Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTKY DIPLOMOVÉ PRÁCE

Jméno studenta: Tomáš Janeček

Název práce: Bezpečnost webových aplikací v PHP

Autor posudku: Daniela Ponce

Cíl práce: Poskytnout přehled nejčastějších technik prolomení zabezpečení webových aplikací, pokrýt typické způsoby penetračního testování a navrhnout optimální strategii zabezpečení webových aplikací v PHP.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**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)	☒	☐	☐	☐	☐	☐

Vyjádření k výsledku anti-plagiátorské kontroly

Výsledkem antiplagiátorské kontroly je podobnost 0%.

Dílčí připomínky a náměty:

Cílem práce je mimo jiné navrhnout optimální strategii zabezpečení aplikace. Postrádám v práci vysvětlení a zdůvodnění, podle jakých kritérií se optimálnost strategie zabezpečení posuzuje.
Kapitola 5 se věnuje obraně proti hrozbám v PHP. Nicméně, obsahuje i obecný výklad, jehož platnost není omezena jen na jazyk PHP (např. 5.2.1 hashovací algoritmy, 5.2.2 zásady bezpečného zacházení se session, 5.4.1 kategorizace XSS útoků, 5.5 popis útoku CSRF).

Celkové posouzení práce a zdůvodnění výsledné známky:

Práce podává přehled nejčastějších technik prolomení zabezpečení webových aplikací, a to jak obecně, tak specificky pro jazyk PHP; dále jsou představeny metody ochrany před těmito technikami. Tyto metody ochrany jsou následně demonstrovány na zabezpečení ukázkové aplikace a jejich účinnost je ověřena jedním konkrétním testem vybrané metodiky penetračního testování. Součástí práce je rovněž přehledový popis typických způsobů penetračního testování.
Problematika je podaná jasně, přehledně, vyváženě a správně, s logickým členěním a uspořádáním. Praktická ukázka velmi dobře souvisí s teoretickým výkladem, je sestavena správně, účelně a názorně.
Jazyková a formální stránka práce má vysokou úroveň.
Stanoveného cíle diplomové práce bylo dosaženo.

Otázky k obhajobě:

1) Možné zabezpečení webové aplikace v PHP demonstrujete na ukázkové aplikaci a testujete jeho funkčnost použitím testu typu reversal dle metodiky OSSTMM (Open Source Security Testing Methodology Manual). Proč považujete za vhodný právě tento test? Vedlo by použití jiného testu (příp. i jiné metodiky) k závěru, že demonstrované zabezpečení ukázkové aplikace má bezpečnostní mezery?
2) Která místa zabezpečení ukázkové aplikace a proč by bylo nutné prověřit v případě změny použitého PHP ekosystému (verze jazyka PHP, verze použitého PHP frameworku, změna hostingu)?

Práci doporučuji k obhajobě.

Navržená výsledná známka: A

V Hradci Králové**, dne 23. května 2018.**

_____

podpis