Database for managing penetration testingn

The database is used for management of penetration testing. Testers can create projects in the application and invite other users to join the project. The application includes all phases of penetration testing according to specific methodologies (e.g. OWASP, OSSTMM, PTES, ISSAF).

All users have an account account with required parameters of email, first and last name, salted-hashed password (SHA-512) and optional: avatar (avatar image url from Robohash) and phone number.

Each project has a name, start date and end date (deadline). The project description is optional. Project administrator can create tasks and assign them to specific users in the project. Tasks also contain the targets to be tested with the corresponding description. Task can be assigned to a category that contains checklists according to a certain methodology or a custom definition (users can also create their own checklists in the application). These will vary by target, for example network vs. web application. If a vulnerability is found on a target, it is assigned with a corresponding description and identification number (CVE), which is optional. The same vulnerability can be present in multiple targets to avoid duplications.

Users can also upload a document (file) to the system, which can be added additionally to the project and shared with other users. After uploading, the document contains metadata containing the document format (type), size, date the document was created and last updated. The functionality is similar to Google Docs, so one document can be shared across multiple projects.

Each section that can be displayed using a url contains a slug by its name, which is usually automatically created from the title (it can also be created manually). The name that is used as the slug is unique.

All parts of the application are restricted by user role and permissions. Roles are divided by type. The default role types are global (application) or project roles. For example, only the project admin can invite other users to the project. These permissions can be scaled and used to define what users can do in the project.

Each user action is logged with a time stamp and a description of the event. Furthermore, everything that can be created or edited contains a timestamp (created, updated).

The application is highly scalable and can be extended in the future with additional parts (structure, database, functions) that would increase penetration testing management capabilities.