Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: **Bucsa Serghei** **Oponent:** **Ing. Petr Žáček, Ph.D.**

Studijní program: **Softwarové inženýrství**
Studijní obor / specializace: **Softwarové inženýrství**
Akademický rok: **2023/2024**

Téma bakalářské práce: **Metodiky testování a zabezpečení webových aplikací**

Hodnocení práce:		**A**	**B**	**C**	**D**	**E**	**F**
		Hodnocení: A – nejlepší; F - nevyhovující					
1.	Aktuálnost řešeného tématu	☒	☐	☐	☐	☐	☐
2.	Obtížnost zadaného úkolu	☒	☐	☐	☐	☐	☐
3.	Splnění všech bodů zadání	☐	☐	☐	☐	☐	☒
4.	Vhodnost zvolené metody řešení	☐	☐	☐	☐	☒	☐
5.	Logické členění práce	☐	☐	☐	☒	☐	☐
6.	Úroveň jazykového zpracování	☐	☐	☒	☐	☐	☐
7.	Formální úroveň práce	☐	☐	☐	☒	☐	☐
8.	Práce s literaturou a její citace	☐	☐	☐	☐	☒	☐
9.	Úroveň zpracování teoretické části	☐	☐	☐	☐	☒	☐
10.	Kvalita zpracování praktické části	☐	☐	☐	☒	☐	☐
11.	Dosažené výsledky práce	☐	☐	☐	☐	☒	☐
12.	Přínos práce a její využití	☐	☐	☐	☒	☐	☐

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou bakalářskou práci doporučuji k obhajobě a navrhuji hodnocení

F - nedostatečně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Otázky k obhajobě:
1. Jaký je rozdíl mezi etickým hackerem a penetračním testerem ?
2. Na co byl v práci využitý nástroj Burp Suite (když pomineme překlep "Burb Suite") ? Nepodařilo se mi najít jeho praktické využití, i když student uvádí, že "byly prozkoumány".
3. Kolik je vaše práce a kolik je převzato / parafrázováno ?
4. Jakou vazbu v kontextu práce měly výkonnostní / zátěžové testy (tedy nefunkcionální testování) ? Já zde nevidím jejich využití či ověření / otestování. Splňuje práce tedy tyto požadavky a jak jste testoval nefunkcionální požadavky ?
4a. Jak spolu souvisí výkonnost / účinnost a bezpečnost ? Uvádíte, že by to mohlo přispět k zabezpečení.

5. Testuje nástroj Burp Suite staticky či dynamicky ?
6. Jaký je rozdíl mezi hrozbou a rizikem ? student jednou mluví o rizicích a jednou o hrozbách.

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):
Na úvod musím konstatovat, že jsem docela zklamán z terminologie v oblasti testování SW, kterou by měl mít student po absolvování mnou garantovaným předmětem zvládlou - funkční vs nefunkční požadavky, nekorektní rozdělení druhů testování a nebo uvedení pojmu "testovací scénář" a další …

Student jinak celkově vypracoval aktuální téma, které si kladlo za cíl odstranit základní problémy zabezpečení webových aplikací. Je škoda, že například OWASP Top 10 zde není zmíněn přímo, ale pouze v kontextu vybraných 5 z nich. V teoretické části a volbě metodiky by bylo celkový kontext vhodné uvést. V tomto kontextu si nejsem jistý, jak zapadá riziko "Brute-force attack". Nicméně další pojmy, které by stály za zmíňku a využití v práci by mohly být OSSTMM nebo CVSS. Obzvlášť v kontextu volby frameworku, kdy jejich zranitelnosti verze hrají naprosto zásadní roli! Student uvádí, že penetrační testy často testují staticky - zde opět nařážím na nepochopení problematiky testování SW. Navíc i zdroj, který student uvádí, toto explicitně nezmiňuje.

Bohužel i po formální stránce práce vykazuje nedostatky - chyba v odkazech v textu, mírně zmatené citování či v neposlední řadě neseřazení seznamu zkratek.

Po praktické stránce bohužel musím konstatovat, že student sice provedl preventivní opatření pro základním hrozbám (to jsou plusové body), ale celkové ověření a otestování bylo spíše slabší. SQL Injection - jeden test namísto využití právě nástroju Burp Suite ši sqlmap. Obdobně u XSS. Práce se mi jeví v tomto ohledu, že to sice student v plánu měl, ale nestihl to. I přes pouze vzorovou aplikace mohly být jednotlivé nadpisy elementů lépe popsané (jednou je použitá angličtina, jednou čeština), než-li jak uvádí student. Lze pouze poznamenat, že naštěstí UI/UX a použitelnost nebyly součástí návrhu. Nicméně, pokud bychom brali v potaz bezpečnost, tak by systém při ověřování uživatele nikdy neměl zmínit, zda-li "uživatel existuje nebo ne"

Ale naprosto nejzásadnější mě vede k hlavní otázce -> kolik práce je studentovým dílem, jelikož je většina citována. Viz otázka k obhajobě číslo 3. Dále jaké frameworky zvolil a hlavně proč? A jak student provedl analýzu bezpečnostních a testovacích mechanismů ? Student uvádí Laravel, Django a Ruby-on-rails a následně v praktické využívá Bootstrap, Django, Python, HTML, CSS a SQLite, narážím zejména na bod zadání číslo 2 - "Vykonejte analýzu bezpečnostních a testovacích mechanismů u vybraných vývojových frameworků a technologií". Dle mého je bohužel tento bod zadání spíše nesplněn než splněn. Student sice vybrané frameworky popisuje i ve správném kontextu, ale chybí zde jejich vzájemné srovnání -> celkově formálnější analýza.

Celkově bohužel musím konstatovat, že daná práce se jeví spíše "nedomrlým" dojmem a k přihlédnutí bodu zadání číslo 2 leč práci doporučuji k obhajobě, ale doporučuji klasifikaci stupněm F - nedostatečně a práci dopracovat. Po zapracování a opravě by to mohlo být hezké D.

Datum 24.5.2024 Podpis oponenta bakalářské práce