Posudek oponenta závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Jiří Levý
Oponent práce: Ing. Tomáš Zahradnický, Ph.D.
Název práce: Služba pro zasílání push notifikací
Obor: Webové a softwarové inženýrství

Datum vytvoření: 4. 5. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* *2=náročnější zadání,* ***3=průměrně náročné zadání,*** *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Zadání diplomové práce hodnotím jako středně obtížné.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	*1=zadání splněno,* ***2=zadání splněno s menšími výhradami,*** *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání práce považuji za naplněné s mírnou výhradou. Výhrada spočívá v tom, že implementace pro platformu Windows Phone nebyla v rozporu se zadáním uskutečněna. Rešerše pro tuto část je však provedena řádně. Student uvádí i důvod nesplnění, který akceptuji.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Práce splňuje rozsahem požadavky na diplomovou práci.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*75 (C)*

Popis kritéria:
Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře.

Komentář:
Práce je členěna do 7 kapitol – Úvod, Cíl práce, Vybraná konkurenční řešení, Analýza, Návrh, Realizace a Závěr. Toto členění považuji za vhodné. Mám drobnou výhradu ke kapitole Analýza, která obsahuje části, z nichž mnohé patří do návrhu (první odstavec kapitoly).

Studenta chválím za to, že při návrhu postupuje metodicky a navrhuje a implementuje testy.

Výhrady mám k tomu, že se práce nevěnuje dostatečně bezpečnosti. Ta by měla být součástí návrhu aplikace podle principu SD3 (Secure by Design, Secure by Default, Secure in Deployment) a nevznikat dodatečně. V seznamu literatury nenacházím žádné odkazy do bezpečnostní literatury. Databáze navržená k uložení hesla neobsahuje ani sůl ani počet iterací, které by se použily se studentem navrhovaným algoritmem bcrypt. Nenacházím nic o zabezpečení vlastní komunikace mezi serverem a klientem a ani o zabezpečení databáze MongoDB. To je vidět například na autorizačním tokenu, u kterého student vymýšlí jakési řešení (2 uživatelé se stejným heslem budou mít stejný token), které hašuje uživatelské heslo namísto toho, aby použil například JWT Token (RFC 7519 a RFC 7797), který je právě pro tyto účely.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*75 (C)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Po formální stránce je práce vpořádku s výjimkou prohřešků v jazykové a typografické stránce.

Jazyková stránka. Práce obsahuje množství anglických výrazů (open-source, one page site, landing page, ...), pro které existují české překlady, navíc některé z nich skloňované podle českého pravopisu (routy, wireframu, endpointů, developerského, ...).

Typografická stránka. První polovina práce je vpořádku, druhá obsahuje sem tam vytékající slova ze zrcadla strany (např. str. 39, 51), jednoznakové předložky na koncích řádků atd.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*75 (C)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Práce šetří citacemi. To nepovažuji za vhodné, protože v některých místech citace opravdu chybí. Jako příklad uvádím sekci 4.2.5 na straně 38-39, kde jsou jmenovány mnohé technologie bez jakéhokoliv odkazu na ně.

Seznam literatury obsahuje pouze webové zdroje. Nenacházím žádné odkazy do bezpečnostní literatury ani do knih.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*80 (B)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Student implementoval „další“ nástroj na rozesílání push notifikací pro mobilní telefony, dal k dispozici zdrojový kód a umožnil jeho využití pod MIT licencí.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Nástroj by měl být použitelný pro rozesílání push notifikací.
Jako slabší stránku vidím bezpečnost produktu, která bohužel nebyla příliš součástí návrhu. Některé části nejsou chráněny vůbec, jiné mohou obsahovat injekční chyby. Hesla nejsou uložena dostatečně bezpečně. Autorizační tokeny jsou nestandardní (nemají časovou platnost, nejsou odolné proti změně).
Nástroj není implementován pro platformu Windows Phone.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
1. Model na straně 32 obsahuje tabulku User, ve které je e-mail uživatele a jeho heslo. V textu se dočítám o tom, že heslo je zpracováno hašovací funkcí. Nenacházím zde sůl a počet iterací, které by měly vstupovat do výpočtu hesla podle standardu PBKDF.2. Jakým způsobem se ukládá heslo a jak je chráněno proti útoku pomocí duhových tabulek a útoku hrubou silou?

2. Jak je řešena bezpečnost MongoDB?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*75 (C)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Diplomovou práci pana Bc. Jiřího Levého doporučuji k obhajobě a hodnotím ji stupněm C (dobře).

Podpis oponenta práce: