Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Posudek vedoucího diplomové práce

Jméno studenta: Bc. Martin Volenec

Téma práce: Bezpečnost webových aplikací

Téma a cíle diplomové práce
Cílem diplomové práce je popis aktuálních témat souvisejících s webovou bezpečností a vytvoření sady ukázkových příkladů demonstrujících vybrané techniky související s webovou bezpečností.

Použité metody v diplomové práci
Diplomant ve své práci využil zejména znalosti z oblasti programování webových a databázových aplikací a pokročilé znalosti bezpečnosti softwarových systémů.

Co diplomant při vypracování diplomové práce vytvořil
V teoretické části se diplomant věnuje teoretickému úvodu do kryptografie a kryptografických systémů, následně je navázáno problematikou autentizace a autorizace v kontextu webových aplikací. V následující kapitole se popis zaměřuje na vybrané bezpečnostní problémy související s webovými aplikacemi (injection, XSS, CSRF a další) a problematikou bezpečnosti spojednou s protokoly http a https.

V rámci praktické části jsou vybrané problémy demonstrovány v nezabezpečené i zabezpečené variantě. Dále byly vytvořeny dva komplexnější příklady na realizaci autentizace s využitím lokální databáze a funkcionalitou ztráty a obnovy hesla a příklad demonstrující nasazení standardu security.txt, tyto příklady využívají php framework Nette. Veškeré příklady jsou připraveny pro spouštění s využitím kontejnerové technologie docker (resp. docker-compose).

Prokázání správnosti navrženého řešení
Vytvořené příklady je možné spustit a otestovat, v popisu jednotlivých příkladů jsou uvedeny nebezpečné vstupy, které je možné otestovat a ověřit jejich správné ošetření.

Splnění zadaných cílů diplomové práce
Teoretický popis bezpečnosti webových aplikací a sada realizovaných praktických příkladů plně splňují požadavky kladené v zadání diplomové práce.

Hodnocení textu diplomové práce z hlediska jeho kvality, struktury, srozumitelnosti, jazykové a typografické úrovně
Práce je po formální stránce poměrně dobře strukturována. V práci se na několik místech vyskytují drobné chyby.

Jak byla vyhodnocena kontrola textu DP (případně zdrojových kódů softwaru) pomocí systému pro odhalování plagiátů mezi závěrečnými pracemi?
Samotný text práce vykazuje shodu menší než 5 %. V souboru popisujícím databázovou strukturu jedné z ukázkových aplikací byla nalezena shoda 32 %, ale zde se jedná o náhodnou podobnost struktury tabulky. Práce není plagiátem.

Další nejasnosti a otázky:

- V textu práce chybí základní představení praktických příkladů a jejich použití.

Otázky k obhajobě:

1. S ohledem na psaní bezpečné webové aplikace, lze doporučit konkrétní framework (v php nebo i v jiném jazyce), který by specificky napomáhal psaní bezpečné aplikace?

Doporučení práce k obhajobě: ano

Navržený klasifikační stupeň: A (výborně)

V Pardubicích dne 27. 5. 2020 Ing. Roman Diviš