SWE 550 Threat Modeling for Web Application

Owner: Simon Codrington
Reviewer:
Contributors:
Date Generated: Thu Oct 31 2024

Executive Summary

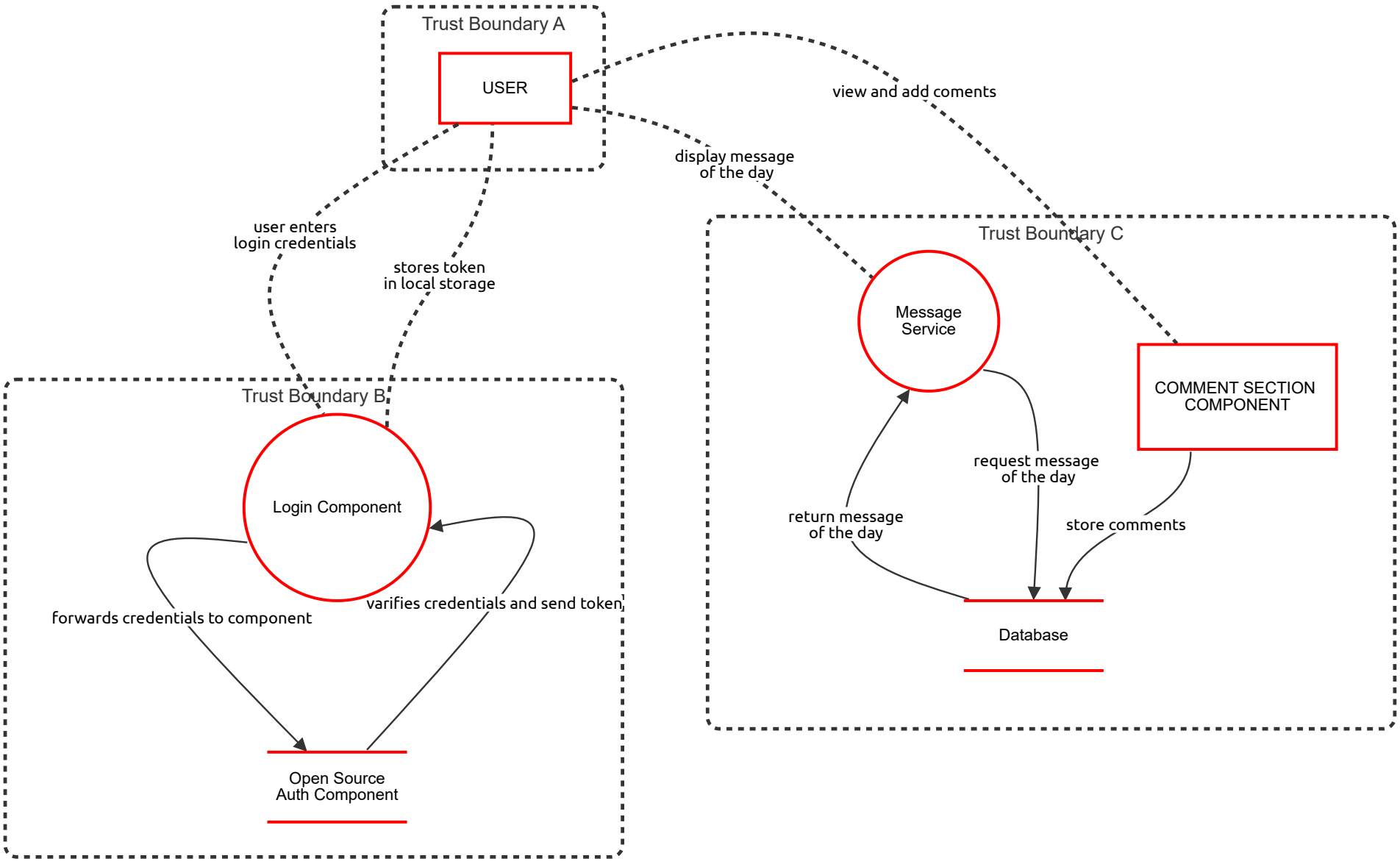
High level system description

Not provided

Summary

Total Threats	6
Total Mitigated	0
Not Mitigated	6
Open / High Priority	0
Open / Medium Priority	6
Open / Low Priority	0
Open / Unknown Priority	0

New STRIDE diagram



New STRIDE diagram

USER (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
17	New STRIDE threat	Spoofing	Medium	Open		Ensuring that the user identity is genuine	Use HTTPS to encrypt communications and consider multi-factor authentication

COMMENT SECTION COMPONENT (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
27	New STRIDE threat	Spoofing	Medium	Open		Ensuring that only authorized users can alter data.	Provide remediation for this threat or a reason if status is N/A

forwards credentials to component (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

varifies credentials and send token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

return message of the day (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request message of the day (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

store comments (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
24	New STRIDE threat	Information disclosure	Medium	Open		Unauthorized access to sensitive data	Apply role-based access control and encrypt data at rest

Open Source Auth Component (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	New STRIDE threat	Denial of service	Medium	Open		excessive requests, causing it to become unavailable to legitimate users	rate limiting to control the volume of requests, monitoring to detect and respond to unusual traffic patterns.

Login Component (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	New STRIDE threat	Tampering	Medium	Open		Ensuring that data isn't altered between the login component and the authentication module	Implement input validation, access controls, and secure token handling

Message Service (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
26	New STRIDE threat	Information disclosure	Medium	Open		Sensitive data exposure	Use HTTPS and encrypt sensitive data in storage and transit