FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Dostál, Ph.D.
Student:	Eliška Krátká
Název práce:	Bezpečnostní analýza výdejních boxů
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	10. 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

Body 1-3 zadání byly splněny. V bodě č. 4 se uvádí, že se má udělat analýza zdrojových kódů, které jsem nikde neviděl. Nicméně z provedené analýzy vyplývá, že k nim autorka měla přístup. Bod č. 5 je splněn třemi odstavci, ve kterých jsou uvedena pouze obecná doporučení. V zadání je uvedeno, že se má náprava nalezených zranitelností týkat přímo zdrojového kódu. Autorka tak zřejmě nemohla zdrojové kódy zveřejnit ani použít jejich části, což ale není nikde v práci zmíněno.

2. Písemná část práce

60 / 100 (D)

Písemná část práce je hodně nevyvážená. Velmi kladně hodnotím kapitolu, věnující se threat modelingu, která je vypracována velice detailně a metodicky. Co se týče kapitoly věnující se analýze, zde naopak postrádám jakoukoliv metodiku. Předpokládal bych využití nějaké již existující metodologie pro bezpečnostní analýzu případně návrh vlastního postupu, jak analýzu dělat. Co se týče nástrojů, je zde jen tak mimochodem zmíněn Hatch, ale není uvedeno, proč se autorka rozhodla právě pro něj (různých nástrojů je spousta, zde by šla určitě využít např. THC Hydra). De facto zde chybí jedna kapitola, která by se týkala metodologie a požitých nástrojů pro bezpečnostní analýzu. Bezpečností analýza je explicitně zmíněna jak v názvu práce, tak i v zadání a je podle mě hlavním tématem práce - bohužel, v písemné části práce má tato kapitola velice omezený rozsah. V neposlední řadě v práci chybí popis toho, proč se autorka rozhodla pro uvedená konkrétní řešení daného problému.

3. Nepísemná část, přílohy 50 /100 (E)

Nepísemná část práce je tvořena pouze jedním skriptem (Hatch). U tohoto typu závěrečné práce neočekávám velký rozsah nepísemné části, však mohly by zde být např. různé výpisy, výsledky scanů, zachycená komunikace apod. Tento typ informace by určitě ulehčil vývojářům orientaci, co se se systémem dělo a umožnil lépe reprodukovat kroky analýzy. Bohužel, tato data v nepísemné části chybí.

4. Hodnocení výsledků, jejich využitelnost 70 /100 (C)

Threat model je určitě velký přínos a najde využití pro další bezpečnostní analýzu. Bezpečnostní analýza a doporučení jsou ale velmi obecná. Dělá to na mě trochu dojem, že z nějakého důvodu (nejspíše NDA) nemohla autorka zveřejnit detailní část analýzy a doporučení.

Celkové hodnocení 70 /100 (C)

Jako největší nedostatek práce shledávám v tom, že nebyla detailně provedena bezpečnostní analýza, hlavně z hlediska metodologie a doporučených úprav. Dále pak velice povrchně splněné poslední dva body zadání. S přihlédnutím k velmi dobrému threat modelu práci doporučuji k obhajobě a hodnotím stupněm C.

Otázky k obhajobě

Jaká vhodná metodologie by se dala využít pro vlastní bezpečnostní analýzu?
Proč jste konkrétně použila nástroj Hatch?
Byly použity i nějaké další nástroje/techniky, které nejsou explicitně v textu uvedeny?

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.