Posudek vedoucího diplomové práce

Diplomant:	Martin Pieš
Název diplomové práce:	Systém pro detekci napadení databáze metodou SQL injection
Rok odevzdání:	2009
Vedoucí diplomové práce:	Doc. Ing. Václav Jirovský, CSc.
Konzultanti:	

Diplomová práce Martina Pieše je soustředěna na zpracování přehledu používaných technik pro napadení databáze metodou SQL injection, analýz těchto metod, navržení možných způsobů detekce nebo obrany, a vytvoření testovací aplikace umožňující demonstraci práce zvoleného typu ochrany. Práce obsahuje 127 stran včetně seznamu literatury a CD.

V prvních kapitolách je po krátkém úvodu popsán problém a vytvořena taxonomie útoků pomocí metody SQL injection. Ve třetí kapitole se diplomant zabývá možnostmi detekce zranitelného místa a následovně uvádí obtíže, které se vyskytují při detekci útoku využívajícího SQL injection. Analytická část je uzavřena souhrnem a zhodnocením známých metod útoku. V šesté kapitole si diplomant vytváří předpolí pro vytvoření obranného systému, když shrnuje doporučení pro vývoj bezpečného systému, které v následujících kapitolách vyústí v návrh obranného systému a jeho implementaci. Závěr práce je soustředěn na testování a zhodnocení dosažených ukazatelů – pravděpodobnosti falešného poplachu a pravděpodobnosti nezjištění útoku.

Cíl práce, kterým bylo získání přehledu v útocích typu SQL injection, vytvoření jejich kategorizace a návrh vzorového systému detekce napadení databáze uvedenou metodou byl touto prací splněn. Práce je psána hutným stylem, avšak řada uváděných příkladů umožňuje snadnější pochopení diplomantových úvah. Grafické členění práce a její strukturovanost jsou na velmi dobré úrovni a lze konstatovat, že diplomant prokázal schopnost samostatné tvůrčí práce s odpovídající prezentací dosažených výsledků. Práce jako taková dává přehled o používaných technikách útoku SQL injection a i když detekci nelze obecně snadno algoritmizovat, jak správně diplomant uvádí na počátku práce, nalezené a navržené způsoby dávají vysokou pravděpodobnost úspěchu detekce útoku.

Za vhodné lze považovat rozdělení v komponentovém modelu, i když pojmenování „fyzický pohled" není principiálně korektní. Analýza aplikací a zasílaných dotazů je velmi zajímavou částí práce a lze se domnívat, že shrnutí z cca 38 tisíc řádků kódu je dostatečně reprezentativní pro uvedené závěry. Následující implementace detekčního mechanizmu vychází z hostitelské databáze H2, což vzhledem k cíli práce a možnostem, které tato volba umožňovala, je odpovídající. Jistě by bylo zajímavé zjistit chování databází často používaných ve velkých rutinně provozovaných systémech, např. Oracle, ale taková studie sama o sobě by byla příliš náročná a mimo požadovaný rozsah práce.

S ohledem na prokázanou kvalitu diplomové práce, vedoucí práce konstatuje, že bylo splněno zadání a požadavky na diplomovou práci, a tak **doporučuje práci k obhajobě**. Zároveň vedoucí práce navrhuje, aby s ohledem na skutečnosti uvedené v této diplomové práci nebylo použito ustanovení §47b zákona o vysokých školách v celé šíři a práce byla prezentována pouze krátkým souhrnem uvedeným v jejím úvodu. Případné vyžádání práce k nahlédnutí by mělo být řádně dokumentováno (např. záznamem o výpůjčce v knihovně)

V Praze dne 29. ledna 2010

Doc. Ing. Václav Jirovský, CSc.