

Posudek práce

předložené na Přírodovědecké fakultě JU

☐ posudek vedoucího

☒ posudek oponenta

☒ bakalářské práce

☐ diplomové práce

Autor/ka: Patrik Marýška

Název práce: Zabezpečená webová aplikace

Studijní program a obor: Aplikovaná informatika

Rok odevzdání: 2019

Jméno a tituly oponenta: ing. Petr Břehovský

Pracoviště: ÚAI PŘF Jihočeská univerzita, České Budějovice

Kontaktní e-mail: pbrehovsky@prf.jcu.cz

Odborná úroveň práce:

☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Věcné chyby:

☒ téměř žádné ☐ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

Výsledky:

☒ originální ☐ původní i převzaté ☐ netriviální kompilace ☐ citované z literatury ☐ opsané

Rozsah práce:

☐ veliký ☒ standardní ☐ dostatečný ☐ nedostatečný

Grafická, jazyková a formální úroveň:

☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Tiskové chyby:

☒ téměř žádné ☐ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

Celková úroveň práce:

☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Slovní vyjádření, komentáře a připomínky oponenta:

Práce poměrně podrobně krok za krokem popisuje jaká bezpečnostní opatření byla použita při tvorbě aplikace a při konfiguraci WEB serveru. Následně byl systém otestován dle metodologie OWASP (Testing Guide v4) a bylo tak prokázáno, že byla uvedená bezpečnostní opatření implementována správně a že je aplikace bezpečná. Některé nedostatky způsobené pravděpodobně použitými knihovnami (validace PDF souboru) a vedoucí k útokům typu nechráněný upload souboru, se díky jiným bezpečnostním mechanismům (šifrování souborů na disku) neprojeví. Práce by se dokonce dala považovat za bezpečnostní specifikaci produktu, ale aby tomu tak opravdu bylo, musela by být doplněna o podrobnější analýzu hrozeb a relevantních rizik.

Případné otázky při obhajobě a náměty do diskuze:

Jak jsou nastavena přístupová práva operačního systému k šifrovaným dokumentům na disku a jak je chráněn tajný klíč, kterým se dokumenty na disku šifrují?

Proč je na WEB serveru povolen port 80?

Jak by se dala implementovat funkcionality logování neúspěšných validací přístupového tokenu?

Práci

☒ doporučuji

☐ nedoporučuji

uznat jako bakalářskou.

Navrhuji hodnocení stupněm:

☒ výborně ☐ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/opponenta:

V Českých Budějovicích 8.1.2020

