

ZLECENIA DOTYCZĄCE SYSTEMU SETI-1

A. Zadania programistyczne:

1. Zaawansowana obsługa haseł użytkownika w systemie SETI (4-6 tyg.)

- △ wprowadzenie możliwości zmiany hasła na serwerze wyniesionym
 - △ podstawowa funkcjonalność zmieniająca hasło lokalnie już jest, potrzebne jest dodatkowo
 - △ opracowanie i implementacja mechanizmu transferu zmienionych danych logowania (zmienione hasło, data zmiany hasła, timestamp ostatniego poprawnego logowania, timestamp ostatniego błędnego logowania, licznik błędnych logowań, znacznik changeOnLogin - wymuszenie zmiany hasła) z serwera wyniesionego na centralny (jeśli się da to przy użyciu mechanizmu transferu dokumentów)
 - △ zmiana własnego hasła powinna wymagać podania starego hasła
 - △ rozdzielenie haseł do serwera centralnego i wyniesionego (obejmuje poprawki do administracyjnego gui zmiany hasła)
- △ zbyt wiele nieudanych prób logowania (np 5) w zadanym okresie czasu (np 15 minut - potem resetujemy licznik) powinno blokować możliwość logowania na pewien czas (np 15min od ostatniej błędnej próby logowania)
 - △ w trakcie czasowej blokady przy próbach logowania powinien być wyświetlany komunikat informujący o tej blokadzie
 - △ idealnie byłoby, gdyby to był odrębny JAAS login module
 - △ przy odpowiedniej konfiguracji ten sam login module mógłby być odpowiedzialny za blokadę systemu
- △ użycie ziarna oraz wielokrotne wyliczanie skrótu sha512 haseł lub użycie bcrypt -8 iteracji (czas potrzebny do wyliczenia jednego skrótu powinien wynosić co najmniej 10ms)
 - △ mechanizm wymuszający aktualizację skrótów, które ziarna jeszcze nie zawierają (np. przy logowaniu)
 - △ dotyczy także serwera wyniesionego
- △ wprowadzenie konfigurowalnego mechanizmu definiowania oraz kontroli okresu ważności hasła (wstępna konfiguracja: min 7dni, max 1 rok)
 - △ mechanizm ten powinien wymuszać na użytkowniku zmianę haseł przeterminowanych
 - △ nie powinien dopuszczać do zbyt częstych zmian hasła
- △ kontrola jakości haseł przy zmianie (konfigurowalne)
 - △ formularz powinien wyświetlać listę reguł kontroli jakości hasła wraz z informacją, które reguły są przez wprowadzone hasło spełnione
 - △ lista wymaganych reguł:
 - △ min 8 znaków
 - △ musi zawierać znaki z min 3 zbiorów (litery małe, litery duże, cyfry, znaki specjalne)
 - △ wykluczenie popularnych podciągów słownikowych a'la cracklib (oprócz ciągu słownikowego min 6 innych znaków) w tym:
- △ wykluczenie danych osobowych tj. loginu, imienia, nazwiska itp
- △ wykluczenie 3 poprzednich haseł (musi się różnić na przynajmniej 4 pozycjach)
- △ generowanie losowego hasła na żądanie przy ustawianiu/zmianie hasła (oczywiście musi spełniać wszystkie reguły)
 - △ o ile nie wprowadza to dodatkowego ryzyka
 - △ hasła muszą być naprawdę losowe i niepowtarzalne

- ▲ niezbędne byłoby analiza statystyczna wykazująca, że hasła faktycznie są losowe i niepowtarzalne
- ▲ implementacja testów
- ▲ opracowanie raportu opisującego wprowadzone zmiany - szczegóły implementacyjne oraz sposób konfiguracji

2. Księgowanie obrotów magazynowych (3-6 tyg)

- ▲ dodanie widoku niezaksięgowanych dokumentów obrotowych na potrzeby pracowników sekcji finansowej (być może wystarczy tylko zmiana uprawnień)
- ▲ dodanie mechanizmu księgowania dokumentów obrotowych jako rachunki
 - ▲ rachunek powinien być wstępnie wypełniony danymi z dokumentu obrotowego (jedna pozycja na całą kwotę oraz nr zadania taki jak w dokumencie obrotowym)
 - ▲ możliwość zaksięgowania (podziału) obrotu na więcej niż jedno zadanie
 - ▲ tylko dla obrotów zarejestrowanych (po wydaniu materiałów magazynowych)
 - ▲ tylko dla pracowników sekcji FK
- ▲ dodanie możliwości modyfikacji księgowania rachunku na konkretne zadanie/zadania
- ▲ dodanie w kontroli spójności tj.
 - ▲ sumaryczna wartość rachunku musi się zgadzać z wartością dokumentu źródłowego (w tym przypadku obrotowego),
 - ▲ zabezpieczenie przed wielokrotnym zaksięgowaniem dokumentu obrotowego
 - ▲ modyfikacja dokumentu obrotowego powinna być możliwa tylko dla dokumentów niezaksięgowanych
- ▲ dodanie możliwości od-księgowania dokumentu obrotowego
- ▲ dostosowanie wydruku dokumentu obrotowego do wyglądu obecnie używanych druków samokopiujących
- ▲ implementacja testów interfejsu dla nowej funkcjonalności
- ▲ opracowanie raportu opisującego wprowadzone zmiany - szczegóły implementacyjne oraz sposób konfiguracji
- ▲ problem: obecnie dokumenty obrotowe nie są drukowane z SETI!!! - niezbędne wyszukiwanie ręczne w finansach
 - ▲ zgodnie z zarządzeniem rektora dokumenty obrotowe mają być tworzone na drukach samokopiujących

3. Integracja systemu pomocy z kodem systemu SETI (2-4 tyg. pod warunkiem, że uda się wykorzystać zewnętrzną bibliotekę [WikiText](#))

- ▲ tworzenie pomocy powinno być maksymalnie uproszczone najlepiej przy użyciu wiki-tekstu [najlepiej dialekt trac-wiki] ze wszystkimi standardowymi mechanizmami Wiki m.in: automatyczne linkowanie do stron, odnośniki wewnątrz stron, formatowanie itp)
- ▲ opracowanie struktury katalogów dla plików pomocy, która będzie mogła być łatwo rozbita na komponenty i do której łatwo można wygenerować linki
- ▲ pliki pomocy powinny być wersjonowane w SVN razem z kodem, którego dotyczą
- ▲ automatyczne generowanie spisu treści/indeksu
- ▲ strona startowa pomocy
- ▲ dostęp do pomocy z przeglądarki; możliwość intuicyjnego linkowania stron pomocy z plików jsp (np przy użyciu dedykowanego znacznika linkującego)
- ▲ wygląd spójny z systemem SETI
- ▲ dodanie testów interfejsu sprawdzających poprawność działania pomocy
- ▲ opracowanie raportu opisującego wprowadzone zmiany - szczegóły implementacyjne oraz sposób konfiguracji

4. Rozszerzenie modelu podsystemu BD (2 - 3 tyg.)

- △ wprowadzenie możliwości definiowania wielu promotorów dla przewodów doktorskich - BDD_PRZEWOD_DOKTORSKI
 - △ obejmuje modyfikację definicji typu dokumentów, wyglądu, transformat XSL oraz kodu aplikacji
- △ rozszerzenie zawiadomień, zaświadczeń, itp o obsługę wielu promotorów
 - △ obejmuje modyfikację definicji typu dokumentów, wyglądu, transformat XSL oraz kodu aplikacji
 - △ pozostałe typy dokumentów do modyfikacji:
 - △ BDD_GEN_ZASW_DR- wybór dowolnego z promotorów
 - △ BDD_ZAW_PROM_OTW_PRZEW_DR - wybór dowolnego z promotorów
 - △ BDD_DANE_DLA_DO_DR - wielu promotorów
 - △ BDD_SPL_REC_PRZEW_DR - wielu promotorów
 - △ BDD_ZAL_DO_KARTY_SYN- wielu promotorów
 - △ BDD_ZAW_PUB_OBR_PRZEW_DR - wielu promotorów
 - △ BDD_ZASW_OTW_PRZEW_DR - wielu promotorów
 - △ BDD_ZAW_DO_OTW_PRZEW_DR - wielu promotorów
- △ ew. przygotowanie aplikacji do migracji danych do nowego schematu - jeśli potrzebne
- △ aktualizacja testów interfejsu
- △ opracowanie raportu opisującego wprowadzone zmiany - szczegóły implementacyjne oraz sposób konfiguracji, migracji

rozszerzenia:

- △ nowe filtry dla wszystkich list dokumentów w BD
- △ obsługa nowych typów (Zał. do prot. KPD, Zaproszenie na kolokwium hab.)

5. Rozszerzenie funkcjonalności podsystemu księgowego (4-8 tyg)

- △ poprawki podglądu i wydruku faktury, faktury pro-forma, faktury korygującej i noty księgowej
 - △ dodanie opcji terminu zapłaty "zapłacono"
 - △ dodanie na fakturach, notach pola konto sprzedawcy
 - △ dodanie miejsca na pieczęć wydziału
 - △ dodanie etykiety jednostek miary oprócz kodu
 - △ dostosowanie sposobu nadawania fakturom numerów do wzoru
- △ dodanie możliwości księgowania faktury na więcej niż jedno zadanie ([#1683](#))
- △ dodanie możliwości modyfikacji zaksięgowania faktury
- △ dodanie możliwości od-księgowania faktury
- △ dodanie kontroli spójności księgowania
 - △ sumaryczny zaksięgowany wpływ musi być równy kwocie faktury
 - △ nie powinno być możliwości edycji zaksięgowanej faktury
 - △ zabezpieczenie przed wielokrotnym zaksięgowaniem faktury
- △ dodanie możliwości wystawiania faktur z serwera wyniesionego - tylko dla kierowników zadań i osób upoważnionych
- △ dodanie możliwości podglądu i drukowania faktur na serwerze wyniesionym - tylko dla kierowników zadań i osób upoważnionych
- △ dostosowanie zatwierdzania faktur przez pracownika sekcji finansowo-księgowej do zmian w ich księgowaniu
 - △ zatwierdzenie faktury wiąże się z nadaniem jej numeru i zaksięgowaniem wpływu
- △ implementacja testów interfejsu
- △ opracowanie raportu opisującego wprowadzone zmiany - szczegóły implementacyjne oraz sposób konfiguracji

6. Rozbudowa mechanizmu powiadomień systemu SETI (2-3 tyg)

- ▲ wszystkie powiadomienia wysłane mailem powinny być zapisywane także w SETI
- ▲ możliwość ich przeglądania dla adresata
- ▲ lista nowych (nieprzeczytanych wiadomości na pierwszej stronie SETI (po zalogowaniu)
- ▲ formatka wysyłania z SETI dowolnych powiadomień do dowolnie wybranych osób
- ▲ implementacja testów interfejsu
- ▲ opracowanie raportu opisującego wprowadzone zmiany - szczegóły implementacyjne oraz sposób konfiguracji, migracji

problemy/rozszerzenia:

- ▲ możliwość usuwania wiadomości przeczytanych
 - ▲ usuwanie dla adresata w tej chwili niemożliwe gdyż wymagałoby transferu uprawnień na serwer wyniesiony
- ▲ możliwość ustawienia w preferencjach że nie chce się otrzymywać maili (wymaga api preferencji)
- ▲ automatyczne powiadamianie o nowych wiadomościach dla osób zalogowanych

B. Bezpieczeństwo

7. Audyt bezpieczeństwa serwera wyniesionego w zakresie scenariuszy: (3 - 6 tyg.)

- ▲ uzyskanie dostępu do serwera wyniesionego systemu SETI przez osobę nie posiadającą konta
 - ▲ możliwość włamania się na cudze konto w SETI
 - ▲ możliwość włamania się na serwer
 - ▲ możliwość uzyskania nieuprawnionego dostępu do bazy danych
- ▲ eskalacja uprawnień użytkownika systemu SETI - zał.: osoba posiada konto w SETI
 - ▲ możliwość uzyskania nieuprawnionego dostępu do danych osobowych lub finansowych innych osób
 - ▲ występowanie błędów SQL injection
 - ▲ występowanie błędów XSS
- ▲ atak na serwery przy znajomości kodu źródłowego (np. były lub aktualny członek zespołu SETI)
- ▲ opracowanie raportu opisującego znalezione błędy ze wskazaniem sposobu ich poprawienia/uniknięcia w przyszłości

C. Analiza kodu źródłowego

8. Analizator wykorzystania kodu źródłowego w Javie (2-3 tyg.)

- ▲ zliczanie wszystkich (z pominięciem refleksji) wywołań metod (także publicznych) dla kodu źródłowego zawartego w zadanych pakietach
- ▲ możliwość ograniczenia analizowanego kodu do zadanych klas/pakietów/sciezek (dotyczy tylko listy metod dla których zliczane są wywołania)
- ▲ zliczanie powinno obejmować wywołania z całego dostępnego kodu źródłowego (a jeśli się da to także wszystkich skompilowanych jarów dołączonych do ścieżki)
- ▲ generowanie raportu ze szczególnym uwypukleniem metod, które są nieużywane (mają zero wywołań)
- ▲ możliwość oznaczenia (adnotacje lub w komentarzu) metod jako API lub metody wywoływane refleksyjnie - takie metody w raporcie nie powinny być wskazywane jako nieużywane, lecz jako metody api/refleksyjne
- ▲ integracja narzędzia z [Mavenem](#) lub Antem
- ▲ implementacja testów
- ▲ opracowanie raportu opisującego szczegóły implementacyjne oraz sposób konfiguracji

