УНІВЕРСИТЕТ ІМЕНІ АЛЬФРЕДА НОБЕЛЯ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему

«Розробка сайту для координації брутфорс-атак для кількох учасників»

Виконав: здобувач 4 курсу, групи КН-19-2
Спеціальності 122 Комп’ютерні науки
Шляхов О.В.
Керівник: Бабкін В.В., к.т.н.

м. Дніпро
2023

ЗМІСТ

АНОТАЦІЯ

Ця кваліфікаційна робота присвячена розробці веб-сайту для координації брутфорс-атак між кількома учасниками. У нашому дослідженні ми охоплюємо як історичні, так і сучасні алгоритми шифрування, що використовуються для збереження паролів, включаючи md5, sha1, sha256, bcrypt та argon2id. Ми також розглядаємо інші алгоритми, які використовуються в різних контекстах, таких як NTLM, sha512crypt та apr1.

Основна проблема, що стоїть перед нами, полягає в розробці системи, яка б дозволила групі осіб координувати свої зусилля при брутфорс-атаках, обмінюватися результатами і даними в уніфікованому форматі, а також вести обговорення і планування.

Ця проблема має важливе значення, оскільки сучасні рішення, такі як Hashtopolis, хоча і дозволяють розподіляти завдання брутфорс-атаки, але не надають достатньо інструментів для ефективної координації дій між учасниками групи.

Ми проводимо аналіз потреб користувачів, вивчаємо можливості та обмеження існуючих систем та пропонуємо нове рішення, спрямоване на задоволення цих потреб. Питання безпеки, приватності та ефективності є в центрі нашого дослідження.

Результатом нашої роботи є проект веб-сайту, що дозволяє групі користувачів координувати свої зусилля для брутфорс-атак, обмінюватися результатами в уніфікованому форматі та обговорювати стратегії. Ми вважаємо, що це нове рішення може значно полегшити процес брутфорс-атаки для групи користувачів та покращити їх результативність. Ключові слова: Брутфорс-атака, координація, груповий подбір паролів, веб-сайт, хешування, md5, sha1, sha256, bcrypt, argon2id, NTLM, sha512crypt, apr1, безпека, приватність, ефективність, Hashtopolis, Node.js, Vue.js, MongoDB.