Web-based User Feedback System

Owner: Christian Dela Pena
Reviewer: Christian Dela Pena
Contributors:
Date Generated: Thu Jan 30 2025

Executive Summary

High level system description

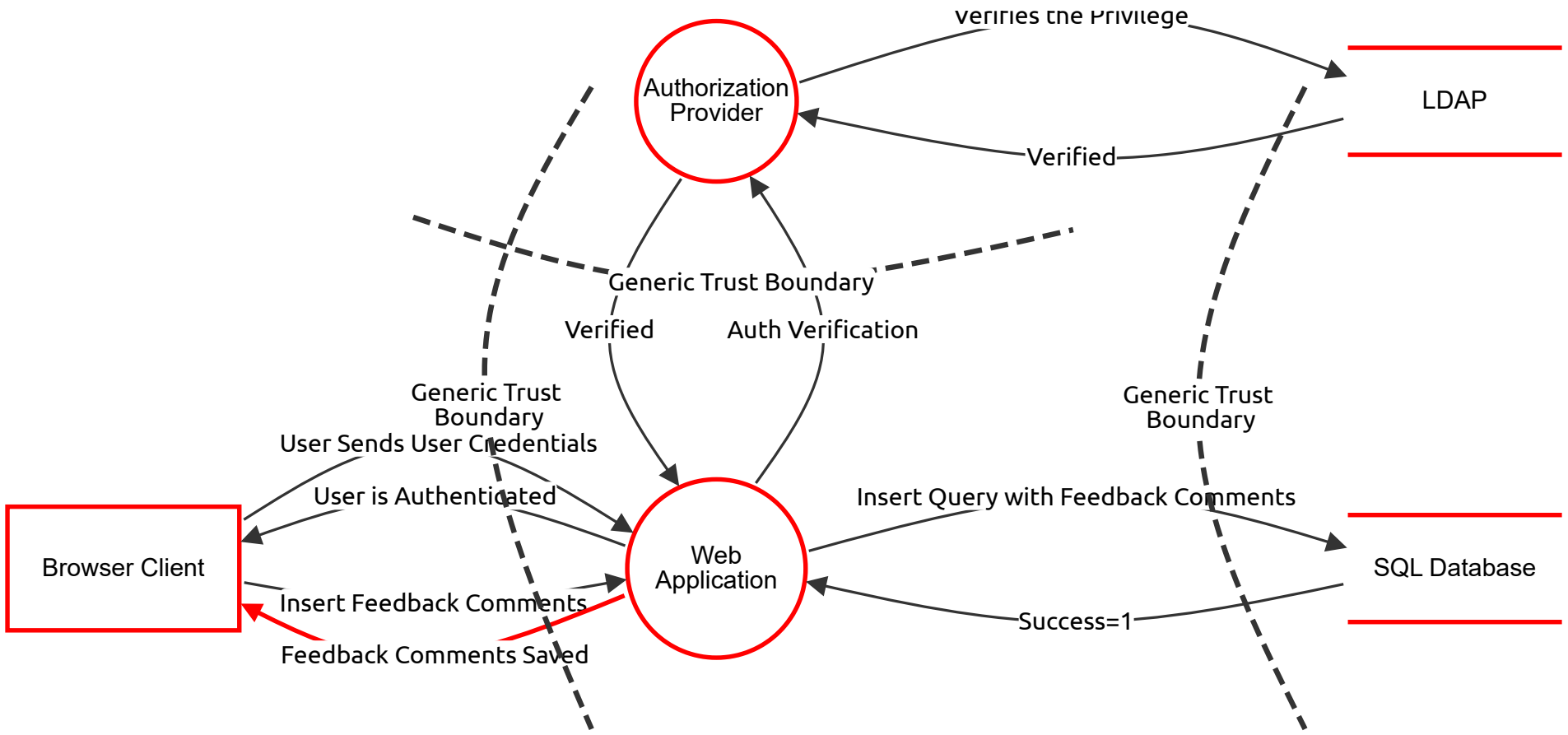
A sample model of a web application, with a queue-decoupled background process.

Summary

Total Threats	7
Total Mitigated	0
Not Mitigated	7
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

Main Request Data Flow

Main Request Data Flow Description



Main Request Data Flow

Browser Client (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	Browser Client Spoofing	Spoofing	TBA	Open		The web application may be spoofed by an attacker and this may lead to unauthorized access to the browser client. (When discussed with the design team, it appears that this is not possible, as a security mechanism to identify the server is present.)	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
109	Web Application Spoofing	Spoofing	TBA	Open		The web application may be spoofed by an attacker and this may lead to unauthorized access to the browser client. (When discussed with the design team, it appears that this is not possible, as a security mechanism to identify the server is present.)	Provide remediation for this threat or a reason if status is N/A

SQL Database (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	SQL Database Spoofing	Tampering	TBA	Open		The SQL Database may be spoofed by an attacker, and this may lead to data being written to the attacker's target instead of the SQL Database. (When discussed with the design team, it appears that this is not possible, as SQL connection is made using the database username and password.)	Provide remediation for this threat or a reason if status is N/A

Authorization Provider (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	Authentication Provider Elevation of Privilege	Elevation of privilege	TBA	Open		The browser client may be able to impersonate the context of the web application in order to gain additional privilege. An attacker may pass data into the browser client in order to change the flow of program execution within the browser client to the attacker's choosing.	Provide remediation for this threat or a reason if status is N/A

LDAP (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	LDAP Tampering With The Data Using The SQL Injection Attack	Tampering	TBA	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. LDAP injection is possible, as the user authentication is verified using an LDAP query.	Provide remediation for this threat or a reason if status is N/A

User Sends User Credentials (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User is Authenticated (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Insert Feedback Comments (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Feedback Comments Saved (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
124	Feedback Comments Saved Tampering	Tampering	TBA	Open		Data flowing across saved feedback comments may be tampered with by an attacker. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved-list input validation approach.	Provide remediation for this threat or a reason if status is N/A
126	Feedback Information disclosure	Information disclosure	TBA	Open		Data flowing across saved feedback comments may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	Provide remediation for this threat or a reason if status is N/A

Auth Verification (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Verified (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Verifies the Privilege (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Verified (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Insert Query with Feedback Comments (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Success=1 (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations