Posudek oponenta bakalářské práce

Jméno a příjmení:	*Ladislav Račák*
Název tématu:	*Implementace bezpečnostní vrstvy DCIx*
Oponent:	*Ing. Petr Včelák – KIV*

1 Obsah práce

Snadné pochopení komplikuje struktura dokumentu, která má nejasnou logickou návaznost jednotlivých částí práce – v obsahu i vlastním textu. Přesto informace potřebné k pochopení řešeného problému, způsobu řešení a dosažených výsledků lze v textu práce s větším úsilím nalézt.

Téma je orientováno primárně jako implementační spočívající v nahrazení původní implementace bezpečnostní vrstvy novým přístupem s knihovnou Apache Shiro v komerčním software. Hlavní požadavek byl na zachování původní funkčnosti aplikace a možností autentifikace a autorizace.

Rozsah práce je na hranici doporučených 30 stran textu. Práce obsahuje jednu přílohu se stručným popisem prototypu použití knihovny. Součástí je CD-ROM se zdrojovými kódy prototypu a zdrojové kódy vytvořené implementace bezpečnostní vrstvy v DCIx s již zmíněnou knihovnou.

2 Kvalita řešení a dosažených výsledků

Prezentované řešení plně respektuje kladené požadavky a umožňuje docílit vyššího zabezpečení, než které bylo možné původně. Studentovi se podařilo odstranit bezpečnostní chybu spočívající v neomezeném přístupu k akcím při znalosti konkrétního URL požadavku, který nebyl původně přístup ověřován. Nejdůležitější část řešení spočívá v jedné metodě o 245 řádcích. V této metodě je vedle autentifikace řešena inicializace pracovního prostředí aplikace DCIx. Nutnost inicializace je evidentně dána logikou aplikace DCIx a student tuto část ovlivnit nemohl. Menu aplikace a konkrétní bloky JSP souborů jsou ovlivněny procesem autorizace určujícím k jakým funkcím má uživatel přístup. V práci je uveden ilustrační příklad použití nové bezpečnostní vrstvy v JSP souborech a zdrojové kody implementace pro komerční aplikaci. Komentovány jsou celé bloky kódu stručně, ale jasně. Je to plně postačující, protože jednotlivé řádky jsou snadno pochopitelné dle použitých názvů a identifikátorů. Řešení student ověřil úspěšným provedením akceptačních automatických testů, které byly jen minimálně upraveny na míru nové knihovně.

3 Formální úroveň

Po formální stránce práce obsahuje řadu překlepů, gramatických i typografických chyb. Číslování stran nemá student dle pokynů. Větší obrázky nebo výpisy jsou začleněny přímo do textu dokumentu, nikoliv do příloh.

4 Práce s literaturou

Práce obsahuje pouze 8 zdrojů z nichž student čerpal. Všechny se vztahují k tématu, ale jedná se pouze o zdroje elektronické. Zdroje neobsahují datum aktualizace, pouze datum citování. Výhradu mám ke zdroji [3], kde je citován celý server, nikoliv konkrétní dokument. V textu student často uvádí zdroje na počátku kapitoly a převzaté obrázky nemají zdroj uveden.

5 Splnění zadání

Zadání je splněno s výhradami. Výhrady mám v případě určení splnění bodů (3), (4) a (6) zásad pro vypracování. Uvedené body nejsou jasně vymezeny a v textu se všechny body zásad pro vypracování

mezi sebou prolínají. Za 3. bod (analýza) lze považovat jeden odstavec kapitol 2.1 a 2.2. Body 4 (návrh), 5 (reimplementace) a 6 (otestování) lze s větším usílím nalézt v textech především 5. kapitoly pojmenované „Implementace bezpečnostní vrstvy".

6 Doplňující informace k práci

Student uvádí použití databázového software s akademickou licencí pro nekomerční použití v bakalářské práci zabývající se vývojem komerčního software DCIx.

7 Otázky

1. K jakým konkrétním problémům docházelo při autorizaci použitím dvou samostatných realmů – databáze a Microsoft Active Directory? Proč tento přístup selhal?
2. Jakým způsobem jsou ve finální podobě v použitém jediném realmu pro autorizaci uživatele kombinovány přístupy ověření z databáze a Microsoft Active Directory? Jaké je jejich pořadí nebo priority při rozhodování? Stručně vysvětlete.

8 Hodnocení

Navrhuji hodnocení známkou *velmi dobře* a práci *doporučuji k obhajobě.*

V Plzni 29. 5. 2013

Ing. Petr Včelák
KIV, FAV, ZČU