FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Bc. Jakub Štrom
Název práce:	Windows Sandbox: Analýza a ověření známých zranitelností
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	21. května 2024

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno. Student popsal všechny požadované části a provedl velmi přesvědčivou analýzu oprav známých zranitelností. Našel při tom i zranitelnost dosud neznámou.

2. Písemná část práce 95 / 100 (A)

Textová část práce je velmi dobře napsána. Velmi důkladně popisuje strukturu a zpracování Windowsových kontejnerů i další části potřebné pro porozumění vlastního přínosu studenta. Analýza známých zranitelností a jejich oprav ukazuje, že student tématu výborně porozuměl - dokonce do té míry, že byl schopen nalézt novou dosud neopravenou zranitelnost.

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

Nepísemnou část práce tvoří zejména záznamy zachycující průběh analýzy; po dohodě s vedoucím sem nebyly umístěny přímo soubory z Ghidry, protože zahrnují copyrightovaný kód, ale jsou nahrazeny obrázky relevantních částí. Dále jsou přítomny vlastní kódy studenta, které při analýze používal. To je pro daný typ práce zcela vyhovující.

4. Hodnocení výsledků, jejich využitelnost 95 / 100 (A)

Práce má hned několik přínosů. V první řadě přináší na jednom místě komplexní popis celého prostředí Windows Sandbox včetně všech jeho klíčových komponent a souborů. Dalším přínosem je popis analýzy, který může posloužit jako dobrý výchozí bod pro další

analytiky, kteří by si mohli chtít ověřit opravu i zcela odlišných zranitelností. Že byla analýza smysluplná je vidět z toho, že student v jejím rámci nalezl další, dosud neznámou a neopravenou zranitelnost, kterou nahlásil Microsoftu - tím pádem bude opravena, doufejme že dříve, než na ni přijdou i útočníci.

5. Aktivita studenta

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

Student pracoval spíše individuálně, jen s minimem konzultací.

6. Samostatnost studenta

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

Celkové hodnocení

95 /100 (A)

Celkově práci hodnotím jako velmi zdařilou a kandidáta na navržení na cenu děkana. Nejde o dílo "do šuplíku", ale má několik jasně viditelných přínosů včetně odhalení nové zranitelnosti. I technická stránka textu je velmi dobrá, včetně použití angličtiny, takže výsledků práce mohou využívat lidé po celém světě. Student tak nade vši pochybnost demonstroval svoji schopnost inženýrské práce a já jeho práci s radostí hodnotím známkou A - výborně.

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.