FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Tomáš Dvořáček
Vedoucí: práce:	RNDr. Daniel Joščák, Ph.D.
Název práce:	Zranitelná webová aplikace jako didaktická pomůcka
Obor:	Počítačová bezpečnost

Datum vytvoření: 22. 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:

Autor práce najprv popisuje zranitelnosti u vybraných aplikácií, ktoré sú používané ako didaktické pomôcky pre pentračných testerov a vývojarov. Následne zraniteľnosti kategorizuje a nachádza dve zraniteľnosti, ktoré vo vybraných aplikáciach nie sú obsiahnuté. V praktickej časti práce autor vytvoril vlastnú sadu zraniteľných aplikácií, kde implementuje tieto dve zraniteľnosti spolu s niekoľkými ďalšími zraniteľnosťami už obsiahnutými v ostaných aplikáciách.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*70 (C)*

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:

Rozsah predloženej práce považujem za primeraný a práca neobsahuje zbytočné texty. Gramatickú stránku textu nedokážem objektívne posúdiť.
Po vecnej stránke mám výhrady k nasledovnému:
1. Logická štruktúra textu. Podkapitola 1.3 je najrozsiahlejsia časť práce, ktorá obsahuje popis zranitelnosti, popis jej hľadania, popis obrany a príklady v skúmaných aplikáciách. Prehľadnosť tejto kapitoly je problematická a jej podkapitoly nie sú uvedené v obsahu práce.
2. Citácie a referencie sú miestami chýbajúce (napr. v úvode pri prvej zmienke projektu HackMe od firmy Foundstone) a miestami nedostatočne presné (chýba rok, prípadne strana, citácie nemajú rovnaký formát). Vzhľadom na šírku témy, ktorú práca pokrýva by bolo nerealne popísať vysvetliť všetky termíny, o to propešnejšie by boli odkazy a referencie na rožširujúci materiál, prípadne zdôrazniť, že popis v práci nie je úplný.
3. V kap. 1.3.1 pri uvedení vety: "V praxi se lze nejvíce setkat s HTTP basic autentizací kombinovanou s TLS" nie je uvedená referencia, naviac v porovnaní s "form based" autentizáciou ide o zriedkavejší typ.
4. Čitateľnosť a štylistika textu je miestami obtiažnejšia.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*93 (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:

Sada vytvorených didaktických pomôcok je veľmi podarená a dobre spracovaná. Autor sa rozhodol pre použite prostredia Django založeného na jazyku Python s databázou SQLite. Týmto rozhodnutím autor išiel proti prúdu aplikácií založených na PHP a tradičných databázach (napr. MySQL, MS SQL). Zároveň dokázal, že zraniteľnostiam webových aplikácií sa nedá zabrániť jednoduchým výberom "bezpečného prostredia (framework)". Práca obsahuje návod pre inštaláciu aj virtuálny obraz predpripraveného prostredia, v ktorom sú vytvorené aplikácie ihneď k dispozícii.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*95 (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:

Vytvorená zraniteľná aplikácia spolu s prehľadom zraniteľností v už vytvorených aplikáciach projektov OWASP BWA a HackMe od firmy Foundstone sú výborným podkladom pre výučbu a nácvik penetračného testovania webových aplikácií napríklad pre predmet etický hacking. Vybrané aplikácie pokrývaju širokú škálu zraniteľností, ktoré si študenti dokážu prakticky vyskúšať. Autor zbierku zraniteľných aplikácii môže ďalej rozširovať.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: *1=výborná aktivita,* ***2=velmi dobrá aktivita,*** *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Študent pri práci postupoval samostatne s pravidelnými konzultáciami s vedúcim práce. Podstatnú časť príprav študent venoval vývoju vlastnej didaktickej pomôcky a jej zdokonaľovaniu. Uvítal by som rovnakú súčinnosť pri konzultáciách textu práce, kde zostal značný priestor na vylepšenie.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*80 (B)*

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:

Práca obsahuje veľmi podarenú praktickú časť, kde bola vytvorená didaktická pomôcka pre potreby nácviku hľadania zraniteľností penetračnými testermi. Predpokladám jej dobré využitie pri výučbe alebo cvičeniach zameraných na etický hacking. Zároveň práca obsahuje menej vyváženú písomnú časť, ktorá celkové hodnotenie posúva nadol. Prácu doporučujem k obhajobe.

Podpis vedoucího práce: