Aplikacja do przechowywania stylizowanych notatek

Hubert Mazur 307487

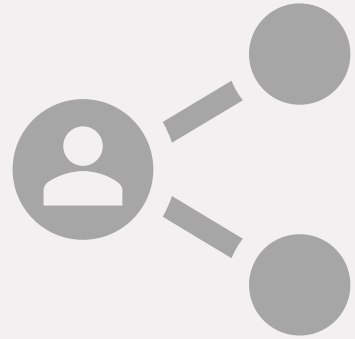
Uwierzytelnianie użytkowników

- Hasła użytkowników są przechowywane w bazie jako wynik funkcji **SHA512** w bazie **sqlite**
- Hasło musi się składać z małej i wielkiej litery, cyfry, znaku specjalnego, mieć min. 12 znaków długości i wysoką entropię
- Zastosowanie **PBKDF2**, **HMAC** oraz losowej **soli** – *werkzeug.security*
- Sprawdzanie poprawności wprowadzonego adresu email oraz jego unikalności
- Ograniczenie informacji o błędnym logowaniu do minimum
- 5 prób logowania na 15 minut dla każdego adresu – *Flask_limiter*
- 3 sekundy opóźnienia przy walidacji danych logowania

Szyfrowanie notatek

- Hasła do notatek są przechowywane w bazie jako wynik funkcji **argon2** w trybie ID
- Losowa sól
- Treść notatki jest szyfrowana przy użyciu szyfru blokowego **CBC**
- Klucz stanowi część digest hash'a hasła, a IV – zakodowana base64 sól hash'a hasła

Udostępnianie notatek

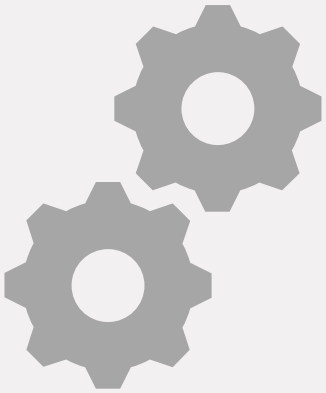


- Należy mieć konto i być zalogowanym aby móc zobaczyć udostępnioną/publiczną notatkę
- Nie można udostępniać szyfrowanych notatek
- Widoczność notatki może zmieniać tylko właściciel notatki
- Tablica par (ID notatki, ID użytkownika) definiuje dostęp dla wybranej grupy użytkowników
- Globalny dostęp otrzymuje się znając ID notatki lub posiadając unikalny link przeznaczony do udostępniania

Walidacja danych wejściowych

- Na każdym kroku sprawdzane jest czy użytkownik jest zalogowany – *flask_login*
- Parametry ścieżki URL są sprawdzane w każdym endpoint'cie
- Sanityzacja zawartości notatek – *bleach*
- Weryfikacja nazw oraz rozszerzeń plików
- Prawda do oglądania/edycji stanu notatki są na każdym kroku sprawdzane

Dodatkowe zabezpieczenia



- Nagłówki we wszystkich odpowiedziach
  - Strict-Transport-Security = max-age=31536000; includeSubDomains
  - Content-Security-Policy = default-src 'self' + zewnętrzny .css
  - X-Content-Type-Options = nosniff
  - X-Frame-Options = SAMEORIGIN
- Ustawienia ciasteczek sesji
  - SESSION_COOKIE_SECURE = True
  - SESSION_COOKIE_HTTPONLY = True
  - SESSION_COOKIE_SAMESITE = Lax
- HTTPS, certyfikat ad-hoc
- Tokeny CSRF – *flask_wtf.csrf*

Dziękuję za uwagę