APIs

- /run-test POST
  - Header -> auth token
  - Request body -> target: List of targets
  - Response -> status code and response body (“the job has been queued” or another descriptive message)
  - Authentication/authorization -> middleware handles token validation and authorizes the target list (if the target list includes the web vulnerability scanner, it makes sure the user is a small business user).
- /register POST
  - Request -> needed information (name, last name, others) and organization ID if applicable
  - Response -> status code and response body as descriptive message
  - Authentication/authorization -> middleware handles authentication and validation of token of user if organization ID is present (user must be admin of organization to add others).
- /log-in POST
  - Request -> username and password
  - Response -> status code, access token, and refresh token
- /get-user GET
  - Header -> auth token
  - Query parameter -> optional to pass user ID for admin of organization to get user of its organization
  - Response -> status code, response body (profile picture, settings, type of user for dashboard, etc)
  - Authentication/authorization -> middleware handles check for assuring user requesting and requested data is for same user or that the requesting user is authorized to request specific other user (maybe organization admin).
- /get-data (generalized) GET
  - Header -> auth token
  - Request body -> necessary specifics depending on what data is being requested
  - Response -> status code and data (such as test results)
  - Authentication/authorization -> middleware handles token validation