FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Filip Kodýtek, Ph.D.
Student:	Bc. Vojtěch David
Název práce:	Bezpečnostní audit Ethereum projektu
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	1. června 2022

Hodnotící kritéria

1. Splnění zadání

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

Student splnil zadání, vzhledem k vybrané testované aplikaci však zadání působí jednoduše.

2. Písemná část práce 70 / 100 (C)

Práce obsahuje velké množství překlepů a různých jazykových chyb a působí tak, že byla napsána ve spěchu a autor si ji po sobě nepřečetl. Nemusel zde být tak dlouhý úvod do problematiky Bitcoinu/Etherea, kapitola o eliptických křivkách je zde v podstatě naprosto zbytečná, jelikož přímo s prací a zadáním studenta nijak nesouvisí. Vzhledem k tématu práce by bylo vhodnější věnovat prostor popisu technik a metodik pro bezpečnostní audity smart kontraktů. Práce je přesto až na řadu rušivých chyb čtivá.

3. Nepísemná část, přílohy 90 / 100 (A)

Student využil vhodné existující nástroje pro testování. Studentem navržené testy mohly být lépe popsány (souhrn testovaných případů).

4. Hodnocení výsledků, jejich využitelnost 90 / 100 (A)

Výstupem práce je bezpečnostní audit aplikace PWN, který může autorům aplikace posloužit pro její možné úpravy, nebyly však nalezeny žádné zásadní bezpečnostně relevantní nedostatky (což ovšem nemusí být chybou auditu).

Celkové hodnocení

80 /100 (B)

Vzhledem k značným nedostatkům písemné části práce navrhuji známku B. K hodnocení také příliš nepřispívá, že zadání práce (vzhledem k volbě auditované aplikace) působí poměrně jednoduše na diplomovou práci.

Otázky k obhajobě

1) V práci navrhujete jako řešení problému vysokých poplatků u využití PWN pro půjčky centralizovaný model s využitím webového serveru. Jaké se tím otevírají jiné potenciální hrozby? Jaký je váš odhad, že se ušetří na poplatcích?
2) Napadá vás jiný způsob řešení výše uvedeného problému tak, aby nedošlo k centralizaci?

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.