SocialNet

Owner: desofs2024_M1B_3
Reviewer: Paulo Moreira <1180778@isep.ipp.pt>
Contributors: Tomás Afonso Soares De Oliveira <1230213@isep.ipp.pt>, Diogo Alexandre Pereira Ferreira <1230176@isep.ipp.pt>, Luís Silva (1181031) <1181031@isep.ipp.pt>
Date Generated: Fri Apr 12 2024

Executive Summary

High level system description

SocialNet: a social network like Twitter

Summary

Total Threats	8
Total Mitigated	8
Not Mitigated	0
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

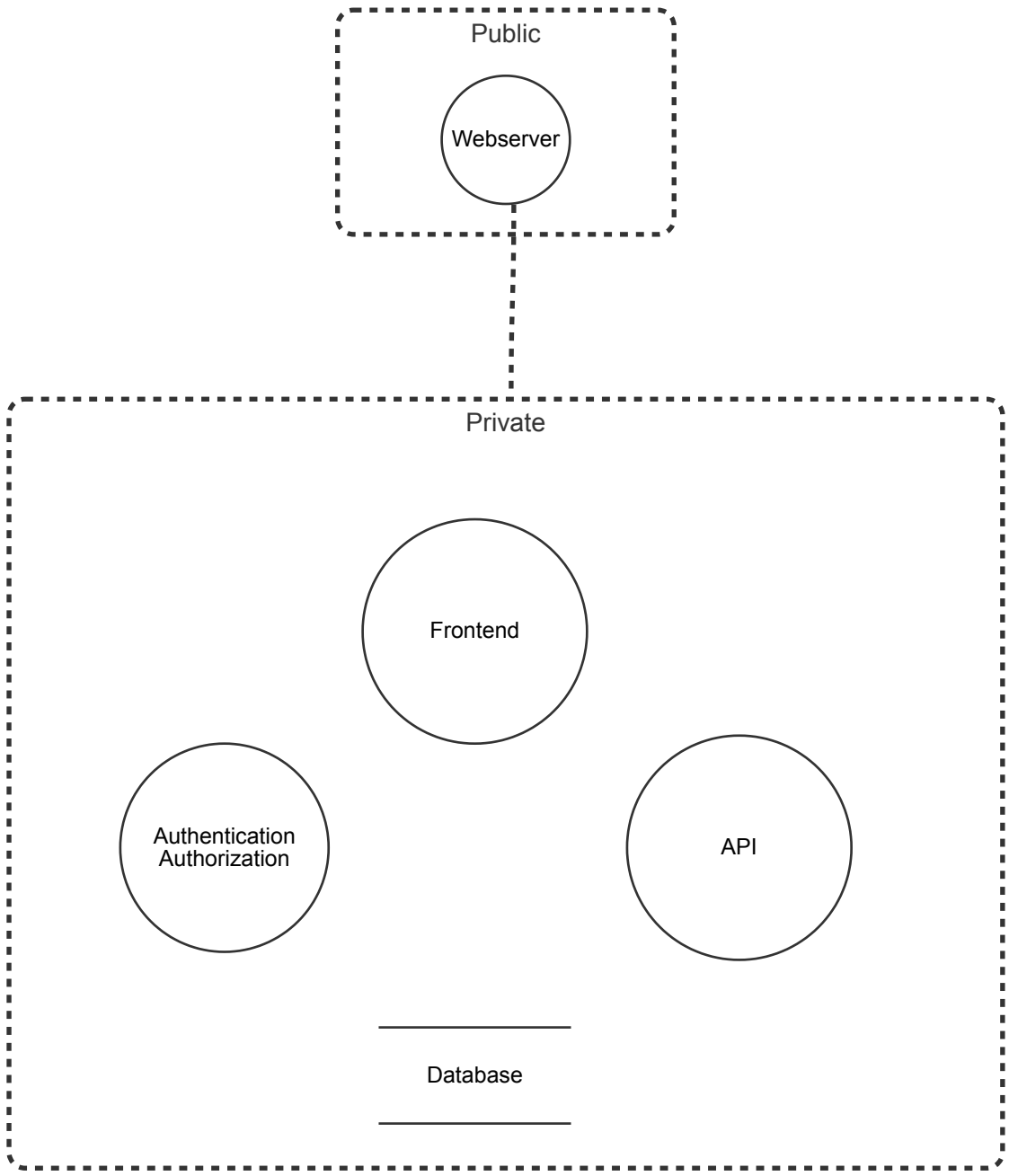
Domain

Domain for SocialNet

Domain

Infrastructure

Infrastructure for SocialNet



Infrastructure

Database (Store)

Database for user credentials and other necessary entities.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	SQL Injection	Tampering	High	Mitigated		Injecting SQL commands onto the database.	Parameterized Queries, DBMS provided by Supabase with well-known architecture. Segregation of permissions with read-only access whenever possible.
10	Data Leaks	Information disclosure	High	Mitigated		After a successful attack one could disclose information not encrypted.	Encrypt any and all sensitive information + protect database access.

Authentication Authorization (Process)

Using Supabase.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Brute Force Attacks	Denial of service	Low	Mitigated		Accessing authentication using brute-force attacks.	With the implementation of an WAF (Cloudflare, for example) + Rate limit by design
8	Escalation of Privileges	Elevation of privilege	Medium	Mitigated		Trying to authenticate and getting authorization for higher levels than supposed.	JWT validations on the components (API, Frontend) that call this + properly encrypted cookies.

API (Process)

Used to manage the endpoints used by the application

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	DDOS	Denial of service	Low	Mitigated		Distributed Denial of Service by abusing multiple requests.	FastAPI with rate limiting + not exposed to the public + behind WAF.

Frontend (Process)

ReactJS Engine

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Distributed Denial of Service	Denial of service	Low	Mitigated		Distributed Denial of Service by abusing requests	Rate Limiting provided by the technology + Behind the WAF + not exposed to the public.
9	Modifying Requests	Tampering	Low	Mitigated		Trying to modify requests that are handled by this component.	Properly parsing all requests, using parameters and validations.

Webserver (Process)

Cloudflared acting as a reverse-proxy.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	DDOS	Denial of service	High	Mitigated		Distributed Denial of Service by the abuse of multiple requests from multiple sources.	Using Cloudflare ensures that DDOS is nearly impossible to achieve due to their protections.