FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš
Student:	Aleš Répáš
Název práce:	Bezpečnost webových aplikací a její penetrační testování
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	22. května 2022

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo v zásadě splněno, v práci jde dohledat všechny jeho body, ale kvalita splnění je nízká a výsledná práce v důsledku toho neplní svůj účel.

2. Písemná část práce 30 / 100 (F)

Text práce je značně problematický. Formálně sice splňuje stanovenou délku, prakticky ale není dobře strukturovaný a obsahuje části, které považuji za zbytečné - např. celou kapitolu 1 až na sekci 1.3, která naopak měla být o dost podrobnější. Řada dalších částí je relevantní, ale jejich umístění v logice textu je zvláštní (např. sekce 2.3 dost nesmyslně pojednává zejména o nástrojích, které jsou k dispozici pro splnění požadavků tohoto kroku penetračního testování, včetně zbytečně detailního popisu OWASP ZAP, který rozhodně patřil jinam).

Hlavní části textu z pohledu zadání jsou vesměs hodně stručné a poměrně povrchní, v řadě případů možná až nesprávné. Např. samotná zranitelnost CSRF, o které má celá práce být, je ve své podstatě popsána na jediné stránce, a to ještě spíš podle jejích projevů než podle toho, co to ve skutečnosti je. Obdobně návrh detekčního pluginu pro OWASP ZAP je nesmírně vágní; jestli jsem ho pochopil správně, tak de facto spočívá na detekci hlaviček Referer a Origin a na kontrole toho, jak na ně reaguje webová aplikace - aniž by však bylo nějak důvěryhodně vysvětleno, proč by zrovna tyto hlavičky měly nějak signalizovat přítomnost CSRF, když jsou plně pod kontrolou prohlížeče zatímco CSRF je zranitelností serverové strany, a aniž by byl jakkoliv objasněn způsob, jak je rozpoznána reakce na jejich změnu (jenom pouhým porovnáním webové stránky mezi dotazy to nejde, mnoho běžných stránek dnes při dalším dotazu zobrazí poněkud jiný obsah, už jen kvůli například

reklamě nebo výběru z "nejzajímavějších článků"; z kódu můžeme zjistit, že student zjišťuje, zda se změnil HTTP Response Code).

Nedostatečná je část testování vyhotoveného pluginu, které proběhlo proti Damn Vulnerable Web Application jakožto testovacímu prostředí a proti nepojmenovanému webu údajně plně ošetřenému proti zranitelnosti jakožto ostrému prostředí. Ani jeden z testů není průkazný - u DVWA bylo CSRF detekováno, ale už neproběhl test, jestli zvýšením úrovně obtížnosti detekce zmizí (vzhledem k použitému řešení by nejspíš měla), u reálné aplikace víme pouze o tom, že plugin generoval množství false positive upozornění, což je obecně problém, protože to plýtvá silami analytika na jejich ověřování. Nevíme ale nic o tom, jestli plugin vůbec dokáže něco relevantního detekovat. Očekával bych přinejmenším test na několika pokusných aplikacích s variací nastavení tak, aby bylo vidět, zda plugin skutečně funguje. Mohla posloužit například aplikace Fakebook, o které víme, že na CSRF zranitelná je.

Také po jazykové stránce není práce dobrá, obsahuje řadu jazykových chyb (čárky, i-y, shodu podmětu s přísudkem atd.) a i některé poněkud úsměvné drobnosti (str. 4 - ARPANET ve skutečnosti není produktem 19. století). V technickém textu by se neměla vyskytovat slova jako "spousta". Značná část odkazovaných článků postrádá autora (aspoň jméno firmy mohlo být!) a je otázka, do jaké míry jsou zdroje skutečně důvěryhodné (např. pro popis Metasploit je nepochopitelně použit web Simplilearn a ne stránky projektu; ponechávám stranou, zda vůbec bylo nutné o projektu psát) nebo důvěryhodně použité (např. zdroj [5] podle mě říká něco výrazně jiného než interpretace studenta). Zajímal by mě zdroj překladu CSRF do češtiny, protože silně nesouhlasím s překladem "podvržení křížového požadavku na webu".

3. Nepísemná část, přílohy

50 /100 (E)

Netextovou část práce tvoří rozšíření projektu OWASP ZAP o detekci práce s hlavičkami Referer a Origin. Skládá se z pěti velmi jednoduchých nových tříd pro detekci hlaviček, které je však velmi obtížné najít, protože nejsou nijak vyznačeny (jedná se o soubory OriginScanRule.java, RefererScanRule.java a OriginRefererScanRule.java v adresářích zap-extensions/addOns/ascanrules/src/main/java/org/zaproxy/zap/extension/ascanrules a zap-extensions/addOns/pscanrules/src/main/java/org/zaproxy/zap/extension/pscanrules). Po stránce implementace jsou v pořádku, dělají právě to, co text říká, že by měly dělat; problém je v tom, že text je zrovna v tomto bodě silně nevyhovující a kód tak sice dělá to, co bylo specifikováno, ale není to to, co by dělat měl.

4. Hodnocení výsledků, jejich využitelnost

20 /100 (F)

Obávám se, že v této podobě nemá práce praktický přínos. Vytvořený plugin možná funguje a možná nefunguje, z důvodu nedostatečné analýzy však není důvěryhodný. Ani textová část není pro uživatele příliš užitečná z důvodů uvedených výše.

5. Aktivita studenta

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

Jedním z důvodů neuspokojujícího výsledku práce je velmi slabá aktivita studenta. V zimním semestru za ní mohly být zdravotní důvody, takovou informaci ale nemám pro letní semestr a stále nerozumím tomu, proč vlastně student nevyužil možnosti odkladu. Jistě by to v takové situaci bylo možné. Ve výsledku tak konzultací proběhlo skoro doslova jen "pár" a v době, kdy nemohly nic podstatného změnit.

6. Samostatnost studenta

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

Kritérium nelze hodnotit, chybí podklady. Student něco samostatně vytvořil, takže asi není nesamostatný, na druhou stranu vytvořené dílo není použitelné, což nesvědčí ani pro samostatnost.

Celkové hodnocení 20 /100 (F)

Obávám se, že v současném tvaru nelze práci považovat za úspěšnou. Text je velmi stručný a povrchní, a to zejména ve svých klíčových částech, které tak zůstávají bez adekvátního vysvětlení. Vytvořený kód je kvůli tomu zcela nedůvěryhodný, i pokud funguje. Podle mě je nutné práci předělat - vrátit se k analýze a přinejmenším lépe vysvětlit možnosti řešení úlohy, následně je implementovat a zejména důkladně otestovat na vzorku, z jehož výsledků se bude dát něco usuzovat; je ke zvážení, jestli raději nepřejít na jinou zranitelnost než CSRF, která se automaticky detekuje obtížně. Zatím bohužel práci nemohu k obhajobě doporučit, hodnotím známkou F = nedostatečně.

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. 52/2021, 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.