Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Sun Nov 24 2024

Executive Summary

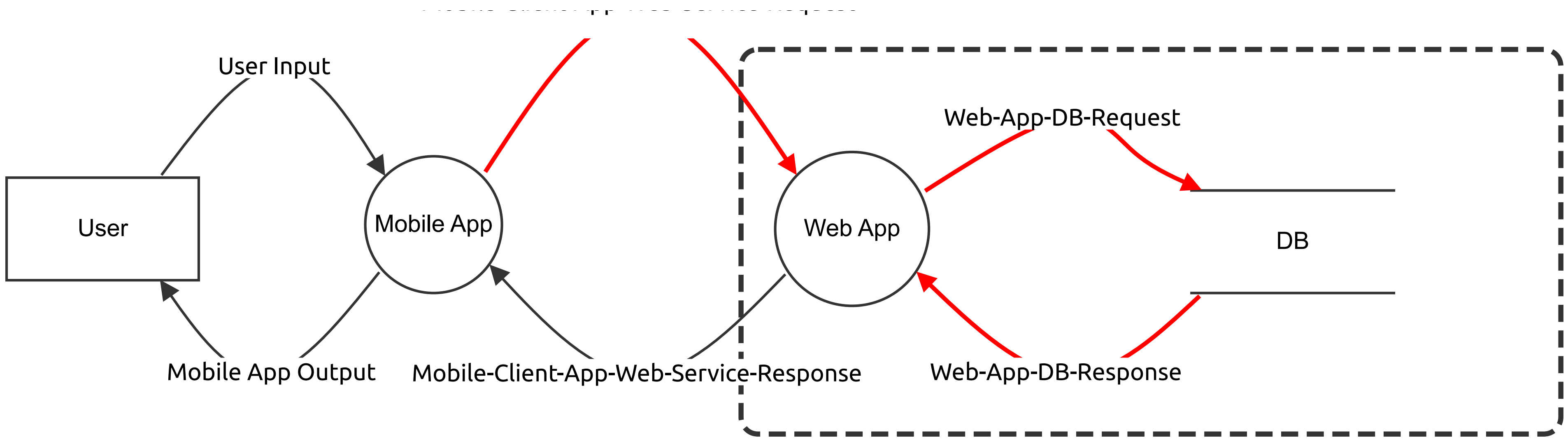
High level system description

Not provided

Summary

Total Threats	9
Total Mitigated	0
Not Mitigated	9
Open / High Priority	0
Open / Medium Priority	9
Open / Low Priority	0
Open / Unknown Priority	0

Rozrobka Android-dodatku dlia zapysu na biuti-servisy



Rozrobka Android-dodatku dlia zapysu na biuti-servisy

User (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web App (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DB (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Mobile App (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User Input (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Mobile-Client-App-Web-Service-Request (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Elevation of Privileges	Tampering	Medium	Open		An adversary may jail break into a mobile device and gain elevated privileges	Provide remediation for this threat or a reason if status is N/A
4	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
5	An adversary can spoof the target web application due to insecure TLS certificate configuration	Information disclosure	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

Web-App-DB-Request (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	An adversary can gain unauthorized access to Azure SQL database due to weak account policy	Tampering	Medium	Open		Due to poorly configured account policies, adversary can launch brute force attacks on Azure SQL Database	Provide remediation for this threat or a reason if status is N/A
7	An adversary can read confidential data due to weak connection string configuration	Information disclosure	Medium	Open		An adversary can read confidential data due to weak connection string configuration.	Provide remediation for this threat or a reason if status is N/A
8	An adversary can gain long term, persistent access to an Azure SQL DB instance through the compromise of local user account password(s)	Tampering	Medium	Open		An adversary can gain long term, persistent access to an Azure SQL DB instance through the compromise of local user account password(s).	Provide remediation for this threat or a reason if status is N/A
9	An adversary may abuse weak Azure SQL Database configuration	Tampering	Medium	Open		An adversary may abuse weak Azure SQL Database configuration	Provide remediation for this threat or a reason if status is N/A

Web-App-DB-Response (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	An adversary can reverse weakly encrypted or hashed content	Information disclosure	Medium	Open		An adversary may abuse weak Azure SQL Database configuration	Provide remediation for this threat or a reason if status is N/A
11	An adversary can gain access to sensitive data by performing SQL injection through Web App	Tampering	Medium	Open		SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.	Provide remediation for this threat or a reason if status is N/A

Mobile-Client-App-Web-Service-Response (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Mobile App Output (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations