Posudek vedoucího bakalářské práce

1. Identifikační údaje

Název práce: **Útoky na webové aplikace**
Autor práce: **Jan KOLÍNEK**

2. Cíl práce a jeho naplnění

Cílem práce bylo zjistit, jakým způsobem lze v současné době útočit na webové aplikace, jaké jsou možnosti obrany proti těmto útokům a zároveň vytvořit alespoň jednu multimediální prezentaci pro výuku, která bude obsahovat předvedení útoku na běžnou volně šiřitelnou webovou aplikaci. Autor zpracoval dané téma na úrovni dostatečné pro bakalářskou práci a naplnil celkový cíl práce.

3. Obsahové zpracování a přístup k řešení

Kapitoly jsou uspořádány logicky, práce svým rozsahem odpovídá zadanému tématu. V úvodních kapitolách je zmíněna architektura webových aplikací, v následující části práce jsou zmíněny obvyklé typy útoků na ně. Poslední část práce se zabývá přípravou testovacího prostředí s běžně používanou webovou aplikací WordPress a provedení dvou druhů útoků na tuto aplikaci. Tyto útoky, včetně instalace aplikace, jsou detailně popsány v tutoriálech 1 až 3 a postup jednotlivých akcí je přiložen na CD ve formě filmu.

Autor přistupoval k řešení dané problematiky samostatně.

4. Formální náležitosti a úprava

Práce je zpracována čistě a přehledně. Lze jí vytknout některé drobné nedostatky jako například nekvalitní provedení obrázku 3, ukázkový skript na straně 31 začíná tagem </script> a nevhodnou formulaci na straně 19, že funkce mysql_real_escape_string() „odstíní“ speciální znaky.

5. Připomínky

Autor v práci u některých typů útoků nedostatečně ozřejmil praktickou obranu webových aplikací proti uvedeným útokům (například v kapitolách 3.2.2 a 3.2.3) a zůstává pouze u obecného tvrzení, například že každý vstup musí být ošetřen.

Práci **doporučuji k obhajobě** a hodnotím ji stupněm

velmi dobře

Pardubice, 31. srpna 2009

Martin Novák