FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Kokeš
Student:	Bc. Jaroslav Kříž
Název práce:	Analýza bezpečnosti webové aplikace Seznamovák
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	14. května 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 bylo z mého pohledu splněno. Nevšiml jsem si řešení pro požadavek "Zahrňte již známé problémy celé aplikace", v kontextu zbytku práce mi ale připadá nepodstatný a možná takové problémy ani neexistují.

2. Písemná část práce 95 / 100 (A)

Písemná část je velice pěkně napsaná. Je detailní, ale přitom ne zahlcující, a přehledně a systematicky provádí uživatele celým procesem analýzy aplikace Seznamovák. Určité pochybnosti mám u zahrnutí konkrétních oprav přímo do kapitoly 3, spíš bych je očekával v samostatné kapitole, jde ale také o legitimní přístup. Určitě bych ale doporučoval do hodnocení přidat i další aspekty než jen čistě kvantitativní, například u hodnocení vlivu znakové sady na entropii jistě stojí za úvahu i to, jaké náklady by to neslo (např. složitější zadávání hesla na mobilním telefonu) a jestli by přínosy byly nebo nebyly větší než tyto náklady. Ve výpisu kódu 4 bych se v rámci časových útoků asi spíše zaměřoval na odlišení jednotlivých typů selhání než na rozdíl, na kolikátém znaku hashe došlo k neshodě. Zmínku by si také zasloužilo rozdělení rolí, je otázka, do jaké míry je rozumné, aby vývojář měl plný přístup k datům aplikace.

Pochválit musím také jazykovou stránku práce, výskyt chyb je naprosto minimální (jednotky případů, navíc nepříliš závažných).

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

Nepísemnou částí práce jsou pouze reporty vygenerované použitými nástroji. S ohledem na charakter práce to pokládám za přiměřené, zároveň ale není, co hodnotit.

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

Práce nepochybně plní cíl, který na ni byl kladen - provést bezpečnostní analýzu aplikace Seznamovák a tuto analýzu následně předat vývojářům k opravě chyb. Tím bude budoucím účastníkům akce zajištěna větší bezpečnost.

Celkové hodnocení 95 /100 (A)

Předložená práce představuje kvalitní bezpečnostní analýzu aplikace Seznamovák. Student aplikaci podrobil manuálnímu studiu částí zdrojových kódů a také automatizovanému penetračnímu testování a odhalil některé nedostatky, které následně nahlásil autorům k opravě. V první řadě tak zlepšil bezpečnost aplikace pro její uživatele, v druhé dokázal, že si osvojil potřebné znalosti a schopnosti pro to, aby mohl takovou činnost vykonávat i v praxi. Práci doporučuji k obhajobě a hodnotím známkou A=výborně.

Otázky k obhajobě

V hodnocení bezpečnosti API se pozastavujete nad heslem k API natvrdo zabudovaným do programu (sekce 3.5) a hodnotíte to jako vysoce závažnou zranitelnost (sekce 4.6). V čem konkrétně spatřujete tuto závažnost a jakou nápravu vývojářům doporučujete?

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.