

Posudek oponenta bakalářské práce

Student: Geffert Maroš
Téma: Autorizační a autentizační řešení na platformě Java (id 24106)
Oponent: Rychlý Marek, RNDr., Ph.D., UIFS FIT VUT

- 1. Náročnost zadání** **průměrně obtížné zadání**

V práci autor porovnává rámce pro zabezpečení Java aplikací a implementuje ukázkovou aplikaci s využitím Spring Security. Použité technologie jsou obecně dobře známé a zdokumentované. Jedná se o průměrně obtížné zadání.
- 2. Splnění požadavků zadání** **zadání splněno**

Zadání je splněno bez výhrad.
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**

Od úvodu po závěr obsahuje technická zpráva 41 vysázených stran a je svým rozsahem v obvyklém rozmezí. Rozsah jednotlivých kapitol je vyvážený, přestože některé jejich podkapitoly se jeví v kontextu okolních jako zbytečné (např. sekce 4.9.5 "Bezpečnostný framework" obsahuje pouze jednořádkový odkaz na jinou sekci).
- 4. Prezentací úroveň předložené práce** **75 b. (C)**

Technická zpráva má logickou strukturu, kde na sebe jednotlivé kapitoly dobře navazují. Oceňuji, že v kap. 3 "Porovnanie autorizačných a autentizačných knižnic" autor zvolil, a následně použil, vhodná kritéria pro porovnání uvažovaných bezpečnostních rámců. Kvalitu textu snižují občasná subjektivní a nepodložená hodnocení autora (např. autor na str. 7, kap. 2.2.3, tvrdí o JAAS, že "aspekty autorizácie boli bezmyšlienkové a frustrujúce", ale dále to nevysvětluje, přestože této technologii je věnována samostatná podkapitola). Také některé návrhové diagramy jsou neformální či chybné (např. v UML Use Case diagramu na obr. 4.2, str. 23, je mezi aktéry použit vztah "extends", který by měl být dle UML používán pouze mezi případy užití a zde by byl vhodnější vztah generalizace-specializace). Nevhodný a nic neříkající je také obr. 4.8, str. 27.
- 5. Formální úprava technické zprávy** **65 b. (D)**

Z hlediska formální úpravy obsahuje technická zpráva řadu drobných chyb: počínaje seznamem kapitol, kde název kapitoly přílohy obsahuje pouze písmeno "A" bez rozlišení od ostatních (ne-přílohových) kapitol; neuvozené odkazy na podkapitoly v podkapitole 5.1 "Autentizácia" str. 32; či chybějící názvy a čísla vložených obrázků a kódu (např. obr. na str. 28-29). I číslované obrázky nejsou občas odkazovány z textu (např. obr. 5.4, str. 38) a není tedy jasný jejich kontext. Je zde také řada typografických nedostatků, přestože nejsou tak závažné: použití spojovníku místo pomlčky (např. str. 15); mezery v textu kolem znaku lomenu (str. 25-26); chybná velikost písmen a chybějící mezery ("JavaMailApi" na str. 33; název podkap. 5.3 "OAuth2.0"; "otp" na str. 44); překlapy (např. "knižncu" na str. 44); použití desetinné čárky na místě oddělovače tisíců (grafy rychlosti na str. 41-42).
- 6. Práce s literaturou** **70 b. (C)**

Seznam literatury obsahuje 24 položek, ve kterých jsou zastoupeny webové zdroje k použitým technologiím i odborné knihy. Všechny zdroje jsou odkazovány v textu práce a je jasný způsob a rozsah jejich použití. V textu se však nachází hodně zdrojů chybně odkazovaných pomocí skrytých hypertextových odkazů (bez viditelného URL), místo kterých by bylo vhodnější použít odkazy do seznamu literatury či alespoň URL v poznámkách pod čarou (např. clean architecture na str. 26, či jwt na str. 29).
- 7. Realizační výstup** **85 b. (B)**

Realizačním výstupem je ukázková Java aplikace využívající rámec Spring Security a mající REST rozhraní. Aplikace je funkční, zdrojové kódy jsou dobře rozvrženy a vhodně komentovány. Pro implementaci kontextu autentizovaného uživatele se autor rozhodl použít vlastní řešení z důvodu minimalizace závislostí, což však mohlo být lépe popsáno. V kontextu zadání a snahy minimalizovat závislosti mohl autor zvýšit nezávislost na konkrétním rámci návrhem vlastní abstrakce.
- 8. Využitelnost výsledků**

Vzhledem k ukázkové povaze aplikace nemají výsledky konkrétní využití, avšak mohou přispět k porozumění daným technologiím při tvorbě skutečné aplikace.
- 9. Otázky k obhajobě**
 - V podkapitole 5.4 "Autorizácia" píšete, že jste se rozhodl nepoužívat Spring Authentication objekty z důvodu minimalizace závislostí a implementoval vlastní řešení. Jaké dodatečné závislosti by vznikly v případě Spring Authentication? Uveďte počet dalších rozhraní a knihoven, jejich velikost, atp., ve srovnání se stávajícím vlastním řešením.

- V práci používáte Spring Security se snahou být nezávislý na konkrétním řešení (vizte předchozí otázka).
Co by se muselo udělat v aplikaci pro nahrazení Spring Security jiným rámcem?

10. Souhrnné hodnocení

75 b. dobře (C)

Výsledkem práce je dobrá ukázková aplikace a technická zpráva s drobnými nedostatky. Celkově považuji řešení za průměrné a navrhuji hodnotit práci stupněm **dobře (C)**.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 3. června 2021

Rychlý Marek, RNDr., Ph.D.
oponent