SocialNet

Owner: desofs2024_M1B_3

Reviewer: Paulo Baltarejo Sousa <pbs@isep.ipp.pt>

Contributors: Tomás Afonso Soares De Oliveira <1230213@isep.ipp.pt>, Diogo Alexandre Pereira Ferreira <1230176@isep.ipp.pt>, Luís Silva <1181031@isep.ipp.pt>, Paulo Moreira <1180778@isep.ipp.pt>

Date Generated: Fri Apr 19 2024

Executive Summary

High level system description

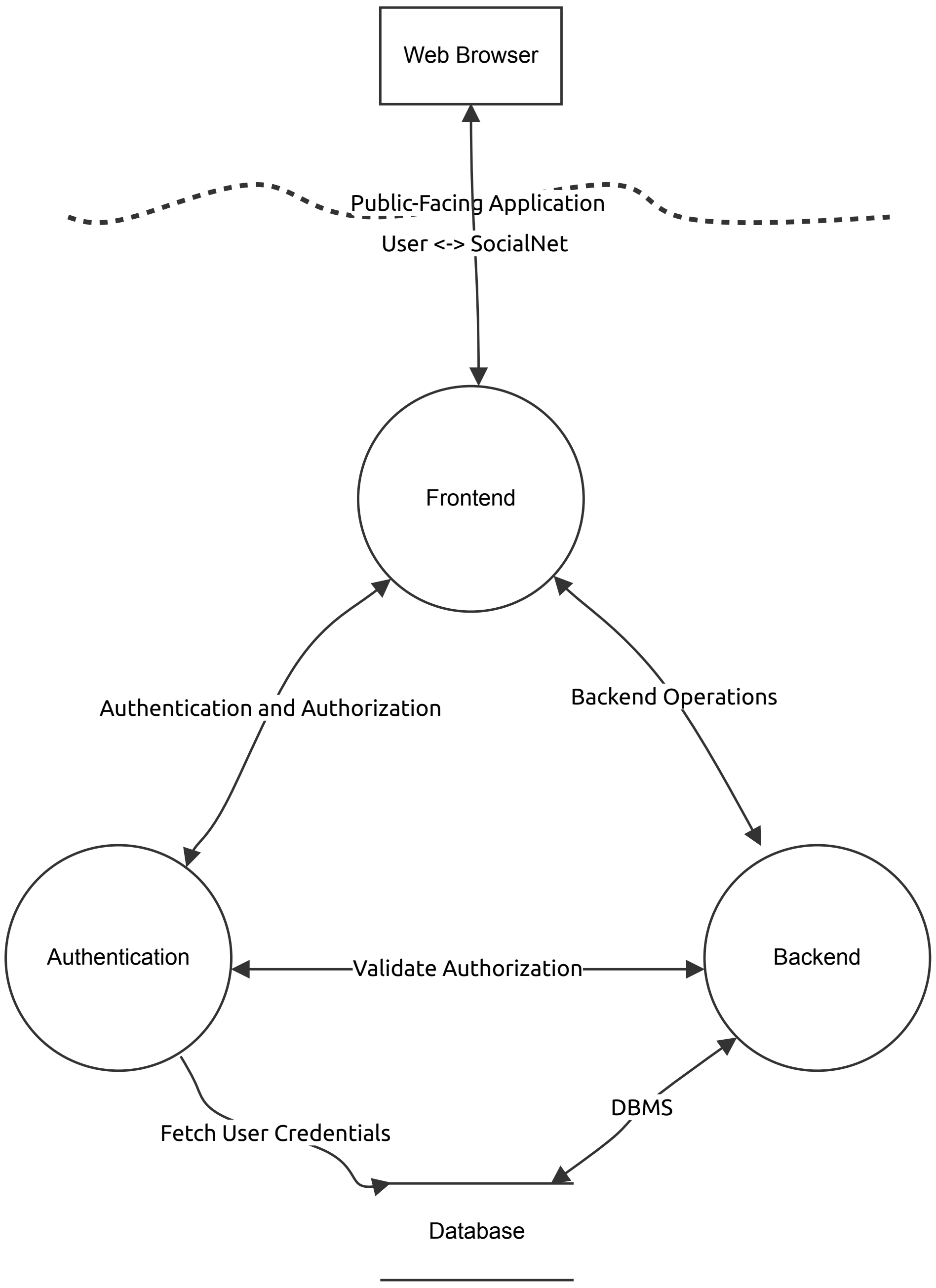
SocialNet: a social network like Twitter

Summary

Total Threats	37
Total Mitigated	36
Not Mitigated	1
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

Deployment

Threat Modeling based on Deployment Diagram



Deployment

Web Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Spoofing	Spoofing	Low	Mitigated	4	Attackers may spoof the identity of the user or the browser to gain unauthorized access.	Implement multi-factor authentication (MFA).
18	Repudiation	Repudiation	Low	Mitigated	4	Users may deny their actions within the browser.	Implement comprehensive logging of user actions and interactions within the application.

Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	Tampering	Tampering	High	Mitigated	15	Unauthorized modification of data stored within the database could lead to security vulnerabilities or data corruption.	Apply encryption of data at rest, access controls using permissions segregation and and input validation using parameterized queries.
23	Repudiation	Repudiation	Medium	Mitigated	9	Without proper logging and auditing mechanisms, users may deny their actions within the application.	Implement comprehensive logging and auditing of the database. Engine can be used to generate a binlog.
24	New STRIDE threat	Information disclosure	Medium	Mitigated	10	Inadequate configurations may result in information leaks.	Implement air-tight configuration for the database to prevent access and mask sensitive information on logs.
25	New STRIDE threat	Denial of service	High	Mitigated	25	Abuse cases may perform too many requests that result in too many database requests.	Configure rate limiting, query optimization and monitor resources.

Authentication (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
33	New STRIDE threat	Elevation of privilege	High	Mitigated	10	Attackers might find vulnerabilities in this component and perform authentication and get authorization for higher ranked useds	Ensure validation of authorization by user type and not only by the information provided by the auth system
34	New STRIDE threat	Denial of service	Low	Mitigated	10	Attackers might try to brute-force authentication and the system might stop responding to new requests	Enable rate limiting and provide means to prevent brute-force attacks and DDOs on components that access the authentication system
35	New STRIDE threat	Information disclosure	Medium	Mitigated	10	Authentication and authorization information, as well as sensitive information might leak due to design and implementation flaws	Enable HTTPS communication to ensure encryption between components

Frontend (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
26	Spoofing	Spoofing	Low	Mitigated	6	Attackers may spoof the identity of the user or the browser to gain unauthorized access.	Implement multi-factor authentication (MFA).
27	Tampering	Tampering	Low	Mitigated	6	Attackers might try to execute malicious code modified at the frontend.	Secure Coding Practices: prevent any and all code from being changed and executed without validation
28	Repudiation	Repudiation	Medium	Low	6	Users may deny their actions within the browser.	Implement comprehensive logging of user actions and interactions within the application.
29	Information Disclosure	Information disclosure	Medium	Mitigated	9	Inadequeate configurations of logging and encryption of information may result in leaks that we do not want	Disclose any information in logs, prevent leaks to the console, encrypt all sensitive information
30	Denial of Service	Denial of service	Low	Mitigated	4	Attackers may try to flood the system with too many requests for a given period of time	Implement rate limits in the frontend, cache responses to prevent computing resources to be wasted
31	Elevation of Privilege	Elevation of privilege	High	Mitigated	12	Attackers might try to impersonate higher ranking users and perform malicious actions	Use RBAC and JWT validations, encrypt session cookies

Backend (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
36	DDoS	Denial of service	Low	Mitigated	4	Attackers will perform frontend operations that will trigger backend requests and perform a denial of service	Apply rate limit between components to throttle too many requests in a given period of time
37	Elevation of Privilege	Elevation of privilege	Medium	Mitigated	8	Attackers may try to access the backend directly with credentials that belong to higher ranking users or propagate an elevation of privilege from the frontend.	Re-validate the authorization provided by the frontend and evaluate the operation being requested.
38	Tampering	Tampering	Medium	Mitigated	6	Attackers might try to modify information stored in the database by performing rogue backend requests with tampered information.	Validate all requests, their origin and what it is trying to modify. Do not allow arbitrary requests.
40	Spoofing	Spoofing	Medium	Mitigated	6	Users might try to impersonate other users by propagating an attack from the frontend to the backend (escalation of privilege or spoofing, for example).	Re-authenticate the user and analyze what action he is trying to make vs permissions and origin of request. for example a premium user cannot delete other people's tweets. Also if a premium user as an ip of 1.2.3.4 it is not expectable to have tweets being deleted from that ip.
41	Disclosure of Information	Information disclosure	Medium	Mitigated	6	Attackers might try to access and release information that can only be accessed using the backend (for example information stored in the database).	Validate requests, encrypt information using DTO and drop all fields that are not needed when performing a request to prevent too much information traveling at once.

User <-> SocialNet (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
44	Too Many Requests - DDOs	Denial of service	Low	Mitigated	4	Abuse cases.	Implement rate limiting.
45	Modifying Requests	Tampering	Low	Mitigated	4	Attackers may try to modify requests made to the frontend.	Implement validations for requests and payloads. Use HTTPS.

Authentication and Authorization (Data Flow)

Requests authorization for users. Validates credentials of users.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
57	Modifying users	Tampering	Medium	Mitigated	6	Attackers may use requests from the frontend to modify credentials of users in the authentication system.	Validate payloads before propagating them.
58	Disclose credentials in the console	Information disclosure	Medium	Mitigated	4	Trying to obtain information regarding authorization.	Configure logging at the frontend level, prevent leaks to the console. Encrypt data and hide sensitive information.
59	DDos of Auth Service	Denial of service	Low	Mitigated	2	Perform too many authentication requests.	Implement rate limiting.

Validate Authorization (Data Flow)

Prevent threats and re-validate authorization.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
53	Trying to impersonate other users	Tampering	Low	Mitigated	1	Attackers may explore vulnerabilities to impersonate higher ranking users and perform backend operations.	Implement latest supabase version.
55	Disclose user credentials	Information disclosure	Medium	Mitigated	2	Poorly configured backend may leak information regarding authorization and authentication.	Implement logging, use dtos and prevent leaks of information.
56	Modifying Information on the authentication server	Tampering	Low	Mitigated	4	Attackers may explore the backend and try to modify the information at rest regarding users.	Validate all requests by user and type.

DBMS (Data Flow)

Query data from the database. Save data to the database.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
46	DDOs to DB	Denial of service	Low	Mitigated	4	Abuse cases may result in too many requests to the database.	Implement rate limiting, cache and query optimization.
47	Disclosing Sensitive information	Information disclosure	Low	Mitigated	4	Bad configurations may result in information being disclosed.	Implement logging configurations with proper levels, encrypt sensitive data, query information that is scoped and hide sensitive information.
48	Mydifying data at rest	Tampering	Medium	Mitigated	5	Attackers may try to access and modify data at rest.	Implement transactional operations with logging so these changes can be reverted. Implement segregation of permissions by using multiple users with scoped permissions (read-only for example).

Fetch User Credentials (Data Flow)

Validate stored credentials agains input credentials

Number	Title	Type	Priority	Status	Score	Description	Mitigations
50	User Information Leak	Information disclosure	Low	Mitigated	1	The auth system may disclose information.	Logging and engine configurations on the database.
51	Abuse case: too many authorization attempts	Denial of service	Low	Mitigated	1	Attackers may try to authenticate too many times.	Rate limiting the authentication requests.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
52	Modifying user credentials	Tampering	Low	Mitigated	1	Attackers may try to modify user credentials.	Encrypt passwords and validate request origin.

Backend Operations (Data Flow)

Perform backend operations and queries.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
60	Modifying more data than it should	Tampering	Medium	Mitigated	4	Trying to modify the data at rest using the backend.	Implement validations of who is performing the request and if the request makes sense.
61	Obtaining information	Information disclosure	Medium	Mitigated	4	Obtaining information by abusing logging configurations.	Implement proper logging, using DTOs, hiding sensitive information.
62	Trying to DDOs the backend	Denial of service	Low	Mitigated	2	Propagating DDOs from the frontend may end in a ddos to the backend.	Implement rate limiting and cache.