



Hodnocení vedoucího závěrečné práce

Student: Bc. Pavlína Kopecká
Vedoucí práce: Ing. Jan Zíka
Název práce: Analýza web skimmingu
Obor: Počítačová bezpečnost

Datum vytvoření: 22. 1. 2021

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: Každý jednotlivý bod zadání byl bez výhrad splněn. Důležité body zadání byly navíc propracovány výjimečně detailně.	
Hodnotící kritérium:	Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):
2. Písemná část práce	80 (B)
Popis kritéria: Zhodnotte 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. Zhodnotte 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. Zhodnotte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.	
Komentář: Po obsahové stránce není v popisové části diplomové práce co vytknout, kladem je i bezesporu velké množství citací. Práce je však bohužel lehce nepřehledně členěna, obsahuje krkolomější formulace a typografické chyby. Je také škoda, že studentka více neakcentovala fakt, že škodlivé kódy a URL, které uvádí pro názornou ilustraci útoků, získala vlastní analýzou napadených stránek.	
Hodnotící kritérium:	Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):
3. Nepísemná část, přílohy	90 (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: Příložené aplikace jsou sice jen jednodušší, ale skvěle doplňují popisovou část práce. Obě aplikace především dokazují, že hypotézy postulované v textu práce platí bez výhrad a že není potřeba tisíců řádků kódu ani pro ochranu koncového zákazníka, ani pro výkaz bezpečnostního analytika. U obou aplikací by sice nevalil delší popis jejich funkce, ale vzhledem k jejich velikosti jistě není nezbytný.	
Hodnotící kritérium:	Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):
4. Hodnocení výsledků, jejich využitelnost	100 (A)
Popis kritéria: Dle charakteru práce zhodnotte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.	

Komentář:

Práci lze rozdělit na dvě části: popisovou, ve které se studentka věnuje teorii web skimmingu a praktickým ukázkám škodlivých kódů, a implementační, ve které napsala dvě samostatné aplikace na ochranu před web skimmingem a testovací stránku, kde lze aplikaci otestovat na příkladech jednotlivých typů web skimmingu.

Co se týče popisové části, studentka představuje obsáhlou rešerši web skimmingu jako takového i detailní analýzy velkých web skimming útoků v nedávné době. Celou tuto část pak doplňuje velké množství praktických ukázek, které během přípravy diplomové práce zajistila. Práce tedy může mít přínos nejen jako úvod do problematiky pro laiky, ale i jako přehledná databáze zranitelností a manuál pro pokročilejší administrátory, kteří neberou zabezpečení uživatelů svých internetových obchodů na lehkou váhu.

V implementační části studentka představila formou jednoduchých aplikací dvě jí vybrané metody ochrany uživatele. Obě aplikace mají sice do produktů, které by si nainstalovalo větší množství lidí, daleko, ale jejich pravý cíl, totiž že bezpečnost nemusí být složitá, akcentují dobře. Čtenář tak může porovnat dva různé přístupy, aniž by musel vyvinout větší úsilí na jejich pochopení. Kvituji také rozmanitost forem a cílů obou aplikací: jedna je javascript doplněk do prohlížeče vhodný pro koncového uživatele, zatímco druhá je python aplikace spustitelná z příkazové řádky pro bezpečnostního analytika.

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 samostatně tvůrčí práce (5b).

Komentář:

Studentka projevila mimořádnou aktivitu a spolehlivost zejména při získávání podkladů k diplomové práci. Na tomto místě je třeba upozornit na časovou omezenost dostupných zdrojů. Web skimming útoky jsou totiž zpravidla brzy odstraněny; pro jejich analýzu je tedy třeba jednat rychleji než administrátoři internetových obchodů. To se studentce podařilo na výbornou; pouze díky její aktivitě bylo možné popsat tolik druhů útoků a získat tolik ukázek škodlivých kódů.

Hodnotící kritérium:

Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):

6. Celkové hodnocení

95 (A)

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:

Diplomovou práci doporučuji k obhajobě a hodnotím ji klasifikačním stupněm A – výborně.

Podpis vedoucího práce: