Katedra informatiky

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH, PEDAGOGICKÁ FAKULTA

KATEDRA INFORMATIKY

POSUDEK KVALIFIKAČNÍ PRÁCE

posudek oponenta **bakalářské práce**

Autor: **Martin Svatoš**

Název práce: **Hesla zadávána hackery při pokusu o průnik do systému**

Studijní obor: Informační technologie a e-learning

Datum odevzdání: 30.6.2022

Posudek vyhotovil: RNDr. Hana Havelková

Aktuálnost tématu:	A
Cíl práce a jeho naplnění:	B
Metodologická stránka práce:	B
Orientace v odborné literatuře:	C
Úroveň zpracování obsahu a interpretace výsledků:	C
Přínosy a aplikovatelnost v praxi:	C
Jazyková, formální a grafická úroveň práce:	C

Vlastní přínos autora:

Práce se zabývá problematikou pokusů o průnik na web Bobříka informatiky.
V teoretické části autor zmiňuje systém Joomla!, v němž je web Bobříka realizován, provádí klasifikaci kybernetických hrozeb a též softwaru využívaném hackery.
Uvádí potenciální dopady bezpečnostních incidentů, bezpečnost a uložení hesel, představuje možnosti přenosu dat mezi klientem a serverem.
Přínosem bakalářské práce je praktická část – autor vytvořil 3 moduly, jejichž prostřednictvím je možné sledovat a evidovat přihlašovací pokusy ve speciální tabulce bobří databáze. Na základě nasbíraných dat pak autor provádí dle jím stanoveného postupu klasifikaci uživatelů: snaží se rozlišit, zda se jedná o hackera či nikoliv, provádí jednoduchou statistickou analýzu uživatelských jmen a hesel z vyčištěných dat neúspěšných přihlašovacích pokusů.

Hlavní nedostatky práce:

Hlavním a zásadním nedostatkem práce je především její text, který obsahuje řadu pravopisných, syntaktických i sémantických chyb, nesrozumitelných a občas nesmyslných stylistických obratů, díky nimž je značně problematické se v práci orientovat, případný nezasvěcený čtenář se v textu může ztratit či nemá chuť ve čtení dále pokračovat.

Tyto chyby se projevují hned v prvním řádku úvodu a v úvodním odstavci.
V kapitole *1 Cíl práce* autor uvádí nejen cíl, ale i skutečnou realizaci práce a zmiňuje přínos práce: „získali jsme kompletní přehled zadávaných hesel a jmen, popřípadě jaké typy útoků se používají…“, což není úplně pravda.
Kapitola *2 Redakční systém Joomla!* je poněkud chaotickým seznamem podkapitol uvádějících vybrané rysy a komponenty zmíněného systému, přičemž není jasné, proč autor popisuje to, co popisuje.
V této kapitole i v pozdějším textu autor opakovaně uvádí chybnou formulaci „dotaz na zdroj dat“, což může vést k domněnce, že se ptáme, kde jsou data uložena, nikoliv že se snažíme provést s daty nějakou operaci.
A kde jsou data uložena, to autor vlastně nezmiňuje přímo, nýbrž v podkapitole *2.2.2 Tabulky a dotazy* rovnou upozorňuje na „řetězení dotazů“.
Kapitola *2.3 Umístění kódu zadané problematiky* nevysvětluje, o jaký kód a problematiku se jedná, a obě její podkapitoly mají natolik podivnou formulaci, že vyžadují opakované čtení.
Název kapitoly *6 Bezpečnost proti hackerům* se jeví trochu nešťastný, měl by znít spíše obrana či jak se bránit…
V textu je opakovaně chybně použit pojem iniciace (zasvěcení) namísto inicializace (nastavení výchozí hodnoty).

Praktická část práce je tvořena třemi moduly, z nichž dva řeší stejnou funkcionalitu, a to přihlášení do systému – v jednom případě jako admin, v druhém jako uživatel, v podstatě by stačil vhodně napsaný modul jediný.
Kapitola *9 Základní analýza programu* příliš analýzu neprovádí, autor pouze zmiňuje nutnost úpravy existujících přihlašovacích modulů a vytvoření modulu pro čištění záznamů, přičemž databázovou tabulku, do níž se data ukládají, blíže nepředstavuje.
Vývojový diagram na obr. 5 v kapitole 10 není správný – v podmíněném bloku testujícím počet pokusů chybí „záporná“ větev, kladná větev končí do ztracena, spojnice vycházející z bloku Start je podivně ohodnocena jako „ne“.
Autor zmiňuje nutnost vytvoření šifrovaných proměnných, což jsou ale obyčejné proměnné, do nichž se ukládá obsah zašifrovaný pomocí algoritmu Base64. To sice zajistí nečitelnost uživatelských jmen (kvůli GDPR) a hesel, nicméně tato data jdou dekódovat, což pak autor pomocí VB kódu provádí, takže je kdokoliv s přístupem do databáze může zpětně zjistit.
V kódu se opakovaně vyskytují tytéž přímé nepojmenované konstanty (např. v podmínkách) – tyto konstanty by měly být pojmenovány, event. uloženy v nějakém ini souboru.
V textu autor uvádí občas jiné pojmenování proměnných než ve zdrojovém kódu, pojmenování proměnných je nekonzistentní – např. proměnná $dateWithFiveHours obsahuje čas posledního přihlášení zvýšený o 30 minut.
Zdrojový kód je nepřehledný – např. metoda login obsahuje 395 řádků a délka kladné větve podmínky testující úspěšné přihlášení činí 225 řádků.
Z první věty kapitoly *13.5 Bonusový záznam* není jasné, proč jde vlastně o bonus.
Z výkladu v kapitole *14. 2 Hackeři v záznamech utočí i na cizí servery* není zřejmé, jak k tomuto tvrzení autor došel.

Otázky pro obhajobu a náměty do diskuze:

Jak jste dospěl k hodnotám konstant ovlivňujících klasifikaci potenciálních hackerů:
Proč je limit počtu neúspěšných přihlašovacích pokusů, po jehož překročení je uživatel klasifikován jako „hacker“ stanoven právě na 9?
Proč je používáte právě 15minutový interval od posledního přihlašovacího pokusu zabraňující výmazu příslušného záznamu při automatickém čištění databáze?

Práci doporučuji k ústní obhajobě.

Navrhuji hodnocení stupněm: C dobře

Místo, datum: České Budějovice, 10.8.2022

. . . . . .

Vysvětlivky:

A – vysoká úroveň (precizní teoretická část, kvalitní rešerše, bohatá a správně citovaná literatura, bez chyb psaní, výstižné formulace, kvalitní grafika, velký rozsah prací, velice inovativní práce, správná volba metody výzkumu, kvalitně zpracované výsledky výzkumu)

B – standard (teoretická část bez chyb, správně a přesně popsán cíl a metoda práce, průměrná odborná úroveň, standardní rozsah práce, s málo překlepy, vzhledem k rozsahu přiměřený počet drobných chyb, správné popisy v grafech, nepřesné citace v textu, chudší literatura – použití převážně 1- 2 zdrojů)

C – slabší úroveň (cíle a metody popsány nepřesně nebo neodpovídají realitě práce, menší rozsah práce, nepřesná terminologie, chybějící vysvětlení hlavních pojmů, malý rozsah práce, nepříliš inovativní a nosné, nedostatečné zdroje, použití převážně jednoho hlavního zdroje, chudá literatura, četné překlepy a slabší grafická úroveň, větší množství méně podstatných chyb, nejasná metoda a analýza výzkumu)

N – nevyhovující (chybějící nebo velmi stručné a formální popsání cílů a metod, malý rozsah práce, částečně opsáno v teoretické části, slabá terminologie, není patrný vlastní přínos, slabá úroveň vyjadřování, nejasné používané pojmy, malý rozsah praktické složky práce, závažné chyby ve výzkumu, nevyhovující grafická úroveň, mnoho hrubých chyb a překlepů, odbyté)