Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Jméno studenta: Josef Čejka

Název práce: Nástroje pro penetrační testování webových aplikacía jejich praktické využití

Autor posudku: Ing. Jiří Štěpánek

Cíl práce: Seznámení s volně dostupnými nástroji pro penetrační testování a jejich možnostmi, popsání jejich použití pro daný účel.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)			
	A	**C**	**E**	**F**
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:

Na straně 57 autor uvádí, že TFS je placený nástroj, což není nutně pravda.
Vzhledem k současnému rozsahu práce a k tématu bych očekával minimálně jeden ukázkový příklad celého řetězce testů na konkrétní aplikaci – od průzkumu po konkrétní zneužití zranitelnosti, které vyústí například ke zcizení dat. Stejně tak by bylo dle mého názoru vhodné u popisovaných typů zranitelností popsat i běžná opatření (např. XSRF + validační token).

Celkové posouzení práce a zdůvodnění výsledné známky:

Autor ve své práci seznamuje s problematikou zabezpečení webových aplikací. Penetrační testování používá jako nástroj pro ověření určitých aspektů bezpečnosti jednotlivých aplikací. V úvodní části představuje základní terminologii a nejčastější chyby ve webových aplikacích. V další části jsou představeny linuxové distribuce, které obsahují celou škálu bezpečnostních nástrojů a poslouží nejen k účelům této práce. Následuje kapitola, ve které jsou přehledně rozděleny bezpečnostní nástroje do několika skupin podle svého účelu – nástroje pro průzkum, trenažéry, nástroje pro

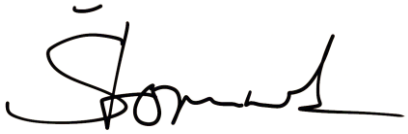
provádění konkrétních útoků. Závěrečná kapitola je věnována vývojové metodě Continous Integration, která napomáhá při tvorbě zabezpečených webových aplikací.
Diplomová práce je pečlivě zpracována, dobře logicky členěna. Jednotlivé nástroje jsou adekvátně popsány. Vzhledem ke zvolenému tématu mi v práci ovšem chybí bližší ukázka popisovaných technik, včetně popisu opatření. Cíl práce byl naplněn, výsledkem je ucelený materiál popisující bezpečnostní rizika webových aplikací a nástrojů pro jejich testování. Práce splňuje metodické pokyny.

Otázky k obhajobě:

Práci doporučuji k obhajobě.

Navržená výsledná známka: B - výborně-velmi dobře

V Mladé Boleslavi**, dne 19. května 2017**



podpis