Posudek oponenta diplomové práce

1. Identifikační údaje

Název práce: **Zranitelnosti moderních webových aplikací**

Autor práce: **Bc. Radek Knytl**

Vedoucí práce: **Ing. Soňa Neradová, Ph.D.**

2. Cíl práce a jeho naplnění

Cílem práce bylo popsat nejčastěji se vyskytující zranitelnosti webových aplikací, vysvětlit metodiky testování úrovně zabezpečení aplikací, představit příslušné nástroje a navrhnout a realizovat případovou studii založenou na penetračním testování.

Autor naplnil stanovený cíl práce a dodržel zásady pro zpracování diplomové práce.

3. Obsahové zpracování (výstup DP) a přístup k řešení (použité metody a ověření výsledku)

Téma práce je vysoce aktuální – práce se zabývá problematikou zabezpečení webových aplikací a je plně zaměřena na zadané téma.

Diplomová práce přináší následující **výstupy**:

- ucelený přehled zranitelností webových aplikací a útoků na ně,
- přehled testovacích nástrojů se stručnými doporučeními k jejich použití,
- vytvořenou testovací aplikaci E-knihovna (včetně popisu použitých technologií a graficky vyjádřeného návrhu),
- vytvořený testovací plán založený na 5 scénářích.

Po obsahové stránce práci hodnotím jako vysoce nadprůměrnou a precizně zpracovanou. Autor se v rozsahu a na úrovni odpovídající diplomové práci vyjádřil ke všem skutečnostem spojeným s naplněním stanoveného cíle práce. Nezapomněl ani na legislativní stránku problematiky, která je v případě experimentálního ověřování úrovně zabezpečení velmi důležitá. Mezi klíčové kapitoly práce patří především kapitola 6, kde autor popisuje svou případovou studii. Kladně cením autorův přístup, zpracování práce v tomto rozsahu je časově velmi náročné.

Autor zvolil systémový a správný přístup k řešení problému. Využil **odpovídající metody**, postupy a nástroje, včetně vlastního experimentu (případové studie) penetračního testování. Pro penetrační testování si autor vytvořil vlastní webovou aplikaci E-knihovna a testovací plán založený na 5 scénářích.

4. Prokázání správnosti navrženého řešení

Celé navržené řešení bylo prakticky realizováno a tím byla ověřena jeho funkčnost. V příloze DP jsou uvedeny všechny výstupy z jednotlivých testů.

5. Struktura, jazyková stránka, formální náležitosti a úprava

Autor předložil práci v rozsahu 106 číslovaných stran (včetně 3 příloh). Práce je uspořádána logicky. Svým větším rozsahem odpovídá řešenému problému.

Práce je psána srozumitelným jazykem, na adekvátní úrovní vyjadřování.

Po formální stránce je práce zpracována čistě, přehledně, úpravně a na odpovídající úrovni sdělování. Lze jí vytknout minimum překlepů a nedostatků po stránce gramatické, stylistické a typografické.

6. Připomínky a otázky

V úvodu práce mohl autor zdůraznit závažnost problematiky uvedením odpovídajících statistik, získaných např. ze stránek organizace CERT.

V kap. 3.2 by bylo vhodné citovat zdroje v každé nečíslované podkapitole textu.

Kap. 6.1 je rozdělena pouze na jednu číslovanou podkapitolu.

V práci mohl být důkladněji zdůvodněn výběr konkrétních nástrojů. Zajímavé by bylo např. pokrytí zranitelností ze seznamu OWASP Top 10 – 2013 jednotlivými nástroji, nejlépe uvedené v přehledné shrnující tabulce.

V závěru autor uvádí, že vytvořená aplikace E-knihovna záměrně obsahuje určité zranitelnosti. V textu práce není uvedeno, o které konkrétní zranitelnosti se jedná, je uveden pouze obecně formulovaný odkaz na zranitelnosti popsané v kap. 4.

V textu práce mohlo být úplně popsáno testovací prostředí, nejen použitý operační systém.

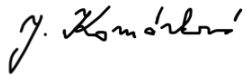
Prosím autora, aby u obhajoby **odpověděl** na následující **otázky**:

1. Uveďte, jaké konkrétní zranitelnosti jste záměrně zanechal v aplikaci E-knihovna.
2. Jakým způsobem byste určil prioritu zabezpečení aplikace proti identifikovaným zranitelnostem v situaci, kdy by aplikace měla sloužit svému účelu v knihovně?

7. Závěrečné doporučení

Výše uvedené drobné nedostatky rozhodně nesnižují kvalitu práce. Práci proto **doporučuji** k obhajobě a hodnotím ji stupněm

výborně



Pardubice, 26. května 2016

doc. Ing. Jitka Komárková, Ph.D.
Ústav systémového inženýrství a informatiky
Fakulta ekonomicko-správní
Univerzita Pardubice