FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Gattermayer, 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

Zadání splněno kromě bodu "Napište fuzzy testy pro parametry funkcí i pořadí volání funkcí (např. pomocí nástroje Echidna)."
Poskytnuté vysvětlení, že v tomto případě fuzz testy postrádají smysl a jsou nahrazeny unit testy považuji za dostatečné.

2. Písemná část práce 50 / 100 (E)

Práce cituje množství relevantních zdrojů, rozsahem o obsahem splňuje požadavky.
Za problém považuji nevhodný vypravěčský styl, který se nehodí pro technický text.

Stylistické chyby:
- Nekonzistentní interpunkce odrážek (strana 3).
- Dopředné reference (strana 13, 69).
- Smíšená CZ/EN terminologie, např. "odlehčený node" (strana 15).
- Interpunkce popisu obrázku (strana 33).
- Výpravný literární druh místo čistě technického popisu, formulace typu "Nyní je čas přistoupit k manuální analýze kódu" do DP nepatří (např. strana 66, 69, 72).

Věcné chyby:
- Floating Pragma anti-pattern v ukázkovém Solidity kódu (strana 33, 60)

3. Nepísemná část, přílohy 70 / 100 (C)

Podařilo se implementovat unit testy s coverage 100%.

S výtkou k architektuře projektu PWN úplně nesouhlasím. Jedná se o decentralizovanou finanční aplikaci, z podstaty zadání tedy není možné přemístit části aplikace na klasický backend. Spíše bych jako řešení viděl současný provoz na více Layer 2 side chainech. Ale je to otázka priorit.

4. Hodnocení výsledků, jejich využitelnost 80 /100 (B)

Při manuální code review se podařilo najít zajímavé zranitelnosti (např. Timestamp v bloku), je škoda, že není nastíněno možné řešení.
Jednotlivé issues by bylo dobré lépe strukturovat, popsat a navrhnout řešení pomocí ukázek kódu.
Ale i v této formě jsou odhalené problémy přínosem.

5. Aktivita studenta

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

6. Samostatnost studenta

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

Celkové hodnocení 60 /100 (D)

Student úspěšně nastudoval technologii Ethereum a programovací jazyk Solidity.

Praktická část práce se věnovala protokolu PWN, který je vhodného rozsahu a má veřejně přístupné zdrojové kódy.

Protokol se studentovi podařilo otestovat na lokálním prostředí, implementovat unit testy a provést manuální code review. Jejím výstupem jsou doporučení a odhalené nesrovnalosti v implementaci oproti white paperu. Fuzz testy se student rozhodl nahradit unit testy, zdůvodnění považuji za dostatečné.

Za nejslabší část práce považuji textovou část, která místy není technický text, ale spíše přepis neformálního rozhovoru.

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.