FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Bc. Martin Pozděna, MSc.
Student:	Pavel Khunt
Název práce:	Bezpečnostní audit portálu LearnShell
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	2. června 2021

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

V bodu 3. Zadání je uvedeno „Proveďte white-box bezpečnostní audit / penetrační test všech vektorů útoku nalezených v kroku 2." V době zadání BP nebyl znám rozsah a počet vektorů útoku v aplikaci LearnShell. Výstupem kroku 2 byl seznam 11 vektorů útoku, kdy provedení penetračního testu pro všechny tyto vektory by výrazně převyšovalo standardní rozsah bakalářské práce. Po konzultaci se studentem jsem doporučil zúžit počet testovaných vektorů útoku na 4 hlavní – infrastrukturní test 147.32.232.212 a 10.38.5.90, penetrační test webu https://learnshell.fit.cvut.cz a penetrační test GraphQL API.

2. Písemná část práce 70 / 100 (C)

Práce má adekvátní logickou strukturu a rozložení. Práce má nadprůměrný rozsah, ale obsahuje části, které mohou být pokládány za zbytečné, například: detailní popis různých typů skenování portů v nástroji nmap. Práce obsahuje občasné překlepy či nedokončené věty jako „Hodnocení se tedy opírá o porovnání mých nálezů a zmíněné konzultace ohledně těchto". Občasné lehce neakademické výrazy: „Z obrázku 4.12 je vidět, že příkaz je povolený a shodí Redis." Některá faktická tvrzení jako „Tento způsob hešování je považován organizací NIST za bezpečný." by bylo vhodné doplnit citací. Občas se vyskytuje nevhodné využití anglických výrazů v rámci české věty: request vs požadavek. V případě tvrzení „Hodnocení závažnosti je založeno na CVSS v3.1." by bylo vhodné uvést i samotné CVSS v3.1 skóre.

3. Nepísemná část, přílohy 95 /100 (A)

Práce spočívala v provedení bezpečnostního auditu (penetračního testu). Zranitelnosti, které student odhalil jsou opakovatelné a v bakalářské práci doložené adekvátními důkazy (screenshoty).

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Práce odhalila relativně velké množství zranitelností v portálu LearnShell. Na samotném výsledku bakalářské práce je vidět, že student investoval nadprůměrné úsilí do praktické části. Jsem přesvědčen, že odhalené zranitelnosti jsou v praxi velmi dobře použitelné pro zvýšení kybernetické bezpečnosti portálu LearnShell.

5. Aktivita studenta

[1] výborná aktivita
▸ **[2] velmi dobrá aktivita**
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student projevil výbornou aktivitu během praktické části práce a průměrnou aktivitu během psaní bakalářské práce. Celkově po zprůměrování tedy hodnotím jako velmi dobrou aktivitu.

6. Samostatnost studenta

[1] výborná samostatnost
[2] velmi dobrá samostatnost
▸ **[3] průměrná samostatnost**
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Student projevil výbornou samostatnost během praktické části práce, kdy naprosto autonomně nastudoval všechny typy zranitelností, nástrojů k jejich odhalení, vyhledával dané zranitelnosti a úspěšně je zneužíval (exploitoval). V rámci teoretické práce a během zpracování a prezentování výsledků penetračního testu byla samostatnost obecně slabší, ale ještě dostatečná. Student může být v oblasti bezpečnostního auditu či výzkumu úspěšný za předpokladu, že zapracuje na svých soft skills – psaní technických zpráv, strukturovaná prezentace výsledků atd.

Celkové hodnocení 85 /100 (B)

Praktickou část hodnotím jako výbornou – A. Teoretickou část jako C.

Instrukce

Splnění zadání

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.

Písemná část práce

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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Aktivita studenta

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.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

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.