FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Tomáš Dvořáček
Oponent práce:	Ing. Josef Kokeš
Název práce:	Zranitelná webová aplikace jako didaktická pomůcka
Obor:	Počítačová bezpečnost

Datum vytvoření: 20. 1. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
V diplomové práci student analyzuje sadu známých zranitelných aplikací, systematicky jejich zranitelnosti člení a popisuje, v čem spočívají. Na to navazuje vytvořením sady nových zranitelných aplikací, které zahrnují stejné ale i nové zranitelnosti. Zadání hodnotím jako splněné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*60 (D)*

Popis kritéria:
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. 26/2017, 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.

Komentář:
Písemná část práce vykazuje bohužel řadu problematických míst. Mezi ně patří tato:

1) Značné množství jazykových chyb. Narazil jsem na hrubky v i/y, nesoulad pádů, neshodu podmětu a přísudku, chybějící čárku za vloženou vedlejší větou (velmi často!).

2) Nezanedbatelné množství překlepů, chybí důkladnější kontrola odevzdané práce. Například ani jedna ze zmiňovaných licencí není v seznamu zkratek uvedena správně (pokud je tam vůbec).

3) Není vhodné, aby podkapitola neměla žádný text a rovnou navazovala podpodkapitolou, jako např. u kap. 1.1, 1.2, kde by se vysvětlení, co je trénovací resp. zranitelnou realistickou aplikací myšleno, velmi hodilo.

4) Pro ukázky kódů by mělo být použito prostředí, které nemění význam jednotlivých znaků (typicky v práci z programátorského apostrofu vznikl typografický).

5) Celkově problematická struktura. Zvolená struktura má svůj logický smysl, vede ale k tomu, že čtenář naráží na nesrozumitelné zkratky zranitelností, které budou vysvětleny později, a k tomu, že stěžejní část textu je uložena v kapitole 1.3, kterou tvoří více než 30 stran bez dalšího členění v obsahu, což činí dodatečné dohledávání velmi komplikovaným. Preferoval bych samostatnou kapitolu pro zranitelnosti a na ni navazující samostatnou kapitolu pro popis přítomnosti těchto zranitelností v aplikacích.

6) Velmi problematická práce s externími zdroji. Velká část odkazů ve skutečnosti slouží jen jako odkaz na stránky použité aplikace, nejde o citaci dokládající faktické tvrzení. Přitom ale nejsou odkazovány všechny aplikace, citelně chybí ty z projektu Foundstone; to, že k nim neexistuje oficiální zdroj, tím spíš vyžaduje přesné doložení, jaká verze aplikace byla zkoumána! Faktická tvrzení často nejsou dokladována vůbec (např. str. 6 nahoře, že nejčastější formou HTTP autentizace je basic+TLS). Z kapitoly 1.3 (nejrozsáhlejší část práce) je odkazováno velmi sporadicky, není jasné, jestli proto, že všechno, co nebylo explicitně citováno, pochází ze zdroje [12], nebo proto, že student citace zcela pominul. Speciálně zde přitom citace jsou nutné, protože samotný popis je stručný až na hranu únosnosti, odkazy na další zdroje by zde byly vysoce užitečné.

7) Formální provedení citací je na nízké úrovni. Mnohdy chybí autor, téměř vždy chybí rok vzniku, struktura je nekonzistentní ([1] používá [autor, název]; [2] používá [název], [3] používá [autor], [11] používá [název, autor], [19] používá [autor, autor]). Autoři u zdroje [20] jsou uvedeni jak ve formě [příjmení, jméno], tak [jméno příjmení] a tentýž autor je u zdroje [16] uveden jako [příjmení, j.].

8) Důsledkem relativní stručnosti kapitoly 1.3 (ve smyslu "délka děleno počtem zranitelností") je i to, že popisy jsou poměrně povrchní a/nebo nekompletní, typicky chybí popis příčin nebo řešení (obrany), eventuálně rozbor podmínek, za kterých může být zranitelnost zneužita (např. které verze prohlížečů řeší problematiku SOP). Popisy místy vyvolávají dojem mnohem užšího problému, než o jaký skutečně jde (např. zranitelnost 1.5.2 se zdaleka netýká jen tabulkových procesorů).

9) Chybí mi objektivnější zdůvodnění, proč je vhodné používat jako zdroj knihu z roku 2011 nebo aplikaci z roku 2006, ke které už ani neexistuje oficiální distribuční místo. Chápu, že to vyplynulo z požadavků vedoucího, ale přesto bych u tak dynamického tématu, jako je bezpečnost webových aplikací, očekával aktuálnější zdroje.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*92 (A)*

Popis kritéria:
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

Komentář:
Vytvořené výukové programy jsou velmi zdařilé. Vítám použití méně obvyklého prostředí (Python+SQLite) proti běžnému PHP+MySQL, protože studenti potřebují vidět, že jde o obecné problémy, které nejsou vázány na nějaké konkrétní prostředí, i že se musí zabezpečení věnovat sami, protože prostředí to za ně neudělá. K práci je přiložen jak návod na instalaci "od nuly", tak funkční virtuální prostředí, které lze okamžitě nasadit. Zvolená licence je pro daný účel vhodná. Nelíbí se mi úplně, že pro studenty, kteří mají ve vytvořených aplikacích najít zranitelnosti, existuje "jediné správné řešení", preferoval bych otevřenější přístup.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*92 (A)*

Popis kritéria:
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.

Komentář:

Práce řeší a implementuje známá bezpečnostně citlivá místa. To je v pořádku, stejně jako zaměření na ty nejznámější problémy - při výuce má jistě smysl akcentovat, s čím se budou studenti v praxi setkávat nejčastěji. To odevzdaná práce zajišťuje velmi pěkně a jistě bude pro výuku etického hackování přínosná. Chápu také, že objem odvedené práce musel být značný. Přesto mě mrzí, že méně běžné zranitelnosti nebyly více využity, i kdyby jen jako "bonus" pro aktivní studenty.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

1) Na straně 7 tvrdíte, že podle zdroje [10] bychom měli kontrolovat hesla na určité skutečnosti. Odkud pochází tato doporučení? Ve zdroji [10] nic takového nevidím.

2) Za předpokladu, že bude uvolněno financování US státních organizací, srovnejte svoje doporučení z předchozí otázky a loňská doporučení NISTu (publikace SP800/63b).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*75 (C)*

Popis kritéria:
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.

Text hodnocení:

Odevzdanou práci vnímám jako rozporuplnou. Vytvořené programy jsou velmi pěkné a užitečné, naproti tomu textová část práce vykazuje řadu problémů. Některé mohly být vynuceny zadáním (ale proč v tom zadání jsou?!), řada jich ale vyplývá z odbyté a/nebo nestihnuté kontroly, což je škoda. Zejména citace jsou provedeny poměrně špatně a je snadno představitelné, že čtenář bude kapitolu 1.3 hodnotit místy až jako plagiát. Z toho důvodu volím pouze hodnocení "dobře", přestože z pohledu zadání a jeho splnění je práce přinejmenším "velmi dobrá", ne-li výborná.

Podpis oponenta práce: