POSUDEK DIPLOMOVÉ PRÁCE

Autor: *Bc. Edvard Rejthar*
Název: *Detekce škodlivého kódu ve webových aplikacích*
Posudek vypracoval oponent práce: *Ing. Peter Macejko*

Autor ve své práci zpracovává téma detekce škodlivého kódu na webových serverech. Cílem je rozšířit a uživatelsky zpříjemnit detekci takovýchto kusů kódu.

Autor začíná vysvětlením motivace zadání práce (kap. 1.) a pokračuje popisem systému, který má rozšířit (kap. 2). V další kapitole (kap. 3) se nachází analýza různých způsobů útoků na webový prohlížeč uživatele a krátké shrnutí možnosti obrany proti těmto útokům (jak na straně uživatele, tak na straně serveru). V následující kapitole (kap. 4) je návrh systému, kde je popsáno proč autor došel k závěru implementovat zadaní pomocí 2 oddělených řešení. Další kapitola (kap. 5) popisuje již stručně samotnou implementaci obou částí. Závěr práce se skládá z kapitoly o testování (kap. 6), diskuzi výsledků (kap. 7) a následně shrnutí přínosu celé práce (kap. 8).

Z práce jde poznat, že autor zpracovávanému problému rozumí. A v rámci textu předkládá nejednu zajímavost z této oblasti. V práci jsem bohužel nenašel podrobnější rozbor proč nedošlo k rozšíření funkčnosti existujícího systému MDM, ale použil se modul do prohlížeče na straně obsluhy aplikace. Což také souvisí s tím, že kapitola (č. 3) Analýza by měla být obsáhlejší a více zaměřená na objasnění zvolených postupů v rámci návrhu a následné implementace finálního řešení. Také je nutno upozornit, že na CD se nenachází část zdrojových kódů, pravděpodobně z důvodu utajení autentizačních mechanizmů CZ.NIC, což ale v práci není nikde zmíněno.

Po formální stránce má práce velké množství malých i větších chyb. V práci se vyskytuje veliké množství překlepů a stylistických chyb. Práce se nedrží doporučovaných přístupů k citaci literatury, odkazy na obrázky jsou velmi špatně zpracovány a místy matoucí. Seznam obrázků je na nestandardním místě a v anglickém jazyce. Co se ještě týče samotných obrázků, tak mám výhrady ke způsobu provedení anonymizace dat, které zachycují. Co se týče obsahu CD, tak na něm chybí některé zmiňované výstupy práce (funkční konfigurace Firefoxu) a také textová verze samotné práce.

Celkově práce splnila zadání a je na velmi dobré technické úrovni, dolů ji však sráží nedostatečná dokumentační část.

K autorovi mám tyto otázky:

1. Proč nebylo možné rozšířit/opravit/optimalizovat funkci stávajícího systému MDM?
2. Jaká je finální HW konfigurace virtuálního stroje pro „analyzér“ a jaká je jeho průměrná výkonnost (počet analyzovaných podezřelých stránek za hodinu)?

Předloženou diplomovou hodnotím známkou: **C – dobře**

V Praze 29.1. 2016
Peter Macejko