Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Posudek oponenta diplomové práce

Jméno studenta: Bc. Petr Váňa

Téma práce: Systém pro automatickou kontrolu odevzdaných zdrojových kódů

Téma a cíle diplomové práce
Cílem práce je návrh a vytvoření webové aplikace, která umožní automatizované odevzdávání a kontrolu zdrojových kódů v jazyce Java. Aplikace by měla být prakticky nasazena v rámci vyučovaných programovacích předmětů na FEI.

Použité metody v diplomové práci
Diplomant ve své práci využil zejména znalosti z oblasti programování, návrhu softwarových systémů a pokročilých databázových systémů.

Co diplomant při vypracování diplomové práce vytvořil
V teoretické části se diplomant věnuje teorii testování aplikací a následně rešerši existujících webových aplikací, které realizují obdobnou funkcionalitu jako je cíl práce. V praktické části je navržena a implementována webová aplikace pro automatizované testování zdrojových kódů.

Prokázání správnosti navrženého řešení
Výslednou aplikaci je možné spustit a prakticky otestovat. Nasazení na server Tomcat, popisované v textu práce, není korektní, ale výslednou aplikaci lze spustit alternativním způsobem.

Při testování aplikace bylo identifikováno několik základních nedostatků a bezpečnostních problémů, které by znemožňovaly praktické nasazení aplikace. Diplomant promptně reagoval na tyto připomínky a aplikaci upravil. Nedostatky byly částečně opraveny. Detailní popis připomínek je uveden níže.

Splnění zadaných cílů diplomové práce
Aplikace splňuje minimální požadavky stanovené v zásadách vypracování práce. Textová část práce se věnuje problematice v dostatečném rozsahu.

Hodnocení textu diplomové práce z hlediska jeho kvality, struktury, srozumitelnosti, jazykové a typografické úrovně
Práce má poměrně dobré logické uspořádání, kvalita textu je na dobré úrovni. V práci je používáno nepříliš vhodné odkazování na zdroje z literatury.

Jak byla vyhodnocena kontrola textu DP (případně zdrojových kódů softwaru) pomocí systému pro odhalování plagiátů mezi závěrečnými pracemi?
Samotný text práce byl vyhodnocen se shodou méně než 5 %. V ostatních souborech (soubor s licencí, deskriptor projektu, …) bylo identifikováno několik shod (až 100 %), nicméně se jedná o soubory, jejichž základem jsou typické jednotné šablony nebo generovaný kód a nepovažuji tuto shodu za výjimečnou. Práce není plagiátem.

Další nejasnosti a otázky:

Připomínky k textové části práce:

- Tabulka 1 a následný textový popis obsahuje necitované a potenciálně zavádějící informace. Rovněž jsou zde přítomny zjevné chyby, v tabulce je uvedeno, že REST podporuje WS-Security, v textovém popisu je tato technologie uvedena u protokolu SOAP.
- V rešerši obdobných služeb a příslušné tabulce 2 zcela absentují informace o podporovaném API, které lze testovat. Například jestli je možné testovat práci se soubory, počítačovou sítí, práci s vlákny, aj.

Připomínky k praktické části práce:

V odevzdané práci bylo nalezeno několik fatálních chyb, které by znemožnily bezpečné použití aplikace. Zpracování API v backendu postrádalo správné ošetření autorizace operací a libovolný student tak mohl vykonávat operace za jiné studenty. Kompilace a spouštění kódu bylo extrémně nezabezpečené a umožňovalo provést libovolný útok na aplikaci a operační systém. Kompilace a spouštění kódu dále obsahovaly race condition při spuštění více testů v jednom okamžiku, aplikace pak neposkytovala korektní výsledky.

Vzhledem k závažnosti uvedených nedostatků jsem kontaktoval diplomanta a vyzval jej k vyjádření k uvedeným problémům. Diplomant reagoval aktualizací aplikace a snahou o odstranění nedostatků. Specificky pak:

- Autorizace v API byla doplněna a je korektní.
- Ochrana před škodlivým kódem byla upravena a je schopna zachytit většinu pokusů o útok na aplikaci či operační systém. V kódu ale nadále zůstaly zranitelnosti zahrnující neošetřený kód na vstupu a neopravitelnou zranitelnost, kdy kód může alokovat veškerou dostupnou operační paměť.
- Race condition byla téměř kompletně ošetřena a je nyní velmi nepravděpodobné, že k této situaci dojde.

V práci se vyskytují i další nekritické problémy:

- Strohé a nepříliš povedené UI. Navigace na jednotlivých stránkách je zmatečná a nepřehledná.
- Chyby a varování jsou v UI prezentovány zcela mimo pracovní oblast a bez vhodného formátování.
- Načítání dat na pozadí bez zobrazení vhodného indikátoru činnosti či placeholderu.
- Zabezpečení CORS není správně aplikováno.
- V textu práce ani nikde jinde není zmíněn fakt, že je třeba vygenerovat bezpečný klíč pro podepisování JWT a nastavit jej ve zdrojovém kódu.
- Nasazení frontendu je v práci realizováno na Apache HTTP server a je vyžadován soubor .htaccess pro správnou funkcionalitu, soubor ale není k práci přiložen.
- Konfigurace aplikace se nachází na několika různých místech, část v příslušném konfiguračním souboru, část je nutno upravovat ve zdrojových kódech aplikace.

Celkově práce prakticky splňuje zadání a požadavky, ačkoliv její vizuální a funkční stránka je nízké až průměrné kvality. Vzhledem ke zvolenému způsobu realizace aplikace (a absenci rešerše možných alternativ realizace) práce obsahuje neodstranitelné bezpečnostní riziko, které může a nemusí způsobit problémy. Její praktická funkce je rovněž omezena kvůli striktním ochranám na vstupní kód a zvolený způsob realizace.

Otázky k obhajobě:

1. Jaké alternativní způsob kompilace a spouštění kódu lze zrealizovat, tak aby byly výše uvedené nedostatky odstraněny?

Doporučení práce k obhajobě: ano

Navržený klasifikační stupeň: E (dobře)

V Pardubicích dne 3. 6. 2021 Ing. Roman Diviš, Ph.D.