OWASP 10

This document explains the precautions applied for Mentornity systems to secure it against the top 10 security risks in OWASP.

A01:2021-Broken Access Control

All API requests use proper HTTP methods with Access Tokens to identify users and cross check their role with the permission for the given action.

A02:2021-Cryptographic Failures

All requests are redirected to HTTPS and transmitted through secure connections. Only TLS 1.3 and 1.2 are supported and the older versions 1.1 and 1.0 are disabled.

A03:2021-Injection

All API requests are validated. Unexpected parameters fail the requests or ignored.

A04:2021 – Insecure Design

The system is built with set of security layers from the server request protocols to micro validations in each action.

A05:2021 – Security Misconfiguration

Trusted cloud providers are used to set up the system architecture. Only limited number of employees have access to the cloud provider accounts. The connections to servers are established on the small number of ports that are required by the applications. The rest of the ports are unaccessible.

A06:2021 – Vulnerable and Outdated Components

All the servers are maintained to include the latest security updates. The servers in the serverless systems are updated automarically by the cloud provider. The rest of the small number of servers are manually updated frequently.

A07:2021 – Identification and Authentication Failures

There are very few functionalities that allows anonymous user requests like login and reset password. These requests are validated via the user email. Once the user authenticates, the rest of the requests contain a valid access token that identifies the user. Requests fail if the identification metadata is absent.

A08:2021 – Software and Data Integrity Failures

The code is stored in private repositories. There is a review process for project code changes. The changes in code are first tested on test/qa environments. Then the changes are manually merged by employees with specific permissions. Code compilation, Docker image generation and server updates happen in the cloud provider systems automatically in a closed system to ensure the security and quality of the entire build pipeline.

A09:2021 – Security Logging and Monitoring Failures

A wide range of logs are stored in different formats in related storages. User login errors are moderated in the system admin dashboards. The server access and application logs are stored in the cloud provider logging services which are only accessible by very few system admins.

A10:2021 – Server-Side Request Forgery (SSRF)

All the requests are authenticated via tokens and each action is checked to ensure the user has necessary permissions to perform the actions on the related resources.