УДК 004.056
Корольков Р.Ю.[1], Рева В.І.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ GOOGLE DORKING/HACKING ДЛЯ ПОКРАЩЕННЯ СТРАТЕГІЙ ЗАХИСТУ

Використання операторів розширеного пошуку пошукової системи Google відомо як "Google Dorking/Hacking". Ця техніка дозволяє знаходити конфіденційні дані та вразливі веб-сайти без необхідності використання спеціалізованих програмних інструментів. До операторів розширеного пошуку відносяться cache, link, related, info, define, stocks, site, allintitle, intitle, allinurl, inurl та ін. Деякі з них можуть надати цінну інформацію для зловмисників. У більшості випадків зловмисники можуть шукати каталоги для перегляду, конфіденційну інформацію, таку як імена користувачів, паролі, журнали помилок, архіви резервних копій та ін [1].

Наприклад, "filetype:sql intext:username password" – запит який зловмисники можуть використовувати для пошуку файлів баз даних зі словами "username" і "password" в тексті. Запит "filetype:xlsx email" дозволить знайти файли Excel, які містять адреси електронної пошти. Зловмисники можуть використовувати його для пошуку списків розсилки або баз даних з контактами. "site:example.com inurl:admin" – це запит, який зловмисники можуть використовувати для пошуку панелей адміністратора, які не захищені паролем. Запит "intitle:"index of" знайде веб-сторінки, які містять фразу "index of" і часто відображають список всіх файлів, які знаходяться в певній директорії на веб-сервері. Зловмисники можуть використовувати їх для пошуку конфіденційних файлів, які не повинні бути доступні публічно.

"ip:192.168.1.0/24" - цей запит зловмисники можуть використовувати для сканування локальних мереж з метою пошуку вразливих пристроїв, та ін.

Всі ці ризики виникають внаслідок небезпечної конфігурації сервера. Тисячі веб-сайтів знаходяться під загрозою через базові помилки в налаштуванні безпеки, а деякі сервери навіть дозволяють необмежений доступ до файлових каталогів.

Сьогодні існує велика база даних пошукових запитів Google Hacking Database (GHDB), яка була зібрана та опублікована спільнотою експертів з кібербезпеки та ентузіастами [2]. GHDB містить близько 8000 різноманітних пошукових запитів для Google і оновлюється майже щодня новими запитами, які дозволяють виявляти різні вразливості, конфіденційну інформацію та інші цікаві ресурси в мережі Інтернет.

Важливо відзначити, що техніку розширених пошукових запитів можна застосовувати не тільки в Google, але й в інших пошукових системах. Будь-яка пошукова система, така як Bing, Yahoo та DuckDuckGo, може прийняти пошуковий запит та повернути відповідні результати. Однак, навіть якщо дві пошукові системи підтримують однакові оператори, вони часто повертають різні результати пошуку через різницю в індексації кожної пошукової системи.

Техніка Google Hacking може допомогти досліднику безпеки знайти кращі способи зробити веб-сайт більш безпечним, оскільки дуже важливо перевіряти конфігурацію сервера та вживати всіх необхідних заходів для захисту файлів і даних.

Для запобігання індексації конфіденційної інформації пошуковими системами рекомендується: захистити приватні зони за допомогою автентифікації користувачів та паролів, а також за допомогою обмеження за IP-адресами; шифрувати конфіденційну інформацію, таку як дані користувачів, паролі, номери кредитних карток, електронні листи, адреси, IP-адреси, номери телефонів тощо; регулярно проводити сканування вразливостей сайту, використовуючи популярні запити Google Dorks з бази даних Exploit DB Dorks [2], що можуть ефективно виявляти найбільш поширені вразливості; застосовувати блокування конфіденційного контенту за допомогою файлу robots.txt, розташованого в кореневому каталозі веб-сайту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Messier R. CEH V12 Certified Ethical Hacker Study Guide. – John Wiley & Sons, Incorporated, 2023. – 768 p.

2. База даних OffSec Exploit Database Archive. Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers – https://www.exploit-db.com/