database due to loose authorization rules	Elevation of privilege	Medium	Open		Database access should be configured with roles and privilege based on least privilege and need to know principle.	Provide remediation for this threat or a reason if status is N/A
11	An adversary can spoof the target web application due to insecure TLS certificate configuration	Spoofing	Medium	Open		Ensure that TLS certificate parameters are configured with correct values	Provide remediation for this threat or a reason if status is N/A