POSUDEK BAKALÁŘSKÉ PRÁCE

Autor:	Jakub Zelenka
Název:	Online aplikace pro zdravotnickou ordinaci
Posudek vypracoval:	oponent práce RNDr. Ondřej Žára

Bakalářská práce realizuje informační systém pro zdravotnickou ordinaci, který se soustředí zejména na evidenci pacientů, organizaci jejich návštěv a správu vydaných receptů. Jedná se o komplexní aplikaci s webovým rozhraním a koncepčně odděleným REST API. Z uživatelského pohledu je web dobře funkční, i když pro náhodného recenzenta může být uživatelské rozhraní občas matoucí. Jistě by v tomto prospěly titulky, které bohužel schází u víceméně všech interaktivních prvků ve stránce. Klíčové požadované funkce jsou nicméně naimplementovány a fungují.

Text práce je na výborné jazykové a typografické úrovni a tradiční drobné nedostatky (uvozovky použité pro zvýraznění, *copy-paste* chyby) se vyskytují v přiměřeném množství. V práci bohužel není ani jeden obrázek uživatelského rozhraní výsledné aplikace. Zdrojový kód (PHP framework Symfony, JS knihovna Vue.js) je dobře dokumentován a k projektu existuje užitečná automaticky generovaná dokumentace.

Jedinou mojí výhradou tak zůstává otázka zabezpečení. V zadání práce je bezpečnost uživatelských dat explicitně zmíněna, nicméně v praxi k žádnému zabezpečení nedochází. Přestože je v aplikaci připraven jistý autorizační mechanismus, jeho použití není nikde vynuceno a data jsou tak volně přístupna. Tato skutečnost je v textu práce zmíněna, ale to dle mého názoru nesnižuje závažnost takového nedostatku.

Připravená bezpečnostní infrastruktura staví na neotřelém, ale dle mého názoru nevhodně zvoleném konceptu klientských tokenů JWT. Tyto jsou určeny k použití v HTTP hlavičce `Authorization`, což zcela eliminuje bezpečnostní riziko CSRF. Nicméně:

1. **Došlo k zásadnímu zesílení bezpečnostního rizika XSS.** Citlivé údaje (autorizační token) jsou uloženy v `localStorage`, což je v přímém rozporu s doporučeními organizace OWASP. Každý kód třetí strany tak má plný přístup k autorizačnímu tajemství přihlášeného uživatele.
2. **Autorizační tokeny nejsou ukládány na serverové straně.** Kvůli tomu nelze auditovat přihlášení a provádět jejich revokaci. Tokeny proto mají jen velmi krátkou životnost a pokud správně chápu implementaci (nebylo možno vyzkoušet v praxi), bude přihlášený uživatel každou hodinu nucen k opětovnému přihlášení.

Bakalářská práce bohužel nevysvětluje, na základě jakých rozhodnutí bylo přistoupeno k realizaci netradičního mechanismu JWT, v porovnání například s běžnými HTTP cookies.

Bezpečnostní aspekt práce považuji za výtku, která značně ovlivňuje hodnocení jinak výborného výsledku. Proto navrhuji bakalářskou práci ohodnotit známkou **C – dobře**.

V Praze dne 17. ledna 2018 RNDr. Ondřej Žára