FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Michal Valenta, Ph.D.
Student:	Vojtěch Zabořil
Název práce:	Bezpečnostní analýza aplikace Anketa ČVUT
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	9. června 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 považuji za splněné ve všech dílíčích bodech.

2. Písemná část práce 85 /100 (B)

Text se dobře čte, jednotlivé kapitoly na sebe dobře navazují a čtenář, ikdyž není odborníkem na bezpečnost (což je můj případ), se v textu příliš neztrácí.
Po formální stránce je text práce zcela v pořádku. Autor korektně cituje téměř 40 relevantních zdrojů. Vesměs se jedná o webové zdroje, což je ale vzhledem k zadání práce zcela pochopitelné.

Kritčtější připomínky k textu mám pouze dvě:

1. Zdůvodnění, proč byl vypbrán právě framework OWASP se jeví spíše jako subjektivní, rozhodně relativně málo zdůvodněné.

2. Není zřejmé, zda pro analýzu byl použit nějaké konkrétní nástroj či sada nástrojů a jak byly zvoleny.

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

Původním netextovým výstupem práce jsou reporty z použitých nástrojů pro bezpečnostní analýzu a také jeden exploit soubor, ze kterého jsem, příznávám, poněkud zmatený. V textu práce je zřejmě vysvětlen, ale předpokládal bych nějaký krátký popis i zde.

4. Hodnocení výsledků, jejich využitelnost 92 /100 (A)

Za nejhodnotnější výsledek práce považuji kapitolu 4 předloženého textu. Ta přehledně shrnuje jednotlivé bezpečnostní nálezy a také částečně dává návod k tomu jak se s nimi vypořádat. Z těchto výsledků budeme dále čerpat s týmem studentů, kteří v rámci předmětu BI-SP2 pracují na dalším rozvoji aplikace Anketa ČVUT.

Celkové hodnocení 88 /100 (B)

Práce splnila očekávání. Pokytuje podrobnou bezpečnostní analýzu aplikace Anketa ČVUT podle frameworku OWASP, nálezy přehledně shnruje a nabízí návod na lepší zabezpečení aplikace. Na výsledcích může stavět tým vývojářů a zároveň je tato práce solidním dokumentem, který si mohou prostudovat studenti a vyučující, když mají pochybnosti o bezpečnosti systému a spolehlivosti dat.

Otázky k obhajobě

1 Můžete krátce shrnout jaké konkrétní nástroje jste pro analýzu použil.

2. Můžete stručně vysvětlit princip ukázkového kompromitačního kódu v adresáři exploit v přílohách práce?

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.