

# Posudek vedoucího bakalářské práce

## předložené na Matematicko-fyzikální fakultě Univerzity Karlovy

Autor: Vojtěch Žák  
Název práce: Zranitelnosti webových aplikací  
Stud. program a obor: informatika, programování a vývoj software  
Rok odevzdání: 2023  
Jméno a tituly vedoucího: Mgr. Martin Mareš, Ph.D.  
Pracoviště: Katedra aplikované matematiky  
Kontaktní e-mail: mares@kam.mff.cuni.cz

<b>K celé práci</b>	lepší	OK	horší	nevyh.
Obtížnost zadání		X		
Splnění zadání		X	X	
Rozsah práce		X	X	

Práce se zabývá bezpečnostními problémy webových aplikací. Obsahuje teoretický rozbor jejich druhů a způsobů obrany. Součástí je také software – soubor aplikací Vulpes, který jednotlivé zranitelnosti demonstruje.

Práce vznikala ve spolupráci se společností CZ.NIC.

<b>Textová část práce</b>	lepší	OK	horší	nevyh.
Formální úprava		X		
Struktura textu		X	X	
Analýza		X	X	
Vývojová dokumentace		X	X	
Uživatelská dokumentace		X		

Úvod práce rekapituluje technologie používané ve webových aplikacích.

Poté se rozebírají jednotlivé zdroje bezpečnostních problémů. Jednak ty běžné, jako jsou SQL injection, cross-site scripting a cross-site request forgery. Ale také méně známé útoky založené na vlastnostech Unicode. Vždy je vysvětleno technické pozadí, princip útoku a obvyklé způsoby prevence.

Poslední část práce popisuje demonstrační aplikaci. Její dokumentace je velmi stručná, uvítal bych více detailů.

Práci bych obecně vytkl, že se zabývá zejména těmi nejběžnějšími útoky a v džungli bezpečnostních aspektů webu prochází pouze po okraji. Téma by si zasloužilo důkladnější zpracování.

Na druhou stranu fakt, že základní útoky jsou proti mnoha webovým aplikacím stále úspěšné, potvrzuje, že se jimi stále je potřeba zabývat.

Po formální stránce je práce v pořádku, drobné jazykové a typografické chyby nejsou na újmu srozumitelnosti. Použité zdroje jsou korektně citovány.

<b>Implementační část práce</b>	lepší	OK	horší	nevyh.
Kvalita návrhu		X		
Kvalita zpracování		X		
Stabilita implementace		X		

Rozsah i zpracování demonstrační aplikace jsou adekvátní.

Aplikace obsahuje velké množství bezpečnostních chyb, což je v tomto případě cílem.

**Celkové hodnocení:** velmi dobře

**Práci navrhuji na zvláštní ocenění:** ne

V Praze dne 24. srpna 2023  
Martin Mareš