FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jan Bělohoubek, Ph.D.
Student:	Jakub Sulovský
Název práce:	Bezpečnostní analýza carsharingového systému
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	22. února 2024

Hodnotící kritéria

1. Splnění zadání

[1] zadání splněno
▸ **[2] zadání splněno s menšími výhradami**
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Zadání obsahuje terminologickou nejasnost (riziko vs. zranitelnost vs. hrozba), což není zřejmě chybou studenta, ale z kontextu je jasné, co má student provést. V textu práce jsou již termíny užity správně.

2. Písemná část práce 75 / 100 (C)

Celkově text práce hodnotím jako kvalitní. Práce se poměrně dobře čte, je prosta velkých faktických, gramatických nebo stylistických problémů a obsahuje minimum překlepů.
Zaujala mě studentova obliba výrazu "spousta" ve všech možných podobách. Ze stylistického hlediska by neškodilo občas zvolit synonymum, na některých místech také upravit skloňování.
Zejména však by v textu BP bylo vhodnější vyhnout se častým vágním obratům jako "spousta aplikací" a pokusit se seriózně a přesně kvantifikovat, např. "dle [XY] 80% webových aplikací", apod.

Obecně práce poněkud trpí vágními obraty. Vhodné by také bylo podrobit zdroje (zejména marketingového charakteru) kritickému zhodnocení, např. převzaté prohlášení "Uniqway je zároveň první projekt v České republice, vzniklý na akademické půdě, který byl následně překlopen do reálně fungující služby" je zjevně zavádějící - na akademické půdě vzniká "spousta" startup projektů (ano, nikoli carsharingových), navíc služba Uniqway byla ukončena pro nerentabilitu.

Práce se zdroji je formálně v pořádku. V práci jsou však použity téměř výhradně online zdroje, byť kredibilní, doplněné o zákon o kybernetické bezpečnosti. To je vzhledem k charakteru práce pochopitelné, ale chybí v nich syntéza a potřebný nadhled, což se následně promítá i do textu BP.

Teoretická část práce je dobře členěná a vysvětluje všechny důležité pojmy. Z hlediska členění práce nemám významných námitek, snad jen hodnocení uživatelských rolí mohlo být provedeno podrobněji a odděleno od popisu architektury, jež je prerekvizitou pro více částí práce (black-box testování).

Popis zranitelností, jejich hodnocení a popis dalších souvislostí se drží pouze kategorií z OWASP TOP 10, což je poměrně omezující, ale pro bakalářskou práci přijatelné zjednodušení.
V některých případech by bylo vhodné lépe oddělit popis zranitelnosti, a návrh opatření (např. v 5.2.4 dokonce black-box přístup přechází na gray-box).

Za poměrně závažný nedostatek považuji absenci ohodnocení jednotlivých základních metrik - pro každou zjištěnou zranitelnost je uvedeno pouze sumární CVSS skóre.

Zkratky by měly být při prvním výskytu rozepsány (nikoli pouze v rejstříku) - v některých případech to tak není.
Většina obrázků v práci není explicitně referencována v textu.
Výraz metodologie je na několika místech použit nesprávně ve významu "metodika", jinde je správně použit výraz "metodika".

3. Nepísemná část, přílohy 100 /100 (A)

Byly použity standardní nástroje.

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Výsledky je možné využít ke zvýšení bezpečnosti systému Uniqway v případě jeho opětovného spuštění (projekt byl ukončen v průběhu řešení práce studentem).

Celkové hodnocení 75 /100 (C)

Obtížnost zadání práce hodnotím jako přiměřené pro BP.
Práce je zpracována poměrně dobře, zadání je splněno a text neobsahuje závažné nedostatky.
Některé části práce jsou však příliš vágní a/nebo zbytečně zkratkovité.

Otázky k obhajobě

Prosím, ukažte ohodnocení základních metrik CVSS skóre pro alespoň dvě zjištěné zranitelnosti a jednotlivá hodnocení stručně zdůvodněte.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.