FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Hodnocení vedoucího závěrečné práce

| | |
|---|---|
| **Student:** | Bc. Tomáš Stefan |
| **Vedoucí: práce:** | RNDr. Daniel Joščák, Ph.D. |
| **Název práce:** | Security assessment of web application penetration testing tool |
| **Obor:** | Počítačová bezpečnost |

**Datum vytvoření:** 23. 1. 2021

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

Zadanie bolo splnenené podľa popisu. Autor práce si vybral za predmet analýzy nástroj Burp od poskytovateľa Portswigger. Popísal jeho funkcionalitu, navrhol a vyskúšal testovanie jej niektorých zraniteľností a výsledky sumarizoval.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **2. Písemná část práce** | *80 (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:*

Rozsah predloženej ZP je primeraná zadaniu a ciele zadania spĺňa. Teoretická a praktická časť práce sú rozsiahlosťou vyvážené a po vecnej stránke v poriadku. V teoretickej časti práce by som ocenil podrobnejšie zdôvodnenie výberu a popis použitej metodológie, a prečo sa autor rozhodol venovať práve popísaným aspektom bezpečnosti, prípadne odkazy na alternatívne spôsoby.
Jazykovo je práca napísana vo veľmi dobrej angličtine. Formálne a typograficky je práca spracovaná dobre, autor pomerne často využíva poznámky pod čiarou, bibliografia by mohla byť napísaná efektívnejšie (napr. RFC 6455 sa v nej nachádza osemkrát), ale závažnejšie chyby alebo omyly sa v nej nenachádzajú.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **3. Nepísemná část, přílohy** | *85 (B)* |

*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:*

Nepísomná časť práce je stručná, ale obsahuje všetko, čo autor v práci popisuje. Vytvorené skripty a časti programov sú čitateľné a zrozumiteľne okomentované.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **4. Hodnocení výsledků, jejich využitelnost** | *90 (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:*

Výsledky práce majú význam jednak pre autorov aplikácie Burp a jednak pre jej používateľov. Autori aplikácie môžu použiť výsledky pre preukázanie jej kvality respektíve reakciu na spomenuté vlastnosti a nedostatky - hlavne nedokumentovaného REST API volania umožňujúceho zastavenie aplikácie (reakcia autorov aplikácie Burp v čase odovzdania práce nebola známa). Za veľmi zaujímavý a originálny považujem popis ako zachytávať a analyzovať celú komunikáciu nástroja Burp smerom k jej autorom alebo inam a popis obsahu danej komunikácie.

| *Hodnotící kritérium:* | *Způsob hodnocení – následující škálou 1 až 5:* |
|---|---|
| **5. Aktivita a samostatnost studenta** | 5a:<br>***1=výborná aktivita,***<br>*2=velmi dobrá aktivita,*<br>*3=průměrná aktivita,*<br>*4=slabší, ale ještě dostatečná aktivita,*<br>*5=nedostatečná aktivita*<br>5b:<br>***1=výborná samostatnost,***<br>*2=velmi dobrá samostatnost,*<br>*3=průměrná samostatnost,*<br>*4=slabší, ale ještě dostatečná samostatnost,*<br>*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, ktoré boli ovplyvnené súčasnou pandemickou situáciou.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **6. Celkové hodnocení** | *82 (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:*

Celkovo je práca hodnotným prínosom pre nezávislé posúdenie bezpečnosti nástroja pre penetračné testovanie webových aplikácií Burp. Autor sa venuje jej novým funkcionalitám, ukazuje nápad ako ich analyzovať a prináša zaujímavé výsledky. Veľmi užitočný je aj popis ako zachytávať a analyzovať komunikáciu nástroja Burp a popis obsahu danej komunikácie.
ZP považujem za veľmi dobrú a doporučujem ju k obhajobe.

Podpis vedoucího práce: