МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

ЗВІТ

з виконання лабораторної роботи №1

з дисципліни «Захист інформації»

за темою «Аудит власної цифрової безпеки»

Виконала:

Студентка 4 курсу

групи 6.04.122.010.22.1

факультету ІТ

Халіна Ольга Дмитріївна

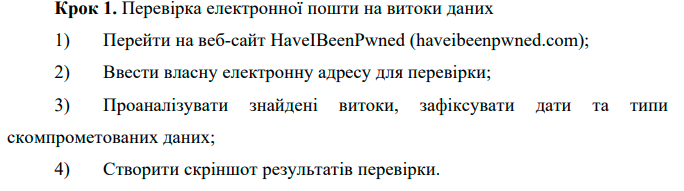
Перевірив:

Доцент кафедри кібербезпеки та ІТ

Тютюник Вадим Володимирович

Харків – 2025

**Мета роботи:** Проаналізувати власні ризики цифрової безпеки та навчитися оцінювати рівень захищеності особистих даних.



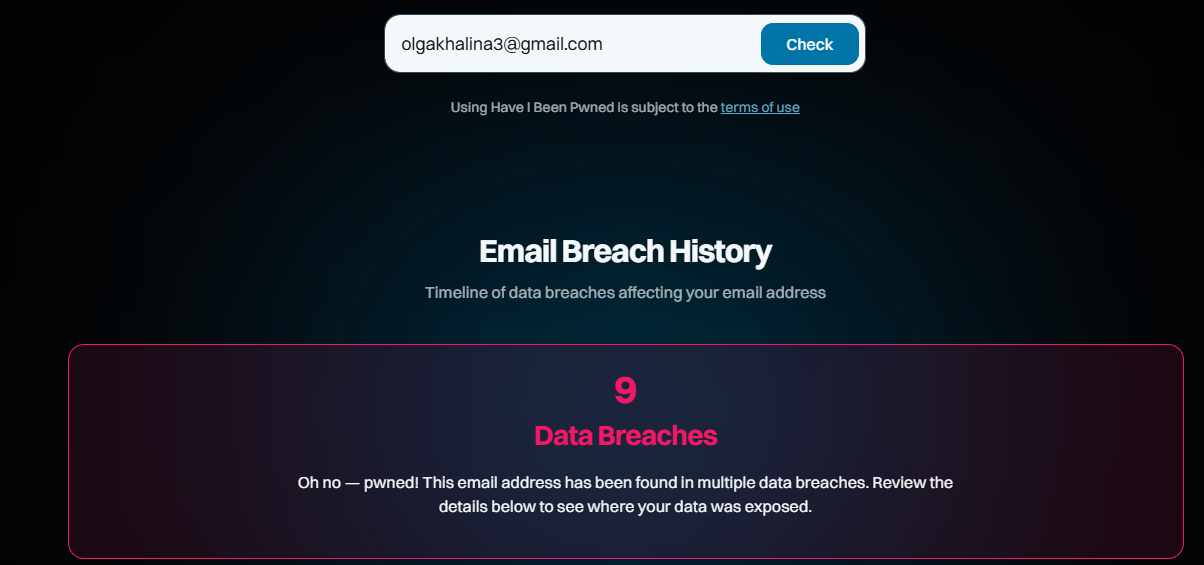


Рис. 1. Основна електронна адреса

Було знайдено 9 витоків даних, нижче приведено декілька прикладів, більш детально я описала в табл. 1.

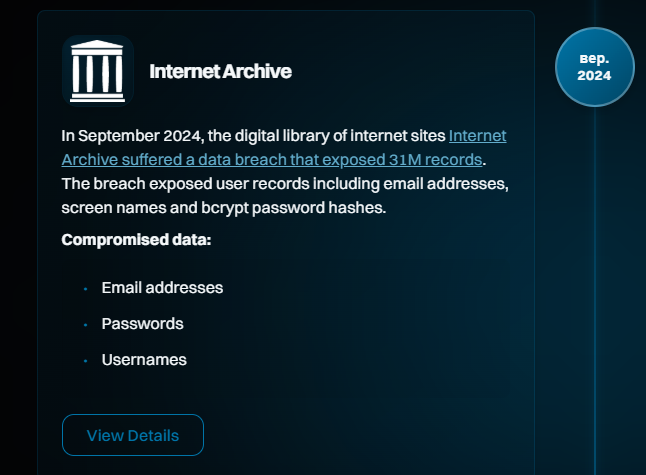


Рис. 2. Виток даних Internet Archive

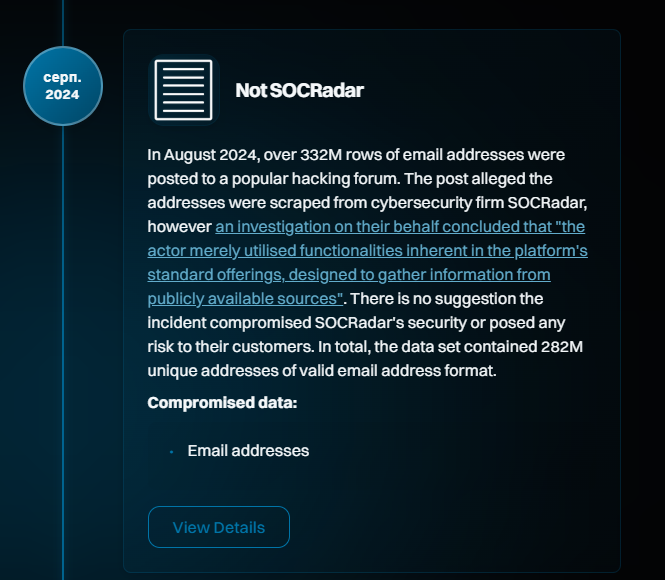


Рис. 3. Виток даних Not SOCRadar

Таблиця 1

Аналіз витоків даних

|  |  |  |  |
| --- | --- | --- | --- |
| № | Сервіс | Дата інциденту | Скомпрометовані дані |
| 1 | R2 (2017 forum breach) | Початок 2017 | Email, Імена користувачів, Паролі, Активність |
| 2 | EyeEm | Лютий 2018 | Email, Імена, Імена користувачів, Паролі, Біографії |
| 3 | Animoto | Липень 2018 | Email, Імена, Географічне розташування, Паролі, Дати народження |
| 4 | Canva | Травень 2019 | Email, Імена, Географічне розташування, Паролі, Імена користувачів |
| 5 | Deezer | Квітень 2019 (витік даних 2019 року, розкрито 2022 року) | Email, Імена, Географічне розташування, IP-адреси, Дати народження, Стать, Імена користувачів |
| 6 | Wattpad | Червень 2020 | Email, Імена, Географічне розташування, IP-адреси, Паролі, Дати народження, Соціальні профілі |
| 7 | Twitter (200M) | Початок 2023 (дані отримані у 2021) | Email, Імена, Імена користувачів, Соціальні профілі |
| 8 | Not SOCRadar | Серпень 2024 | Email |
| 9 | Internet Archive | Вересень 2024 | Email, Імена користувачів, Паролі |

Аналіз виявив, що облікові дані були скомпрометовані у 9 різних сервісах, що охоплюють період з 2017 по 2024 рік. Встановлено, що 6 з 9 інцидентів призвели до витоку хешів паролів. Сукупність викрадених даних (дати народження, стать, IP-адреси, імена) надає зловмисникам достатньо інформації для проведення високоперсоналізованих (цільових) фішингових атак.

Інша електронна адреса не була скомпрометована, що підтверджено на рис. 4.

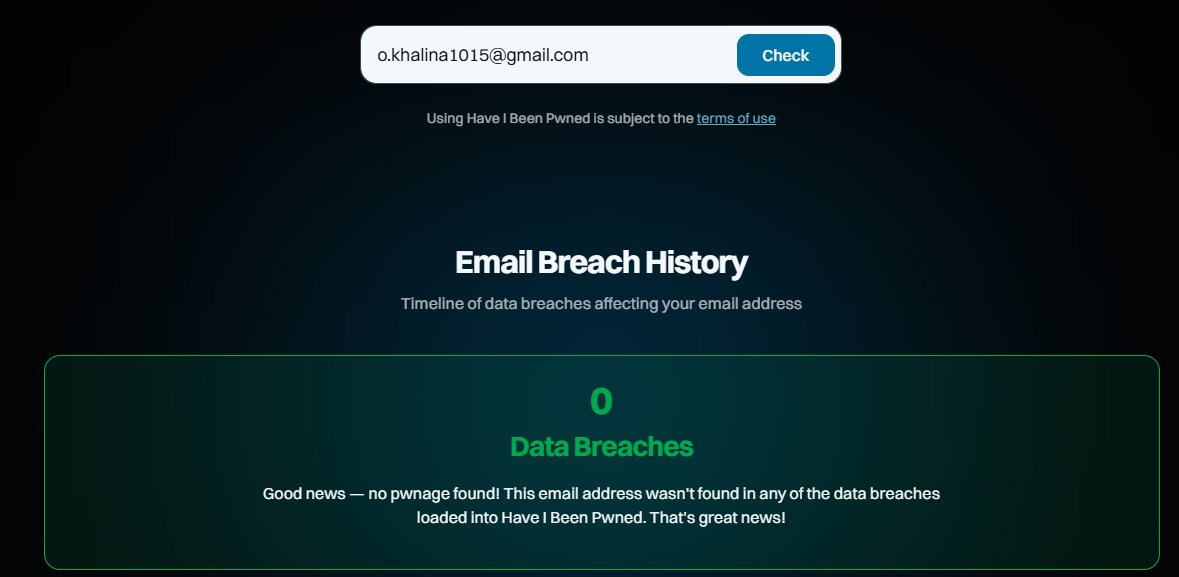
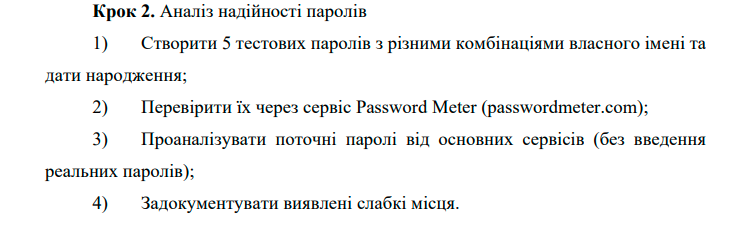


Рис. 4. Друга електронна адреса



Придумані паролі:

1. KhalinaOlha10052005
2. Olha2005!10May
3. KOlha\_10.05.05
4. Khalina1005
5. Olhakhal

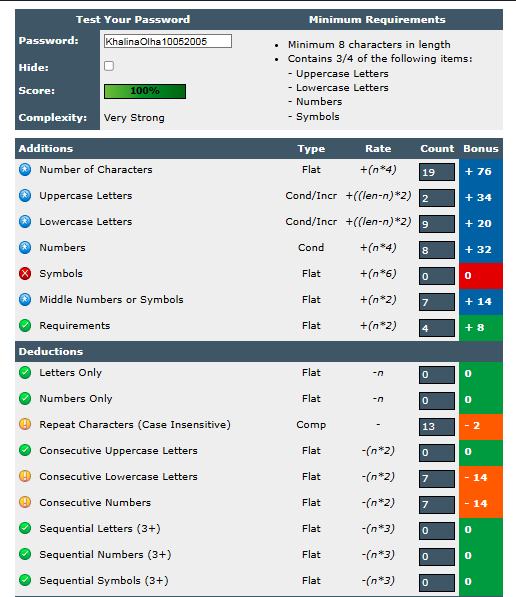


Рис. 5. Аналіз пароля KhalinaOlha10052005



Рис. 6. Аналіз пароля Olha2005!10May

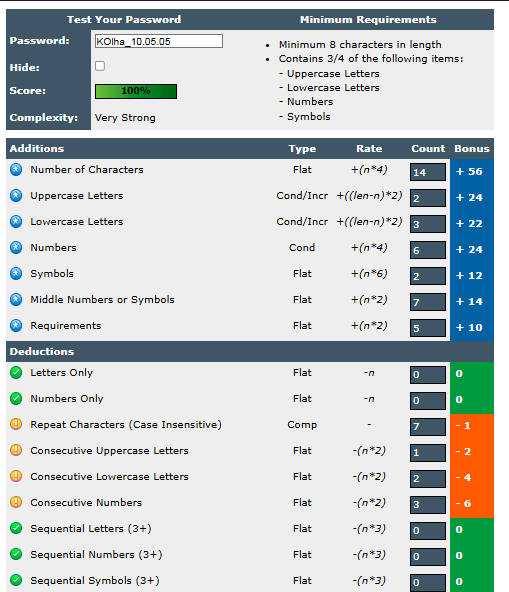


Рис. 7. Аналіз пароля KOlha\_10.05.05

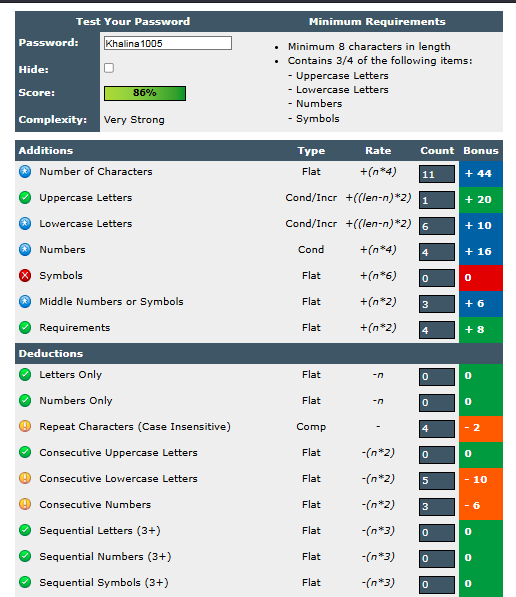


Рис. 8. Аналіз пароля Khalina1005

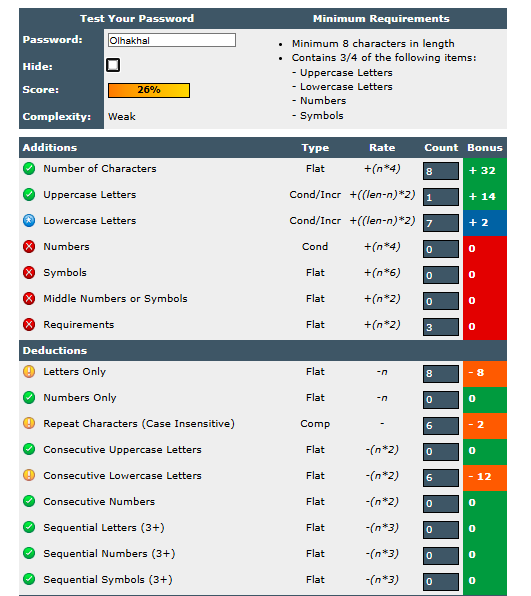


Рис. 9. Аналіз пароля Olhakhal

Перші три паролі виявились доволі потужними, інші два − навпаки. Пароль Olhakhal доволі легко зламати, бо він має мінімальну кількість символів та це тільки літери. Пароль Khalina1005 вже не так легко зламати, але не вистачає спеціальних символів. Пароль KhalinaOlha10052005 достатньо складний, але відсутність спеціальних символів спрощує шлях до зламу.

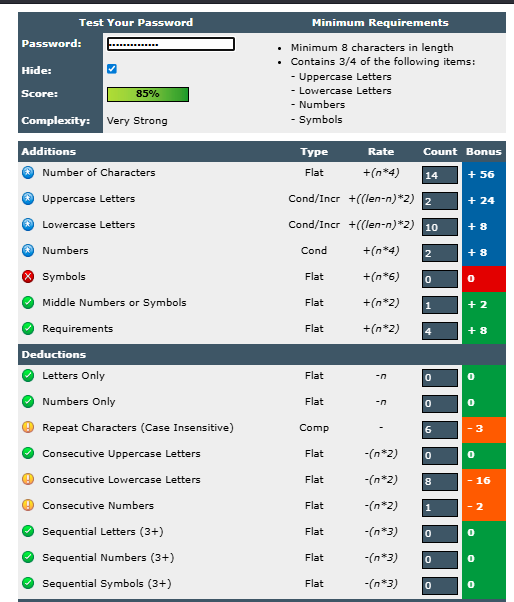
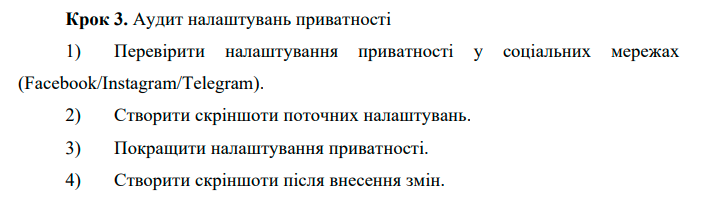


Рис. 10. Перевірка паролю від пнс

Пароль від пнс є достатньо сильним, але хтось все-таки може викрасти мої звіти, тому потрібно додати ще символів.



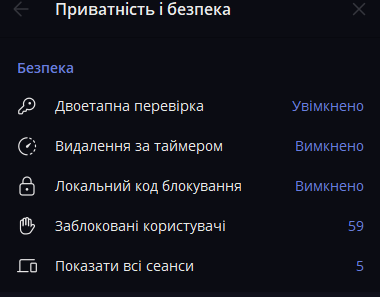


Рис. 11. Налаштування безпеки в Telegram

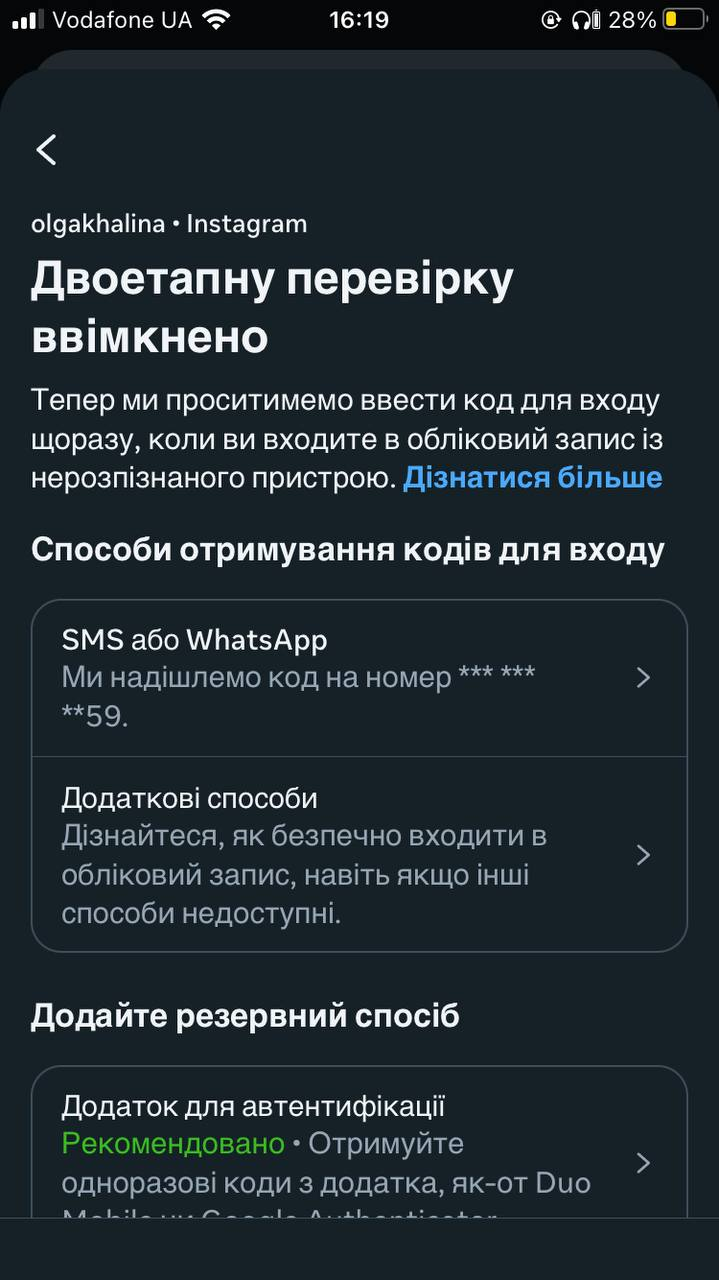
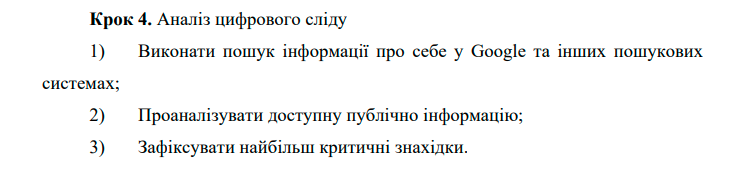


Рис. 12. Налаштування двоетапної перевірки в Instagram

Як можна побачити, то налаштування безпеки мають захистити мій обліковий запис від зламів за рахунок двоетапної перевірки.



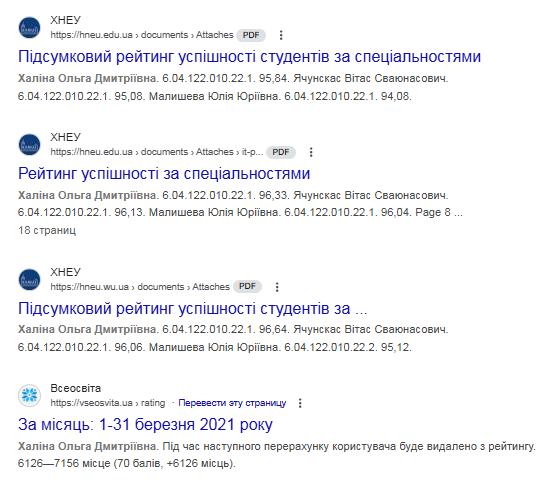


Рис. 13. Знайдені дані

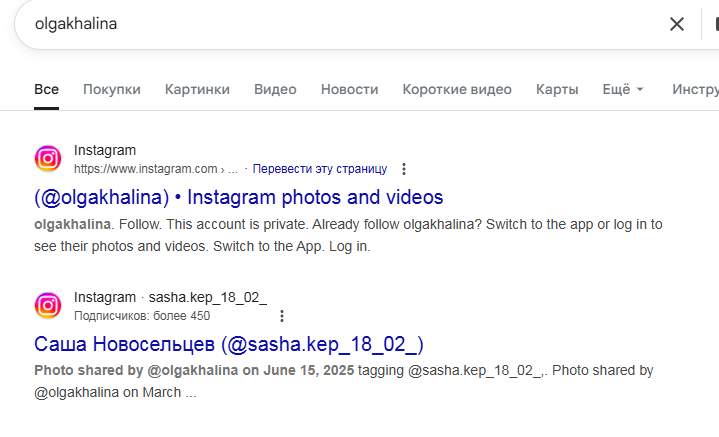
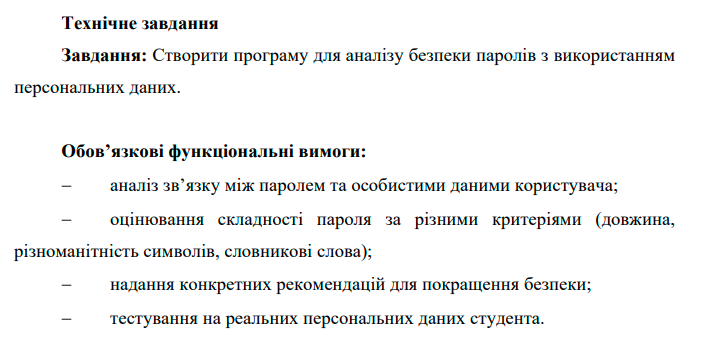


Рис. 14. Результати пошукових запитів

Загалом, якщо шукати тільки моє ім’я та прізвище, то існує багато людей з такою комбінацією. Проте якщо шукати повністю ПІБ, то можна знайти лише дані про моє навчання.



Посилання на GitHub: <https://github.com/olhakhalina33/cybersecurity-labs-khalina/tree/main/lab01>

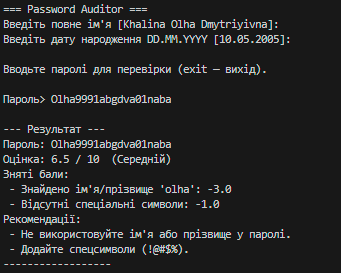


Рис. 15. Приклад використання програми

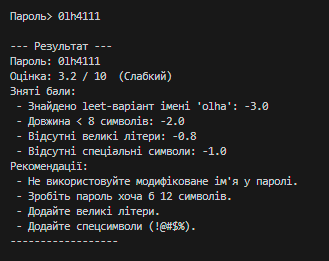


Рис. 16. Приклад використання програми

Створене рішення представляє собою консольну програму для оцінки безпеки паролів з урахуванням персональних даних користувача − імені та дати народження. Програма аналізує пароль на наявність частин імені або прізвища (у звичайному та leet-варіанті), дату народження, довжину, різноманітність символів, популярні словникові слова та прості послідовності, після чого нараховує або знімає бали та формує підсумкову оцінку від “Дуже слабкий” до “Надійний” з детальними причинами зняття балів і практичними рекомендаціями для покращення пароля.

**Висновки:** У ході лабораторної роботи я проаналізувала власні ризики цифрової безпеки та навчилася оцінювати рівень захищеності особистих даних.