FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Pavlína Kopecká
Oponent práce:	Ing. Josef Kokeš
Název práce:	Analýza web skimmingu
Obor:	Počítačová bezpečnost

Datum vytvoření: 15. 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:
Zadání bylo splněno v mimořádném rozsahu i kvalitě.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

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 je velice detailní a rozsáhlá a komplexně pojednává o předmětné oblasti. Obsahuje obrovské množství informací, které nejsou běžně dostupné, a už jenom rešerše musela dát studentce obrovskou práci a sama o sobě by bez problémů mohla fungovat jako samostatná diplomová práce. Po faktické stránce také není mnoho co vytknout, jedinou skutečnou výhradu mám proti tvrzení, že chyba typu File Inclusion se týká pouze aplikací v PHP (str. 8).

Výraznější nedostatky shledávám v jazykové a formální stránce práce. Za nejpodstatnější chybu považuji velmi časté míchání češtiny a angličtiny i tam, kde k tomu není důvod, mnohdy i bez vysvětlení, co daný termín vlastně znamená. Vzhledem k už tak značnému rozsahu práce to chápu, text se tak ale stává velmi nepřátelský vůči čtenáři, který předmětnou oblast dopředu nezná. Stejnou výhradu i stejné pochopení mám k úrovni detailů kapitoly 4, je proti předchozím kapitolám citelně stručnější a působí, jako kdyby na ni nezbylo tolik času. Není chybná nebo špatná, ale je znát velký rozdíl proti kapitolám předchozím. Chybí mi každopádně aspoň stručná připomínka, že uživatel má možnost falešnou platbu kartou i dodatečně stornovat (chargeback) a že banky typicky mají velmi sofistikované mechanismy pro detekci a prevenci neobvyklých plateb.

Otázkou je zdroj jednotlivých demonstračních skriptů. Je jich obrovské množství a pokrývají jak širokou oblast, tak velké časové rozpětí. Není jasné, jestli je studentka nasbírala a zpracovala (např. deobfuskovala) všechny sama nebo jestli některé pocházejí z cizích zdrojů (např. záchyty v Avastu).

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:

Studentka vytvořila obranný plugin do prohlížeče Firefox. Je poměrně krátký a jednoduchý, ale svoji práci plní a jeho jednoduchost je spíše dokladem velmi dobře provedené analýzy, díky které mohla jít studentka přímo k jádru problému. Uvítal bych nicméně, kdyby přímo v manifestu pluginu nebo aspoň v nějakém readme souboru byla uvedena licence, nyní ji uživatel musí hledat v textu diplomové práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*98 (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:

Práci považuji za velice přínosnou jak po stránce teoretické, kde představuje mimořádně kvalitní rešerši předmětné problematiky, tak po stránce praktické. Samotný plugin pro prohlížeč je spíše proof-of-concept, pro praktické využití by potřeboval dopracovat mechanismy uchovávání a aktualizace dat včetně uživatelských black- a whitelistů, ale jeho jádro je dobré a stojí na pevných základech.

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) Odkud pocházejí skripty, kterými demonstrujete jednotlivá tvrzení ve své práci?
2) Zveřejnila jste už někde svůj plugin a máte reakce od uživatelů?
3) Můžete odhadnout náročnost úpravy pluginu pro prohlížeče postavené na jádru Chromium?
4) Na základě jakých kritérií jste vybírala domény pro naplnění whitelistu vašeho pluginu?

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:

Posuzovaná diplomová práce představuje velice detailní a podrobné zpracování poměrně náročného tématu. Studentka na ní odvedla enormní množství práce a na kvalitě výsledku to je znát. Výhrady uvedené v jednotlivých částech hodnocení platí, ale s ohledem na celkovou kvalitu práce je nepovažuji za stěžejní. Proto práci doporučuji k obhajobě a hodnotím známkou A-výborně.

Podpis oponenta práce: