Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Oliver Polka** **Oponent:** **David Janota**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2017/2018**

Téma diplomové práce: **Návrh metodiky pro penetrační testování webových aplikací**

Hodnocení práce:
Práce diplomanta se zabývá návrhem metodiky penetračních testů, zaměřených primárně na webové aplikace. Kromě úvodu a závěru obsahuje 5 kapitol, rozdělených rovnoměrně do teoretické a praktické části.

Aktuálnost zvoleného tématu hodnotím jako (velmi) vysokou, poptávka po penetračních testech a etickém hackingu každoročně roste rapidně, což je dáno neustále se rozšiřujícím spektrem nelegálních činností v kyberprostoru. Sám diplomant uvádí velmi výstižně přehled faktů a statistik, která ho k výběru tohoto tématu vedla.

Obtížnost úkolu hodnotím jako poměrně velkou, kromě značných teoretických znalostí bylo nutno prokázat také schopnost teorii uplatnit při samotném penetračním testu. V oblasti znalosti problematiky diplomant prokázal výborné znalosti, povedlo se mu sepsat to nejpodstatnější, co by měl penetrační tester vědět před provedením testu. Taktéž v oblasti praktické nelze pravděpodobně nic vytknout – lze namítat, že spektrum penetračních testů je mnohem širší, nicméně při podrobnějším exkurzu by diplomant značně překročil rozsah práce.

Bohužel, výsledek v poslední části (tvorba metodiky) zůstal jen na půli cesty. Při přečtení úvodu a zadání bych očekával přetavení všech praktických a teoretických kapitol do vhodného step-by-step návodu pro např. začínající etické hackery. Z této části zadání je v práci pouze několik formulářů.

Po formální stránce je práce poměrně zdařilá, vhodně strukturovaná, dobře se čte. Citace jsou dle normy. Je škoda, že v ní zůstalo jisté množství překlepů (marvnostné, úradníka s cieľ získať peňažných, apod.). Při podrobnějším čtení překvapí autorova nechuť psát rozvité věty a zůstávat u jednoduchých, stejně jako občasné podivné umístění čárek tam, kde nemají být, příp. vynechání tam, kde být mají.

K obsahu samotnému mám následující poznámky:

- Demingův cyklus PDCA je dle mého názoru aplikace plan-do-check-act ve smyslu „plánuj-vykonej-zkontroluj jak to dopadlo-konej ve smyslu oprav“, aplikace v práci tomu spíše neodpovídá.
- Definice, které uvádí Ron Patton ve své knize z roku 2006 jsou dnes již zastaralé, oficiální termín pro chybu v softwaru je defekt, rozhodně ne selhání (to je důsledek vykonání kódu s defektem).
- V části vysvětlující projekt OWASP je zmíněn také jakýsi dokument, předp., že se jedná o OWASTP Top Ten.

I přes uvedené výtky nicméně práci hodnotím jako velmi kvalitní a při vhodném dopracování ji lze s úspěchem využít při praktickém vykonávání penetračních testů.

Dotazy:

1. Jak je ukotvena trestní odpovědnost za hacking ve slovenském právu (v ČR §230 Zák. 40/2009 Sb.)?
2. Jaký je rozdíl v aplikaci penetračního testu v agilním modelu vývoje proti klasickému modelu (tzv. vodopádu)?

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

B - velmi dobře.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 5. 6. 2018 Podpis oponenta diplomové práce