Posudek bakalářské práce

Matematicko-fyzikální fakulta Univerzity Karlovy

Autor práce	Vojtěch Žák
Název práce	Zranitelnosti webových aplikací
Rok odevzdání	2023
Studijní program	Informatika
Specializace	Programování a vývoj software

Autor posudku	Pavel Parízek	**Role**	Oponent
Pracoviště	Katedra distribuovaných a spolehlivých systémů		

Prosím vyplňte hodnocení křížkem u každého kritéria. Hodnocení *OK* označuje práci, která kritérium vhodným způsobem splňuje. Hodnocení *lepší* a *horší* označují splnění nad a pod rámec obvyklý pro bakalářskou práci, hodnocení *nevyhovuje* označuje práci, která by neměla být obhájena. Hodnocení v případě potřeby doplňte komentářem. Komentář prosím doplňte všude, kde je hodnocení jiné než *OK*.

K celé práci	lepší	OK	horší	nevyhovuje
Obtížnost zadání	☐	☐	☒	☐
Splnění zadání	☐	☒	☐	☐
Rozsah práce *... textová i implementační část, zohlednění náročnosti*	☐	☐	☒	☐

Komentář

Výstupem této práce je přehled běžných a častých bezpečnostních zranitelností webových aplikací, pro každou zranitelnost popis toho na jakém principu funguje (včetně jednoduchých příkladů), doporučení pro vývojáře jak se těm zranitelnostem mohou vyhnout, popis způsobů jak je mohou odhalit uživatelé, a také vysvětlení jak lze provést útoky které zneužívají tyto zranitelnosti.
Dalším výstupem je sada ukázkových webových aplikací, které demonstrují popsané bezpečnostní zranitelnosti. Sada je zveřejněna formou projektu Vulnerability Presentation Server (Vulpes).
Tato sada webových aplikací může být použita například ke vývoji a testování nástrojů pro detekci těchto zranitelností.

Není zřejmé, co bylo na práci technicky a odborně složité (třeba nový algoritmus, komplikovaná rozsáhlá implementace, řešení nějakého složitého problému).

Není mi také jasné, co je vlastně přínos této práce (ve srovnání s ostatními), protože výstup není z oblasti teoretické (algoritmus, důkaz), ani to není nový pohled na určité téma (oblast), a také to není rozsáhlé softwarové dílo.

Textová část práce	lepší	OK	horší	nevyhovuje
Formální úprava *... jazyková úroveň, typografická úroveň, citace*	☐	☒	☐	☐
Struktura textu *... kontext, cíle, analýza, návrh, vyhodnocení, úroveň detailu*	☐	☒	☒	☐
Analýza	☐	☒	☒	☐
Vývojová dokumentace	☐	☐	☒	☐
Uživatelská dokumentace	☐	☒	☒	☐

Komentář

Text popisuje základní typy bezpečnostních zranitelností (SQL injection, XSS, CSRF), ale víceméně úplně ignoruje složitější komplikovanější případy, jako třeba zranitelnost ve knihovně Log4j která se objevila v roce 2022.

Práce navíc hodně čerpá ze existujících zdrojů (OWASP, RFC dokumenty) a není tak zřejmé, co je hlavní přínos autora.

Dále není taky zřejmé, kdo reprezentuje cílovou skupinu textu, protože vývojáři a dostatečně poučení uživatelé budou znát obsah kapitol 1-3, a vývojáři také obsah dalších kapitol.

Kapitoly 1-3, tedy popis webových stránek, protokolů a webových aplikací, mohly jít více do hloubky, například ukázat jak vypadají a jak se tvoří (navrhují, implementují) skutečně velké moderní webové aplikace (typu iDNES.cz nebo alza.cz), jaké tam jsou největší praktické výzvy. atd.

Obsah kapitoly 7 ("newebové útoky") je hodně zajímavý (pro mě asi nejvíc z celého textu), a dozvěděl jsem se tam něco nového.

V kapitole 8.2 vůbec není zdůvodněno použití (výběr) jazyka Python a knihovny Flask.

V sekci 8.3 a podsekcích nejsou popsány detaily implementace těch demonstračních zranitelností, třeba kde může čtenář najít dotčený kód.

Uživatelská dokumentace v sekcích 8.5 a 8.6 vůbec neříká, jakou platformu (Windows nebo Linux) by měl uživatel použít a jaké důležité závislosti (Python, Docker) musí mít nainstalované.

Dotaz: proč není text napsaný anglicky?

Menší nedostatky:
- Ve kapitole 4 chybí úvodní popis zranitelnosti typu SQL injection.

Implementační část práce	lepší	OK	horší	nevyhovuje
Kvalita návrhu *… architektura, struktury a algoritmy, použité technologie*	☐	☒	☐	☐
Kvalita zpracování *… jmenné konvence, formátování, komentáře, testování*	☐	☒	☐	☐
Stabilita implementace	☐	☒	☐	☐

Komentář

Rozsah softwarové části a kvalita zpracování je odpovídající. Nemám výhrady.

Otázka stability implementace v tomto případě nedává smysl, protože výstupem jsou pouze aplikace, které demonstrují bezpečnostní zranitelnosti.

Celkové hodnocení Velmi dobře (spíše horší)

Práci navrhuji na zvláštní ocenění Ne

Datum 24. srpna 2023 **Podpis**