COMUNICATION_LTD

STRIDE – Threats assessment

Matan Mizrachi 203168026, Nissim Amira 307831388 and Goni Liraz 208494139.

	Weakness point description	**Relevant threat**
1	Security config data is stored in a configuration file unencrypted.	Tampering with Data - Changing configuration file.
2	DB is running on an unsecured environment – local, not encrypted.	Information Disclosure, Tampering with Data - Accessing the DB not via the API.
3	TLS protocol is only implemented on frontend side.	Information Disclosure - API←→DB connection is insecure. Repudiation - No TLS between DB and backend.
4	"Login attempts", "Clients" tables in the DB are never reset.	Denial of Service - Very large tables might grow to unmanageable size.
5	SALT for hashing is stored unencrypted in the DB file.	Denial of Service - If SALT is changed all the users are locked out.
6	No multi factor authentication.	Spoofing Identity - Weak authentication can easily be breached.
7	No privileges are implemented for backend (API) and DB functions.	Information Disclosure, Tampering with Data - Anyone with the API URL can perform operations on the system.
8	[Low security mode] No input validation, allowing SQL Injection.	Information Disclosure, Tampering with Data - Any SQL query can be sent.
9	[Low security mode] No text formatting, allowing XSS.	Information Disclosure - Scripts can be run to insert a cookie or to send data from the user. Tampering with Data - Any HTML manipulation can change the system behavior. Denial of Service - Scripts can be run that will use the system resources.