FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Jiří Šmolík
Student:	Bc. Michal Kovačič
Název práce:	Zranitelnosti komunikačních Web API protokolů
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	5. června 2023

Hodnotící kritéria

1. Splnění zadání

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

Přiložená práce dostatečně a v souladu se zadáním vymezuje cíle a v dostatečné kvalitě je naplňuje. Drobnou výjimkou je 3. bod zadání "Implementujte knihovnu pro zmíněné API technologie ve vybraném jazyce, které pomůže vývojářům snížit rizika diskutovaných útoků.", kde implementace není ve formě, kterou by bylo možné nainstalovat a pro použití je tak nutné dané části vykopírovat. Příčinou může být i těžší nalezení průniku programovacích jazyků jednotlivých technologií (GraphQL převážně JavaScript, gRPC převážně C++).

2. Písemná část práce 80 / 100 (B)

Rozsah práce splňuje požadavky a všechny části zde mají své místo. Logická struktura práce je stavěna srozumitelně. Práce správně pracuje s bibliografickými citacemi. Výhrady míří k nedodělkům ve formě TODO (str. 8), neplatným referencím ?? (str. 29, 48) či lidovým formulacím "kanón na vrabce" (str. 47), "kombinace hodí správný výsledek" (str. 58) a několika překlepům.

3. Nepísemná část, přílohy 75 / 100 (C)

Student vhodně zvolil nástroje a programovací jazyky pro bezpečnostní experimenty a demonstraci a oprav zranitelností (C++ pro gRPC, Node.js a Apollo, graphql-sheild pro GraphQL). Vytvořené kusy software jsou svým rozsahem (22 souborů, 911 řádků) a použitelností nejslabší částí práce - implementace není připravena na to být použita jako knihovna a opravy zranitelností jsou úzce spjaty s ukázkovou aplikací. Výstup obsahuje i

vlastní implementaci Query Builderu pro prevenci SQL injection, kterou pokládám za značně omezující, i vzhledem k hotovým alternativám (např. QSqlQuery)

4. Hodnocení výsledků, jejich využitelnost 85 /100 (B)

Cílem práce byla analýza známých zranitelnosti a vytvoření knihovny pro snížení bezpečnostních dopadů. Teoretická část práce a experimenty jsou dobrým podkladem pro zjištění příčin a důsledků bezpečnostních chyb testovaných protokolů s podrobným návodem na využití chyby a následné opravy. Zmíněná absence knihovny ale limituje využitelnost této části v praxi.

5. Aktivita studenta

[1] výborná aktivita
▸ **[2] velmi dobrá aktivita**
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Velmi dobrá aktivita studenta, která se od výborné liší pouze v dodržování smluvených termínů při blížícím se termínu odevzdání práce.

6. Samostatnost studenta

▸ **[1] výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Celkové hodnocení 80 /100 (B)

Analytická část práce přehledně shrnuje zásadní zranitelnosti testovaných API protokolů, poukazuje na jejich dopady a zmiňuje návrhy na opravy. Za slabší část práce považuji implementaci, která působí nedotaženě a komplikuje to tak její použití. Některých zranitelností se implementace dotýká jen okrajově (např. složitost GraphQL dotazu), některá byla triviálně vyřešena správným nastavením serveru daného protokolu, to vnímám jako důsledek komplexnosti a rozdílnosti testovaných technologií, ne vždy tak bylo možné vyřešit vše elegantním způsobem, proto to zohledňuji i v hodnocení této části.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.