FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš, Ph.D.
Student:	Vojtěch Zabořil
Název práce:	Bezpečnostní analýza aplikace Anketa ČVUT
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	26. 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

Velká většina zadání byla splněna dle očekávání. Určité výhrady mám k bodu 2 (rešerše aktuálně používaných metodologií pro bezpečnostní analýzy), v němž je text práce velice stručný a v důsledku není pro čtenáře dostačující ani pro porozumění jednotlivým metodikám, ani pro pochopení, proč tedy byla zvolena právě metodika OWASP Web Security Testing Guide.

2. Písemná část práce 80 / 100 (B)

Odhlédneme-li od velmi stručné kapitoly 2, je jinak textová stránka práce na vysoké úrovni. Stěžejní třetí kapitola se samotnou bezpečnostní analýzou je velmi detailní a působí důvěryhodně, jak v částech s nálezy zranitelností tak v ostatních (tzn. čtenář patrně může věřit, že části bez nálezů jsou bezpečné). Také čtvrtá kapitola s celkovým vyhodnocením a návrhem opatření odpovídá tomu, co bychom v podobné práci očekávali. Jazyková i technická stránka je v pořádku, nemám k ní výhrady.

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

Nepísemná část práce je velmi omezená, vedle zdrojového kódu samotné zprávy ji tvoří hlavně zdrojové kódy analyzované aplikace (Je toto v pořádku? Mělo by být více viditelně uvedeno, že nejde o dílo studenta!), velmi jednoduchá ukázka načtení kódu aplikace v IFRAME (bez demonstrace samotného clickjackingu, ačkoliv ji název adresáře slibuje) a dále výstup jednotlivých nástrojů použitých pro analýzu aplikace. Tento výstup není přímo v přiložených souborech komentován, jeho klíčové části jsou však vhodně popsány v

textu práce a zde jsou pro úplnost. S ohledem na charakter závěrečné práce je to odpovídající.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Výsledkem práce je dosti detailní a důkladná analýza bezpečnosti aplikačního kódu aplikace. Student tak navazuje na loňskou analýzu anonymity Ankety a dává nyní uživatelům (studentům, vyučujícím i vedení školy) důvody pro důvěru, že data v Anketě jsou poctivá. Nalezené zranitelnosti a doporučení pro budoucí vývojáře, pokud budou zranitelnosti opraveny a doporučení reflektována při dalším vývoji, pak zakládají důvod pro očekávání, že data poctivá budou i v budoucnosti.

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 85 /100 (B)

Student v rámci bakalářské práce vypracoval dosti rozsáhlou a detailní bezpečnostní analýzu aplikace Anketa ČVUT. Způsob provedení odpovídá standardním postupům, student postupoval pečlivě a práci se důkladně věnoval, což činí vytvořenou analýzu dosti důvěryhodnou. Mrzí mě slabší teoretický úvod do State of the Art, který poněkud snižuje hodnotu práce jako práce bakalářské, samotný výsledek analýzy je ale kvalitní. Práci doporučuji k obhajobě a hodnotím známkou B - velmi dobře.

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.