Uprawnienia i stany użytkowników w aplikacji

Użytkownicy w aplikacji będą posiadali różne uprawnienia w zależności od przypisanego poziomu uprawnień oraz stanu.
Stany użytkowników:

- zalogowany
- niezalogowany

Poziomy uprawnień:

- gość (równoznaczny z użytkownikiem niezarejestrowanym) – poziom tych uprawnień pozwalać będzie tylko na przeglądanie treści w postaci opublikowanych zestawów komputerowych
- standardowy użytkownik – będzie posiadać dodatkowo możliwość dodawania nowych treści oraz tworzenia zestawów w celu ich prezentacji. Wymagać będzie posiadania konta w aplikacji.
- moderator – uprawnienia zostaną uzupełnione o możliwość modyfikacji treści umieszczonych przez użytkowników. Tak jak standardowy użytkownik wymagać będzie zalogowania do serwisu.
- administrator – uprawnienia będą nieograniczone. Będzie posiadał możliwość dodawania, przeglądania, modyfikowania oraz usuwania wszystkich treści, łącznie z danymi użytkowników.

Polityka bezpieczeństwa w aplikacji

- Szyfrowanie danych - dane takie jak hasła będą poddawane kodowaniu poprzez mechanizm wbudowany w framework Laravel. Algorytm BCrypt pozwoli na hash hasła metodą Base64
- Dostęp do bazy danych – dostęp będzie chroniony poprzez dane logowania użytkownika bazy danych MySql. W wersji użytkowej użytkownik ten zostanie pozbawiony uprawnień pozwalających na modyfikację struktur tabel danych.
- Kopie zapasowe – będą wykonywane manualnie z powodu braku potrzeby przechowywania ważnych danych związanych z funkcjonowaniem instytucji lub innych ważnych danych personalnych.
- Bezpieczeństwo danych dostępnych poprzez Rest API – dane wynikowe będą wybierane, tak aby nie były przekazywane żadne tokeny, adresy email ani hasła, nawet w swojej zakodowanej formie
- Istotne zabezpieczenia programowe wbudowane w framework:
  - Ochrona przed SQL Injection
  - Ochrona przed atakami typu CSRF
  - Walidacja danych wbudowanymi metodami

Diagram przypadków użycia