НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

Список використанних джерел:

1. Zyskind G., Nathan O., Pentland A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, 2015. URL: https://ieeexplore.ieee.org/document/7163223
2. Conti M., Dehghantanha A., Franke K., Watson S. Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications. IEEE Communications Surveys & Tutorials, 2018. URL: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9739
3. Kshetri N. 1 Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. Telecommunications Policy, 2017. URL: https://www.sciencedirect.com/science/article/abs/pii/S0308596117302483
4. Бойко В., Василенко М., Слатвінська В. *Моделювання живучості та відновлення інформаційно-комунікаційних мереж в умовах дії кіберзагроз.* Інформаційні технології та суспільство, 2024, №1 (12), с. 13–19. URL: https://journals.maup.com.ua/index.php/it/article/view/3143
5. Lihua Song, Zongke Zhu, Menghen Li, Li Ma, Xinran Ju. A Novel Access Control for Internet of Things Based on Blockchain Smart Contract. IEEE Access, 2021. URL: https://ieeexplore.ieee.org/document/9390662
6. GDPR-Compliant Use of Blockchain for Secure Usage Logs – Zieglmeier V., Loyola Daiqui G, 2021. URL: https://arxiv.org/abs/2104.09971?utm_source=chatgpt.com

Ключові слова: блокчейн, журналювання, цілісність логів, система виявлення вторгнень, Hyperledger Fabric, SHA-512, цифрові докази, незмінність даних, криптографічний хеш-ланцюг.

Keywords: blockchain, logging, log integrity, intrusion detection system (IDS), Hyperledger Fabric, SHA-512, digital evidence, data immutability, cryptographic hash chain.

ПРОВЕДЕННЯ SQL-ІН'ЄКЦІЇ З ВИКОРИСТАННЯМ SQLMAP

Клевець Михайло

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

SQL-ін'єкції – одна з найстаріших та одночасно найефективніших технік компрометації вебзастосунків: при вдалому використанні вони дозволяють читати, змінювати або видаляти дані, отримувати облікові дані, а іноді й виконувати команди операційної системи.

Автоматизація атак (наприклад, із застосуванням SQLMap) значно знижує поріг входу для зловмисника і дозволяє за короткий час провести розвідку та екстракцію даних. Це робить регулярне тестування критично важливим для розробників і адміністраторів.

У даних тезах досліджуються методи проведення SQL-ін'єкцій та автоматизація таких атак із використанням утиліти SQLMap. З огляду на те,

що вебзастосунки широко використовують реляційні бази даних і SQL-запити, вразливості на рівні запитів залишаються критичною загрозою безпеці інформації.

Мета роботи – дослідити типи SQL-ін'єкцій, показати їх реалізацію у тестовому середовищі (DVWA), продемонструвати можливості SQLMap та розробити практичні заходи захисту.

У результаті проведеного дослідження узагальнено класифікацію систем керування базами даних (СКБД), зокрема реляційних, документних, ключ-значення, колонкових, графових і гібридних СКБД, та визначено їх характерні особливості з погляду безпеки. Встановлено, що реляційні СКБД (MySQL, PostgreSQL, MS SQL Server, Oracle, MariaDB, SQLite, IBM Db2) є найбільш поширеною основою сучасних вебзастосунків і водночас типовим середовищем виникнення SQL-уразливостей. На основі аналізу предметної області сформовано детальну класифікацію SQL-ін'єкцій, зокрема *in-band* (error-based, union-based), *blind* (boolean-based, time-based), *out-of-band*, *second-order* та NoSQL-ін'єкцій.

За результатами практичної частини підтверджено, що за наявності вразливих параметрів і відсутності належної обробки введених даних вебзастосунки з реляційною базою даних є вразливими до різних типів SQL-ін'єкцій, включаючи *blind* та *second-order* атаки. Експериментально встановлено можливість витягування структури бази даних і її вмісту (таблиць, стовпців і значень), що підтверджує критичний характер зазначених уразливостей у реальних сценаріях експлуатації.

У ході дослідження проаналізовано архітектуру та функціональні можливості інструмента SQLMap і встановлено його здатність автоматизовано виявляти SQL-уразливості з використанням різних технік (*boolean-based*, *time-based*, *union-based*, *error-based*, *stacked*, *out-of-band*), а також працювати з параметрами HTTP-запитів, cookie, заголовками та мережевими посередниками. Визначено набір ключових параметрів конфігурації SQLMap, застосування яких забезпечує гнучке керування процесом тестування та підвищує ефективність виявлення вразливостей.

Експериментальні результати підтвердили можливість автоматизованого отримання інформації про структуру бази даних (перелік баз даних, таблиць і стовпців), витягування вибраних даних, а також аналізу облікових даних, включно з отриманням і розпізнаванням хешів паролів у контрольованому середовищі. Окремо встановлено, що за наявності відповідних привілеїв SQLMap підтримує використання позасмугових каналів взаємодії та може забезпечувати виконання команд операційної системи.

В результаті вдалося підтвердити, що застосування автоматизованих інструментів істотно скорочує час розвідки та експлуатації SQL-уразливостей

порівняно з ручними методами, водночас підвищуючи повноту та відтворюваність результатів тестування.

Висновки. У результаті дослідження встановлено, що за відсутності захисних заходів SQL-ін'єкції дозволяють отримувати конфіденційні дані, порушувати цілісність та доступність інформації, а також здійснювати ескалацію привілеїв. Факторами, що підвищують ризик атак, є відсутність валідації та екранування введених даних, використання динамічних конкатенованих SQL-запитів, зайві права облікових записів баз даних, а також відсутність захисту на рівні мережі та журналювання. Обмеженням дослідження є те, що експерименти виконано у тестовому середовищі; результати є репрезентативними для подібних конфігурацій, проте у реальних системах фактори інфраструктури та політик доступу можуть впливати на прояви атак.

На основі отриманих результатів сформульовано рекомендації щодо захисту вебзастосунків, зокрема застосування параметризованих запитів (prepared statements) або ORM, валідацію та нормалізацію введених даних, обмеження прав облікових записів за принципом найменшого привілею, регулярне автоматизоване тестування з використанням таких інструментів, як SQLMap, а також впровадження систем виявлення вторгнень (IDS/IPS), логування та моніторинг аномалій у запитах. Доцільним є багаторівневий захист із використанням WAF, обмеженням частоти запитів та CAPTCHA на критичних формах.

Отримані рекомендації можуть бути безпосередньо впроваджені в процес розробки програмного забезпечення та політику інформаційної безпеки організації. Проведене дослідження підтверджує необхідність системного підходу до захисту вебзастосунків: поєднання безпечного коду, належного адміністрування баз даних та регулярного тестування є ключем до зниження ризиків, пов'язаних із SQL-ін'єкціями.

Список використаної літератури:

1. Nasereddin M. et al. A systematic review of detection and prevention techniques of SQL injection attacks. Information Security Journal: A Global Perspective. 2023. Vol. 32, No. 4. P. 252-265.
2. Subbulakshmi T. et al. SQL Injection Testing on Website using Sqlmap. International Conference on Trends in Quantum Computing and Emerging Business Technologies. IEEE, 2024. P. 1-4.

Ключові слова: SQL-ін'єкція, веб-безпека, реляційні бази даних, SQLMap, автоматизація атак, тестування вразливостей.
Keywords: SQL injection, web security, relational databases, SQLMap, attack automation, vulnerability testing.

ЗМІСТ