FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Dostál, Ph.D.
Student:	Aleš Répáš
Název práce:	Bezpečnost webových aplikací a její penetrační testování
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	9. června 2022

Hodnotící kritéria

1. Splnění zadání

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

Body zadání č. 2, 3 a 4 možnosti a návrh modulu nástroje OWASP ZAP jsou hlavními body zadaní, přesto je jim v textové části práce věnováno jen nutné minumum.

2. Písemná část práce

55 / 100 (E)

Cílém práce bylo analyzovat možnosti nástroje OWASP ZAP a navrhnout modul pro detekci CSRF. Text práce je velmi nevyvážený a obsahuje nadbytečné kapitoly, např. v Úvod do kybernetické bezpečnosti, kde se autor věnuje sice aktuálním, nikoliv však relevantním tématům - vynecháním této kapitoly by se inofrmační hodnota práce určitě nesnížila. Dále se pak autor v další kapitole věnuje penetračnímu testování webových aplikací. Zde místo úvodu do penetračního testování, představení problematiky, metodologie testů apod. představuje rovnou nástroje, z nichž většina nemá přímou souvislost s prací. Až v posledních třech a půl stránkách autor popisuje nástroj OWASP ZAP, bohužel z těchto tři a půl stránek jsou zde dvě stránky s obrázky GUI daného nástroje. V další kapitole je představena cílená zranitelnost CSRF, avšak opět zcela povrchně popsána. Totéž se dá říct i o vlastním návrhu modulu, jeho implementaci a testování. Testování proběhlo jak na cvičném záměrně zranitelném prostředí, tak i dle tvrzení autora na reálné webové aplikaci. Z nepochopitelného důvodu ale autor vybral webovou aplikaci, pro jejíž testování musel podepsat NDA. V kapitole o výsledcích testování je tak jen zmínka, že z důvodu "mlčenlivosti a bezpečnosti" nemohl výsledky zveřejnit, což vnáší další pochybnosti o tom, jak byly testy vůbec provedeny.

3. Nepísemná část, přílohy 55 /100 (E)

Nepísemnou část tvoří SW dílo - rozšíření aplikace OWASP ZAP a to třídy v jazyku Java (to že se jedná o jazyk Java je zmíněno až v kapitole Závěr, v kapitole o implementaci modolu o tomto autor mlčí). Autor mi funkcionalitu nástroje prezentoval a nástroj díky rozšíření určité zranitelnosti CSRF detekoval. Ovšem kvůli nejasnému popisu testování a jeho výsledku nejsem schopen vyhodnotit, že autorovo řešení pracuje dle autorova tvrzení.

4. Hodnocení výsledků, jejich využitelnost 50 /100 (E)

Výsledkem práce je modul nástroje OWASP ZAP v jazyku Java, který rozšiřuje možnosti detekce zranitelnosti CSRF. Autor bohužel nezmiňuje, jakým způsobem lze modul využít.

Celkové hodnocení 55 /100 (E)

Výsledkem práce je modul nástroje OWASP ZAP v jazyku Java, který rozšiřuje možnosti detekce zranitelnosti CSRF. I přes dost slabou písemnou část autor odvedl určitou práci a s výhradami splnil zadání. Práci doporučuji k obhajobě a hodnotím stupněm E.

Otázky k obhajobě

Proč jste jako cílovou webovou aplikaci zvolil zrovna takovou, pro jejíž testovaní bylo potřeba podepsat NDA a připravil jste se tak trochu nešťastně o možnost zveřejnit výsledky?
Jaký další způsob rozšíření detekce CSRF by bylo možné využít a implementovat?

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.

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.