Review of Bachelor's Thesis

Student: Zádrapa Jan
Title: Secure Coding Guidelines for Python (id 24958)
Reviewer: Holop Patrik, Ing., DITS FIT BUT

1. Assignment complexity **average assignment**

Úspešné zvládnutie práce vyžadovalo zoznámenie sa s problematikou bezpečného programovania a štandardnými prístupmi, ktoré ju riešia. Táto oblasť sa vyučuje až na magisterskej úrovni.

2. Completeness of assignment requirements **assignment fulfilled**

Všetky body zadania boli splnené. Študent sa zoznámil s relevantnými štandardmi a existujúcimi pokynmi pre bezpečné programovanie v jazyku Python. Na základe experimentácie s vybranými zraniteľnosťami spísal sadu pokynov, ktoré majú zoznámiť programátorov s danou problematikou. Vytvoril webovú aplikáciu, ktorá dokáže evaluovať znalosti z rôznych oblastí bezpečného programovania. Efektivita spísaných pokynov bola overená užívateľským testovaním so stručným rozborom výsledkov.

3. Length of technical report **in usual extent**

Rozsah technickej správy zodpovedá požiadavkom na bakalársku prácu.

4. Presentation level of technical report **80 p. (B)**

Práca dosahuje dostatočnú prezentačnú úroveň, jednotlivé kapitoly a sekcie na seba logicky naväzujú. Štruktúra práce je vhodne zvolená a rieši relevantnú problematiku. Úvod práce uvádza riešený problém a motiváciu za jeho riešením, popisuje i štruktúru technickej správy. Druhá kapitola vysvetľuje princípy bezpečného programovania. Výhradu mám k sekcii 2.3 (Goal of this thesis), ktorá je z pohľadu prezentovaného textu zbytočná a väčší priestor mal byť venovaný dopadom nesprávneho prístupu k bezpečnému programovaniu. Tretia kapitola vhodne sumarizuje existujúce štandardy. Štvrtá kapitola popisuje existujúce nástroje pre bezpečné programovanie v jazyku Python. Pri sekcii 4.1 (Existing tools) chýba doplňujúci úvodný text sekcie. Prezentované nástroje boli vhodne zvolené. Kapitola 5 sa zaoberá všeobecnými oblasťami výskytu zraniteľností v zdrojovom kóde. Zvolené oblasti sú dostatočne rôznorodé a pokrývajú podstatné problémy. Šiesta kapitola by podľa jej názvu mala pokrývať porovnanie so známymi zraniteľnosťami v iných jazykoch. Zaoberá sa všeobecnými zraniteľnosťami s príkladmi v jazyku C. V kapitole chýba popis zraniteľností, ktoré sú typické aj pre iné programovacie jazyky, napr. PHP. Kapitola 7 pojednáva o dizajne a implementácii aplikácie, ktorá umožní výuku a testovanie v oblasti bezpečného programovania. Tieto dve oblasti (návrh a vývoj s následným testovaním) bolo vhodné rozdeliť na samostatné kapitoly. V diagrame prípadov užitia (7.1) je nesprávny vzťah zobecnenia účastníka. Obrázok 7.3 so štruktúrou projektu nepovažujem v práci za prínosný. Kapitola 8 podrobnejšie analyzuje vybrané zraniteľnosti. Záver vhodným spôsobom sumarizuje obsah práce.

5. Formal aspects of technical report **65 p. (D)**

Práca je písaná v anglickom jazyku. V práci sa opakovane nachádzajú jazykové a typografické chyby, napr. nekonzistentnosť odkazov na citácie, rôzne typy úvodzoviek, nejednotná kapitalizácia písmen v názvoch kapitol a sekcií. Práca taktiež obsahuje nekonzistentné zvýrazňovanie ukážok zdrojového kódu, názvu modulov, odkazov na obrázky a tabuľky. Neformálne vyjadrovanie autora a nesprávne použitie výrazov v niektorých kapitolách uberá z dojmu formálnej technickej práce.

6. Literature usage **75 p. (C)**

Práca obsahuje 73 odkazovaných zdrojov. Niektoré zdroje bolo možné spojiť do jednej dokumentácie, na ktorú sa autor odkazuje. Viaceré zdroje, ktoré uvádzajú ako autorov názvy inštitúcií a webových stránok, nie sú správne formátované. V prípade niektorých definícií autor využil online blogy. V určitých prípadoch je možné proti ich správnosti argumentovať a bolo vhodné využiť odbornú literatúru. V práci sa taktiež vyskytujú tvrdenia obsahujúce superlatíva (napr. the worst vulnerabilities) bez potrebného zdroja.

7. Implementation results **90 p. (A)**

Realizačným výstupom práce sú pokyny k bezpečnému programovaniu v jazyku Python a webová aplikácia, ktorá umožňuje ich výuku a testovanie znalostí z danej problematiky. Aplikácia je v dobe písania tohto posudku verejne dostupná na webe. Spísané pokyny pôsobia prehľadne, sú jednoducho pochopiteľné a obsahujú praktické ukážky. Drobnú výhradu mám k faktu, že pokiaľ si užívateľ zvolí konkrétnu oblasť, z ktorej chce byť testovaný (napr. webové programovanie), pri vyhodnotení testu sa zohľadnia všetky otázky i z iných oblastí a tak dosiahne nízke hodnotenie. Aplikácia pôsobí jednoducho a neumožňuje zložitejšie operácie. Zdrojový kód je vhodne komentovaný.

8. Utilizability of results

Vytvorenú sadu pokynov a webovú aplikáciu považujem za vhodne využiteľnú nielen pri výuke programovania v jazyku Python, ale i vo firemnom prostredí a školení zamestnancov.

9. Questions for defence

1. Uvažovali Ste, že by sa jednotlivým otázkam v teste priradila rôzna váha pri jeho vyhodnotení, podľa ich závažnosti?
2. V práci uvádzate, že po naštudovaní pokynov bezpečného programovania došlo k zlepšeniu výsledkov, ktoré užívatelia dosiahli v teste. Uvažovali Ste pri vyhodnotení testovania rôzne znalosti respondentov v oblasti všeobecného programovania / znalostí jazyka Python / bezpečnosti?
3. Aplikácia umožňuje registráciu užívateľa. Aké výhody ponúka registrácia v porovnaní s anonymným užívateľom?

10. Total assessment

80 p. very good (B)

Študent si naštudoval problematiku bezpečného programovania a navrhol sadu pokynov, ktoré riešia závažné oblasti danej problematiky. Vytvoril aplikáciu, ktorá dané pokyny prezentuje a vyhodnocuje znalosti užívateľov v danej oblasti. Text práce trpí menej kvalitnou formálnou úpravou a jazykovou stránkou.

Navrhujem uznať prácu ako bakalársku a hodnotiť ju stupňom "B".

In Brno 1 June 2022

Holop Patrik, Ing.
reviewer