Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Adam Mirre** **Oponent:** **Ing. Jaromír Švejda, Ph.D.**

Studijní program: **Informační technologie**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2022/2023**

Téma diplomové práce: **Nástroj pro monitoring kompromitace hesel**

Hodnocení práce:
Diplomová práce se zabývá vývojem nástroje pro monitoring kompromitace hesel. Práce je psána v anglickém jazyce. Sporadicky se v ní vyskytují překlepy.
V teoretické části mohl diplomant více citovat použité zdroje. Text je psán vhodně a srozumitelně, jen se občas nemohu ubránit dojmu, že má autor tendenci občas odbíhat od tématu.
V praktické části jsou popsány všechny aspekty vývoje zmíněného nástroje. Obrázek *Figure 10.1.* by si v textu zasloužil nějaký komentář, nikoliv jej jen tak uvést na začátku kapitoly 10 bez jakékoliv následné zmínky v textu. Na str. 39 je spousta prázdného místa, nebylo nutné mezi tabulkami dávat tak velkou mezeru. Obsahově je popis opět srozumitelný a je z něj pochopitelné, jak náročný je vytvořený praktický výstup.
Samotný nástroj působí dost minimalisticky. Sám o sobě umožňuje vytvořit si uživatelský účet a následné přihlášení. Účet poté umožňuje provádět jednoduché akce v závislosti na tom, jakou roli účet má (Admin/User). Admin může spravovat uživatelské účty aplikace a nastavení API klíčů pro zdroje monitoringu kompromitace hesel. Ty jsou v aplikaci aktuálně dva. User má pak v podstatě jedinou funkcionalitu a tou je vyhledávání, zda došlo ke kompromitaci. Během testování aplikace se objevily problémy např. s odhlášením User účtu, kdy po stisku tlačítka „lougout“ nedošlo k žádné akci. Funkcionalita však byla funkční v prohlížeči Firefox. Z toho lze usoudit, že autor zřejmě nevěnoval dostatečný prostor testování své aplikace napříč aktuálně používanými prohlížeči. Dále se objevil problém ve vytváření účtu s tím, že pokud admin vytvoří účet uživatele s příliš krátkým heslem, tak se k danému účtu nelze prakticky už nikdy přihlásit, neboť takový účet neprojde přes validaci přihlašovacího formuláře – bylo by vhodné již při vytváření účtu od admina vyžadovat dodržení minimální délky hesla, aby k těmto problémům nedocházelo. Dále při prvním přihlášení je u user účtu vyžadována změna hesla. To je v pořádku, nepřipadá mi však vhodné nové heslo zadávat do textového pole, kde je heslo prakticky celé odhalené (nikoliv schované do hvězdiček, jak je běžné) až do potvrzení.
Nelze také opomenout grafickou podobu aplikace. Chápu, že se nejedná o stěžejní výstup práce, přesto na mě výsledné GUI působí poměrně nedotaženě. Celkově je na práci poznat, že některým částem aplikace mohl diplomant věnovat větší pozornost.
Práce ve výsledku splňuje body zadání, nicméně výše uvedené nedostatky v praktické části výrazně snižují kvalitu celkového výstupu.

Dotazy k obhajobě:
1. Jak prakticky probíhá online správa vlastní databáze kompromitovaných loginů?
2. V kterých prohlížečích jste prováděl testování Vaší aplikace?

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

D - uspokojivě.

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

Datum 4. 9. 2023 Podpis oponenta diplomové práce