Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: Ondřej Boura

Název práce: Zabezpečení webových aplikací

Autor posudku: Pavel Kříž

Cíl práce: Účelem této práce je poskytnout lidem zabývajícím se zabezpečením webových aplikací přehled možných útoků na webové aplikace a přehled možností, jak zabezpečení aplikace realizovat.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)			
	1	**2**	**3**	**4**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐
Vymezení cíle a jeho naplnění	☒	☒	☐	☐
Zpracování teoretických aspektů tématu	☐	☒	☐	☐
Zpracování praktických aspektů tématu	☒	☐	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☒	☐	☐	☐
Hloubka a správnost provedené analýzy	☐	☒	☐	☐
Práce s literaturou	☒	☐	☐	☐
Logická stavba a členění práce	☒	☐	☐	☐
Jazyková a terminologická úroveň	☒	☒	☐	☐
Formální úprava a náležitosti práce	☒	☐	☐	☐
Vlastní přínos studenta	☐	☒	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☒	☐	☐	☐

Dílčí připomínky a náměty:

Z hlediska terminologie bych nedoporučil překládat výraz „flags“ jako „vlajky“ v kontextu např. „session cookie secure flag“ (např. nadpis „4.5.2 Využití bezpečných vlajek“ na str. 46). Uvedený termín se v odborné literatuře překládá obvykle jako „příznaky“ nebo se ponechává nepřeložen. I po odborné stránce je kapitola 4.5.2 nepřesná. Autor uvádí, že nastavením „secure flag“ u cookies lze zašifrovat cookie během komunikace mezi klientem a serverem a že stejného výsledku by bylo možné dosáhnout využitím HTTPS, které šifruje veškerou komunikaci. Význam „secure flag“ ovšem spočívá v tom, že prohlížeč takto označenou cookie zasílá pouze přes zabezpečený kanál, tedy HTTPS. Nejde tedy o dvě konkurující si řešení, jak vyznívá z textu autora. Naopak, obě možnosti se vzájemně doplňují tak, aby bylo zajištěno, že cookie nebude odeslána přes nezabezpečené HTTP spojení.

Celkové posouzení práce a zdůvodnění výsledné známky:

Ondřej Boura zpracoval bakalářskou práci na téma zabezpečení webových aplikací. Na podobné téma byla zpracována již celá řada závěrečných prací a je překvapivé, že autor žádnou z podobných prací necituje. Cíl práce považuji převážně za splněný, nicméně práci bych doporučil pouze začátečníkům v této oblasti, nikoliv „lidem zabývajícím se zabezpečením webových aplikací“ (viz cíl), protože text není ani uceleným přehledem (zabývá se pouze čtyřmi typy zranitelností), ani odborně precizním popisem problematiky.
Ovšem jako úvod do problematiky může tento text velmi dobře posloužit všem autorům webových aplikací, kteří stojí před důležitým úkolem ochránit svou aplikaci před nejčastějšími typy útoků. Bakalářská práce Ondřeje Boury je psána srozumitelně a vhodně doplněna ukázkami zdrojových kódů převážně v HTML a jazyce Java. Práce odpovídá metodickým pokynům. Zdrojové kódy webové aplikace, na které bylo zabezpečení demonstrováno, jsou vystaveny na serveru GitHub.com.

Práci doporučuji k obhajobě.

Otázky pro diskusi:

Jakou roli v problematice zabezpečení webových aplikací hraje organizace OWASP?

Navržená výsledná známka: výborně - velmi dobře (podle výsledku obhajoby)

V Hradci Králové**, dne** 11.5.2015

podpis