Posudek bakalářské práce

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze

Autor práce	Natália Tyrpáková		
Název práce	IDE Support for PHP Code Analysis		
Rok odevzdání	2014		
Studijní program	Informatika	**Studijní obor**	Programování
Autor posudku	David Hauzar	**Role**	Vedoucí
Pracoviště	KDSS		

Prosím vyplňte hodnocení křížkem u každého kritéria. Hodnocení *OK* označuje práci, která kritérium vhodným způsobem splňuje. Hodnocení *lepší* a *horší* označují splnění nad a pod rámec obvyklý pro bakalářskou práci, hodnocení *nevyhovuje* označuje práci, která by neměla být obhájena. Hodnocení v případě potřeby doplňte komentářem. Komentář prosím doplňte všude, kde je hodnocení jiné než *OK*.

K celé práci	lepší	OK	horší	nevyhovuje
Obtížnost zadání	☒	☒	☐	☐
Splnění zadání	☐	☒	☐	☐
Rozsah práce *… textová i implementační část, zohlednění náročnosti*	☒	☒	☐	☐

Komentář Obtížnost zadání a rozsah práce považuji za spíše vyšší. Autorka práce sice měla k dispozici analyzátor WeVerca, který provádí statickou a syntaktickou analýzu kódu a hledá v kódu některé chyby, nástroj ale prováděl pouze jednoduchou bezpečnostní analýzu a nebylo ho možné přímo použít pro vizualizace využitelné k hledání bezpečnostních chyb. Nástroj například obsahoval implementaci taint analýzy, která neumožňovala vizualizovat tok dat z uživatelských vstupů do kritických příkazů.

Autorka práce tedy kromě návrhu vhodného způsobu vizualizace výstupů nástroje musela navíc (1) nastudovat problematiku bezpečnostních útoků, aby zjistila, které informace můžou vývojářům sloužit k odhalení bezpečnostních chyb v kódu, (2) seznámit se s technikou statické analýzy a taint analýzy a navrhnout rozšíření statické taint analýzy tak, aby byla schopná zjistit informace z bodu (1), (3) rozšířit analyzátor WeVerca o implementaci navržené taint analýzy.

Textová část práce	lepší	OK	horší	nevyhovuje
Formální úprava *… jazyková úroveň, typografická úroveň, citace*	☒	☒	☐	☐
Struktura textu *… kontext, cíle, analýza, návrh, vyhodnocení, úroveň detailu*	☐	☒	☐	☐
Analýza	☒	☒	☐	☐
Vývojová dokumentace	☐	☒	☐	☐
Uživatelská dokumentace	☐	☒	☐	☐

Komentář Práce je psána v angličtině, jazyková úroven je dobrá, text obsahuje pouze minimální množství gramatických chyb a překlepů. Text by ale mohl být jasnější a na většině míst i stručnější.

Ocenuji analýzu problému. Práce (1) podrobně rozebírá různé typy bezpečnostních útoků a dává dobrý přehled o tom, které informace jsou třeba pro odhalení těchto útoků. Dále práce (2) obsahuje úvod do syntaktické a statické analýzy, který dává přehled o tom, jak tyto analýzy fungují, jaké informace mohou tyto analýzy poskytnout a částečně i o tom, v jakých případech jsou tyto analýzy použitelné. Práce také (3) obsahuje informace o použitém nástroji WeVerca, zejména informace důležité pro rozšíření nástroje o implementaci taint analýzy.

Dále oceňuji pečlivé zpracované vyhodnocení. Práce obsahuje přehledný popis toho, jak je možné vytvořené vizualizace použít k hledání všech bezpečnostních chyb popsaných v práci. Dále práce obsahuje vyhodnocení časového overhead analýzy a pokouší se vytvořený nástroj srovnat s existujícími nástroji.

Jednotlivé části práce jsou někdy nedostatečně zasazené do kontextu práce. Nejvýraznější příklad je část 1.1 PHP Security, kde není vysvětlené, proč je tato část z hlediska práce důležitá, jaké informace pro řešení práce přináší.

Části analýza a implementace by mohly být lépe propojené. Část 2 Problem Statement and Goals, která se o propojení snaží, obsahuje příliš málo konkrétních informací. I když analýza práce obsahuje dle mého názoru všechny důležité informace, ocenil bych, když by tyto informace byly shrnuté a na základě toho by bylo explicitně uvedeno, co se bude vizualizaovat a jak a uvedeno o zjišťování čeho se musí použitý analyzátor rozšířit.

Implementační část práce	lepší	OK	horší	nevyhovuje
Kvalita návrhu *… architektura, struktury a algoritmy, použité technologie*	☐	☒	☐	☐
Kvalita zpracování *… jmenné konvence, formátování, komentáře, testování*	☐	☒	☐	☐
Stabilita implementace	☐	☒	☐	☐

Komentář Oceňuji, že autorka práce prokázala schopnost nastudovat a netriviálně rozšířit/použít poměrně rozsáhlý program/API – analyzátor WeVerca (cca 1 kloc kódu) a API pro tvorbu Eclipse pluginů.

Dále oceňuji, že část implementace, která rozšiřuje analyzátor, je pečlivě otestovaná pomocí unit testů.

Celkové hodnocení Výborně
Práci navrhuji na zvláštní ocenění Ne

Datum 9. 6. 2014 **Podpis**