Posudek diplomové práce

Detekce škodlivého kódu ve webových aplikacích

pana Edvarda Rejthara (dále jen „student“)

Úkolem studenta bylo zpracovat rešerši škodlivého software, napadajícího webové prezentace a implementovat program, detekující takový software ve webových stránkách a napojit jej na existující software vyvíjený společností CZ.NIC. Práce byla vedena odborníkem z CZ.NIC s mým akademickým vedením.

Rešeršní část pečlivě popisuje studentovy zkušenosti se škodlivým software, chybí zde však širší teoretické uvedení do kontextu zpracovávaného tématu. V popisu existující aplikace Malicious domain manager (MDM) obsažené snímky obrazovky mají nízké rozlišení a cenzurou některých údajů nemají příliš vysokou výpovědní hodnotu.

V další části student popisuje současné problémy aplikace MDM a jak tyto problémy vyřešit. V kapitole 4.4.2 student dospěl k tomu, že nejlepší bude napsat vlastní analyzér, zdůvodnění tohoto rozhodnutí však zde chybí.

V kapitole implementace je slovně popsáno, která komponenta jak funguje, diplomová práce by však měla obsahovat i zdůvodnění volby prostředí pro implementaci (nástroje, jazyk), strukturu databázových tabulek, návod na propojení a zprovoznění jednotlivých komponent.

Práce je dobře strukturovaná formátovaná, obsahuje však nezanedbatelné množství drobných chyb (překlepy, bezvýznamová slova, neshodu podmětu s přísudkem, atd) – práci mohl někdo před odevzdáním ještě jednou pečlivě projít.

Dotazy:

- V analýze uvádíte nástroje urlQuery a Sucuri. Zkoumal jste i jiné nástroje před rozhodnutím psát vlastní? Analýza neobsahuje důvody volby právě těchto dvou nástrojů a zdá se mi nepravděpodobné, že by jiné nástroje neexistovaly.
- Nezdá se Vám navržená metoda analýzy stránky mírně těžkopádná? Co si myslíte o možnosti stáhnout kód do nějakého nástroje, který by heuristicky vyhodnocoval chování javascriptového kódu?
- Jaké množství stránek jste schopni nástrojem zpracovat? Není mi jasné, jakým způsobem probíhá vyhledávání webových stránek pro analýzu.

Výsledek odvedené práce považuji za vynikající, dokumentace však mírně pokulhává. Práci doporučuji k obhajobě a hodnotím stupněm

B – velmi dobře.

V Praze, 31.1.2016
Ing. Michal Medvecký
vedoucí diplomové práce