FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Josef Kokeš, Ph.D.
Student:	Radek Večerník
Název práce:	Bezpečnostní analýza zálohovacího nástroje Duplicati
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	28. května 2023

Hodnotící kritéria

1. Splnění zadání

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

Zadání hodnotím jako v zásadě splněné, s výhradou u bodu 3 - určitá analýza použité kryptografie sice proběhla, ale řadu jejích aspektů jen student převzal z dřívějších zdrojů a dále nekomentoval. Domnívám se, že zejména otázka integrity záloh je velmi důležitá a měla proběhnout její nezávislá analýza. Totéž platí i pro kryptografické části mimo zpracování hesla.

2. Písemná část práce

80 / 100 (B)

Text práce v pokrývá předmětnou oblast, domnívám se, že ale mohl být podrobnější. Zejména klíčová kapitola 3 je psána poněkud nešťastně: Části 3.1 a 3.2 jsou velice stručné, takže o použitém šifrování dat víme akorát to, že se používá AesCrypt nebo GPG, ale ani u jednoho neznáme konkrétní nastavení (u prvního zejména odvození klíče a použitý šifrovací režim, u druhého typ a velikost klíče). Část 3.4 a 3.5 je naopak popisovaná velmi rozvláčně, diagram nebo algoritmus by stejnou informaci poskytl v mnohem zhuštěnější a snáze kontrolovatelné podobě, a přitom nedostatečně přesně - teprve z následující kapitoly jsem pochopil, že "zpracováním funkcí SHA256" je myšleno jedno zahashování. Zaráží mě také opakované doporučení na použití PBKDF2 s 10000 iteracemi, což lze dnes chápat spíše jako naprosté minimum než jako vhodné doporučení. Velmi diskutabilní je také ohodnocení zranitelnosti "povolení použít slabé vstupní heslo" jako kritické s hodnotou 10,0. Jinak je ale text po faktické stránce v pořádku.
Co se týče jazyka, student má občas tendenci uchylovat se k ne zcela vhodným slovním obratům jako "spousta dat", časté jsou také překlepy. Zvláště mě dráždí používání TSL

namísto správného TLS, ale aspoň konzistentně napříč celým textem - i včetně přehození popisu písmen v seznamu zkratek.

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

Nepísemná část je velmi chudá, tvoří ji pouze vytvořené soubory dekompresní bomby. Autor klidně mohl přiložit i její zdrojový kód, který je nyní pouze v textu v příloze A. To ale není velký problém. Výrazně více chybí části, na které se student odkazuje v kapitole 4 a v příloze B - zejména bych chtěl vidět zachycené komunikační packety s citlivými údaji nebo uložení citlivých údajů v databázi. To jsou podklady, které jsou pro správné zhodnocení nalezených zranitelností, kritické.

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

Výsledkem práce je bezpečnostní analýza aplikace. Co vidím jako přínosné, je detailní prozkoumání a vyhodnocení toho, jak Duplicati pracuje s heslem. Další části analýzy jsou podle mě výrazně méně užitečné, buď pro chybějící podpůrná data (předchozí bod) nebo proto, že jde jen o odkazy na cizí práce, vlastní nezávislé ověření chybí (samotné šifrování, ověřování integrity).

Celkové hodnocení 75 /100 (C)

Zadání po studentovi požadovalo provedení bezpečnostní analýzy nástroje Duplicati a toto student provedl. Silné zaměření na zpracování hesla je správné, přijde mi však, že tím student považoval kryptografickou část aplikace za vyřešenou a další aspekty pustil z hlavy, což bylo zřejmě předčasné. Nejsem úplně nadšen senzačně vysokým hodnocením nalezených zranitelností, které podle mě spíš neodpovídá realitě. Také doporučená nápravná opatření jsou v některých případech diskutabilní. Toto vše, spolu s chudou netextovou částí, oslabuje důvěryhodnost práce, což mi přijde jako škoda. I tak ale beru účel práce za splněný, doporučuji práci k obhajobě a hodnotím ji známkou C-dobře.

Otázky k obhajobě

Jak reagoval na nalezené zranitelnosti vývojář aplikace?

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.