Initial Threat Model

Owner: Giovanni Rosas-Marin
Reviewer: SWE-550-Professor-Todd
Contributors:
**Date Generated**: Mon Sep 09 2024

Executive Summary

High level system description

 This initial Threat Model is built based on a Message Board applications.
The system sample is as Follows:
Presents the user with a login page (username and password)
Uses an open source component to authenticate the user credentials against a database
If the username and password presented exist in the database, present the user with a message-of-the-day stored in the database
Allow the user to comment on the message-of-the-day (comments will be stored in the database)

Summary

Total Threats	44
Total Mitigated	0
Not Mitigated	44
Open / High Priority	9
Open / Medium Priority	35
Open / Low Priority	0
Open / Unknown Priority	0

Initial Threat Model Diagram
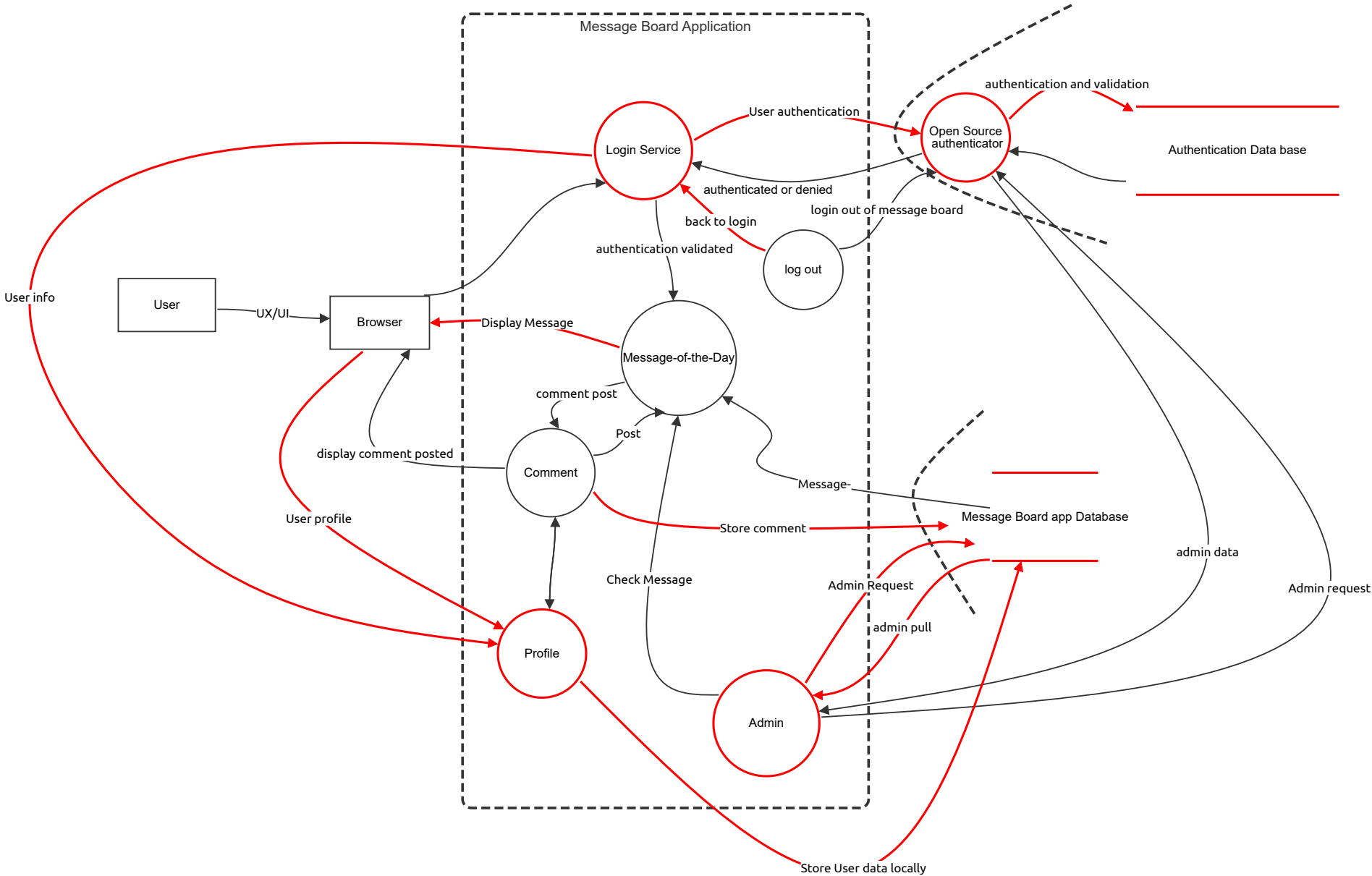
Initial Threat Model Diagram

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Browser (Actor)

User will select preferred browser:
Chrome, firefox, edge

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

back to login (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	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

User authentication (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

authentication and validation (Data Flow)

will check if user information is correct in the login and if the data is register in the authentication data base if not sent back error message or suggest to register new account

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	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

login out of message board (Data Flow)

Will route back to the open source authenticator to send back to the login page to be able to access page

Number	Title	Type	Priority	Status	Score	Description	Mitigations

UX/UI (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

authentication validated (Data Flow)

once logged in an authenticated will route to message of the day

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Display Message (Data Flow)

Will display the message to the user

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Admin request (Data Flow)

to get data from users

Number	Title	Type	Priority	Status	Score	Description	Mitigations

admin pull (Data Flow)

getting response from the database

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Information disclosure	High	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Check Message (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Message- (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Admin Request (Data Flow)

Getting data from the message board data base

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Tampering	High	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	New STRIDE threat	Information disclosure	High	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Store comment (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

admin data (Data Flow)

able to check data table in the data base of the authentication login service

Number	Title	Type	Priority	Status	Score	Description	Mitigations

display comment posted (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Post (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

comment post (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User profile (Data Flow)

Able to have profile to check messages and comments made

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	New STRIDE threat	Information disclosure	High	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

User info (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	New STRIDE threat	Information disclosure	High	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	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
18	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
18	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

Store User data locally (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
40	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
40	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
40	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

Login Service (Process)

Open source to authenticate

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	New STRIDE threat	Information disclosure	Medium	Open		User's information per login can be in risk	This can be address by having 2-verification method available
1	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
1	New STRIDE threat	Denial of service	Medium	Open		If user is not verified it can deny the access	User should complete correct login and also verify with 2-form verification
1	New STRIDE threat	Spoofing	Medium	Open		Other user pretending to be another user to login to another account to post messages or comments	having the user be alerted when someone trying to login from different location or device to remediate risk

Open Source authenticator (Process)

This will depend on the service selected but selected aws cognito operates authentication and registration

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	New STRIDE threat	Denial of service	Medium	Open		If user is not verified it can deny the access	User should complete correct login and also verify with 2-form verification
1	New STRIDE threat	Information disclosure	Medium	Open		Other user pretending to be another user to login to another account to post messages or comments	having the user be alerted when someone trying to login from different location or device to remediate risk
9	New STRIDE threat	Elevation of privilege	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Authentication Data base (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	New STRIDE threat	Denial of service	High	Open		Checking if user is authorized and validated or deny access	send response error message to attempt again or to register account
10	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	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

Message Board app Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
10	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	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

Comment (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Profile (Process)

User profile

Number	Title	Type	Priority	Status	Score	Description	Mitigations
43	New STRIDE threat	Spoofing	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
43	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
43	New STRIDE threat	Repudiation	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
43	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
43	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
43	New STRIDE threat	Elevation of privilege	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

log out (Process)

User login Out of the message board application

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Message-of-the-Day (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Admin (Process)

Check the message of the day and comments and users and app itself

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	New STRIDE threat	Spoofing	High	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	New STRIDE threat	Tampering	High	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
16	New STRIDE threat	Elevation of privilege	High	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A