POSUDEK BAKALÁŘSKÉ PRÁCE

Autor:	Tomáš Smékal
Název:	Návrh a realizace webové aplikace pro sběr a vizualizaci dat z fotovoltaické elektrárny
Posudek vypracoval:	oponent práce RNDr. Ondřej Žára

Těžištěm bakalářské práce je dvojice webových aplikací, které realizují požadovanou funkcionalitu. Rozdělení do dvou komponent, tj. webové služby pro sběr dat a samostatné aplikace pro vizualizaci a správu, považuji za velmi vhodné. Tento přístup je v souladu s aktuálními trendy *Internetu věcí* a architekturou *microslužeb*.

Obě aplikace jsou psány v jazyce PHP, zdrojový kód je dobře čitelný a členěný. Autor při implementaci využil i některé nadstandardní techniky, jako například zachování mazaných databázových položek a detailní záznam průběhu importování dat. To svědčí o promyšleném návrhu celého systému.

K práci mám několik kritických připomínek:

1. **V textu práce schází důležité části.** Rozhraní REST, které bylo navrženo pro komunikaci s webovou službou, je zcela nedokumentováno. Dočteme se jen velmi hrubý popis JSON formátu odpovědi, ale výčet požadavků a jejich parametrů chybí. Ve zdrojovém kódu je jisté množství dokumentačních komentářů, ale v příloze práce není automaticky generovaná dokumentace. V části 2.6 nejsou vůbec uvažovány NoSQL databáze, které by přitom – s ohledem na mnohotvárnost vstupních dat – mohly být velmi dobrou volbou.

2. **V textu práce jsou některé zavádějící údaje.** Několikrát je zmíněna HTTP metoda `UPDATE`, která neexistuje. V části 4.1.2 je zmíněna konfigurace webového serveru pro HTTP autorizaci pomocí MySQL, ale webová služba používá autorizaci souborem `.htpasswd`. V části 3.1.2.1 je popsána hodnota `ERROR_CODE` jako číslo chyby, nicméně například pokus o přihlášení s chybným heslem končí hodnotou 0 (tj. chyba nenastala).

3. **Vstup od uživatele je velmi slabě ošetřen.** Webová služba je učebnicovou ukázkou zranitelností *SQL injection*, kdy vstupní parametry nepodléhají žádné transformaci a do SQL dotazů jsou vkládány nechráněné. Klientská aplikace při komunikaci s webovou službou neprovádí URL kódování lomítek (což způsobí nežádoucí chování aplikace, jakmile se znak lomítka objeví v libovolném uživatelském vstupu) a vstupní parametry chybně ošetřuje ekvivalentem funkce `htmlspecialchars` (což způsobí nežádoucí chování aplikace, jakmile se na vstupu objeví některý z transformovaných znaků).

4. **Další bezpečnostní nedostatky.** Ověření jména a hesla probíhá pomocí HTTP metody GET, heslo se tedy velmi pravděpodobně dostane do logů webového serveru. Pro hashování hesel je použita statická sůl. V textu je několikrát zmíněn protokol HTTPS, ale část 4.1 s konfigurací webového serveru o HTTPS mlčí. Ani poskytnutá instalace aplikace a webové služby není dostupná po HTTPS.

S ohledem na poslední dva body, které výraznou měrou ovlivňují bezpečnost aplikace, hodnotím bakalářskou práci známkou **C – dobře**.

V Praze dne 23. ledna 2017 RNDr. Ondřej Žára