https://www.proconference.org/index.php/usc/article/view/usc34-00-028
DOI: 10.30888/2709-2267.2025-34-00-028

UDC 004.056.53:[004.7:004.032.26]

METHODOLOGY FOR LEARNING SQL INJECTIONS BASED ON A CREATED SOFTWARE APPLICATION FOR BIENDED LEARNING IN THE DISCIPLINE OF «DATABASES»

МЕТОДИКА ВИВЧЕННЯ SQL-ІН'ЄКЦІЙ НА ОСНОВІ СТВОРЕНОГО ПРОГРАМНОГО ЗАСТОСУНКУ ДЛЯ ЗМІШАНОГО НАВЧАННЯ З ДИСЦИПЛІНИ «БАЗИ ДАНИХ»

Pakhomova Victoria / Пахомова Вікторія
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0002-0022-099X
Ukrainian State University of Science and Technology: «Dnipro Institute of Infrastructure and Transport», Ukraine, Dnipro, Lazaryan St., 2, 49010
Український державний університет науки і технологій: «Дніпровський інститут інфраструктури і транспорту», Україна, Дніпро, вул. Лазаряна, 2, 49010
Vichev Daniyl / Вічев Даниїл
bachelor's degree holder / здобувач ступеня «бакалавр»
ORCID: 0009-0004-9204-7857
Ukrainian State University of Science and Technology: «Dnipro Institute of Infrastructure and Transport», Dnipro, Lazaryan, 2, 49010
Український державний університет науки і технологій: «Дніпровський інститут інфраструктури і транспорту», Україна, Дніпро, Лазаряна, 2, 49010

Abstract. *In blended learning for applicants for the bachelor's degree in the specialty «Cybersecurity and Information Protection» in the discipline «Databases», the «Blend DB SQLi» methodology is proposed, which involves: studying SQL injections; classifying SQL injections; the impact of SQL injections; methods for detecting and preventing SQL injections; reviewing control examples and performing an individual task according to the given option based on the use of the «SQL_Testing» software application created in Python: 1) INJECTION (SQL injection vulnerability, which allows obtaining hidden data); 2) AUTH (SQL injection vulnerability, which allows bypassing the system login); 3) LEAK (SQL injection vulnerability, which allows unauthorized data leakage); 4) EXAM (performing the task without using comments); preparing the applicant according to the list of questions; passing the test by the applicant.*

Key words: *SQL-injection; classic; blind; UNION-injection; obtaining hidden data; data validation; query parameterization; privilege restriction; ORM -framework.*

Анотація. *При змішаному навчанні для здобувачів ступеня «бакалавр» спеціальності «Кібербезпека та захист інформації» з дисципліни «Бази даних» запропоновано методику «Blend DB SQLi», що передбачає: вивчення SQL-ін'єкцій; класифікацію SQL-ін'єкцій; вплив SQL-ін'єкцій; методи виявлення та запобігання SQL-ін'єкцій; розгляд контрольних прикладів та виконання індивідуального завдання за виданим варіантом на основі використання створеного мовою Python програмного застосунку «SQL_Testing»: 1)INJECTION (вразливість SQL-ін'єкції, що дозволяє отримувати приховані дані); 2) AUTH (вразливість SQL-ін'єкції, що дозволяє обійти вхід до системи); 3) LEAK (вразливість SQL-ін'єкції, що дозволяє несанкціонований витік даних); 4) EXAM (виконання завдання без використання коментарів);*

підготовка здобувача відповідно до переліку запитань; проходження здобувачем тестування.
Ключові слова: *SQL-ін'єкція; класична; сліпа; UNION-ін'єкція; отримання прихованих даних; валідація даних; параметризація запитів; обмеження привілеїв; ORM-фреймворк.*

Introduction

Formulation of the problem. The current state of affairs in the world, associated with the constant spread of infectious diseases, the continuation of military events that threaten the lives of applicants, and prolonged emergency power outages after missile attacks, has led to the use of blended learning, in particular in the discipline of «Databases», as well as the formation of relevant professional and subject competencies, and the development of «Soft Skills» in applicants for the bachelor's degree in such difficult conditions of today, which confirms the relevance of the topic.

Analysis of the latest research. Competency assessment is the subject of research by many scientists [1]. At the present stage, it is important to compare Ukrainian education in international studies of the quality of education. The analysis of recent studies and publications revealed the following: 1) the absence of unified information and communication technologies for teaching the discipline «Databases»; 2) the existence of various types of SQL injections that have a significant negative impact on databases [4,5]; 3) the existence of means of detecting and preventing SQL injections [3,6]; 4) the existence of the features of generation Z; 5)the development of Soft Skills among applicants, and became the basis for the development of our own methodology «Blend_DB_SQLi».

The purpose of the work is to develop the «Blend_DB_SQLi» methodology for the formation of professional and subject competencies in applicants for the bachelor's degree in the specialty «Cybersecurity and Information Protection» in the study of SQL injections in the discipline «Databases» in blended learning.

General characteristics of the «Blend_DB_SQLi» methodology. In blended learning (combination of face-to-face and distance learning formats, use of ZOOM and LIDER systems [2], communication in social networks), the proposed methodology provides an opportunity for first-degree applicants in the specialty «Cybersecurity and Information Protection» in the discipline «Databases» to: gain an idea of SQL

injections, their classification, as well as their impact and detection methods; based on the created software application «SQL_Testing», analyze a control example of SQL injections and perform an individual task according to the option (20 options are provided), consisting of three parts; formulate an appropriate conclusion; prepare for defense (a suggested list of questions); pass testing.

1. Understanding SQL Injection and its Impact. SQL Injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. A successful SQLi attack can lead to unauthorized access to sensitive data: passwords; credit card details; personal user information [5]. Each type of SQL injection uses different methods to manipulate database queries, depending on what information can be obtained from the application.

2. Types of SQL injections. SQLi can be classified according to various criteria, including the way it interacts with the application and database, as well as the level of observability during the attack process [4].

1) *In-band SQL Injection*: occurs when SQL code is injected directly into queries, which can be done through web form input fields or URL parameters.

2) *Blind SQL Injection*: is based on the use of logical expressions in queries to determine the presence or absence of data in the database without displaying it on the screen. Example of an attack: *‘ OR 1=1; - - ‘*

3) *Error-based SQLi*: this type exploits database error messages that may contain sensitive information about the database structure or its contents.

4) *Time-based SQLi*: uses the delay in query execution to determine whether a certain condition is true or false. For example: *‘ SLEEP(5); - - ‘*

5) *Other types of SQLi*: such as UNION injections, Error-based injections, Out-of-band injections and many combined methods that can exploit various vulnerabilities and weaknesses in web applications to inject and execute malicious SQL code.

3. Methods for detecting and preventing SQL injections [4]:

1) Input sanitization: The first and one of the most effective methods for preventing attacks is to sanitize input data before it is used in SQL queries. This includes removing or escaping special characters such as single quotes (‘) and double

quotes (“), which can be used to inject malicious SQL code.

2) Use parameterized queries: Instead of directly concatenating user input with SQL queries, use parameterized queries that separate the data from the query itself. This helps prevent the possibility of SQL code injection because the input is processed as query parameters, not as part of the SQL code.

3) Use ORM (Object-Relational Mapping): ORM frameworks provide an abstraction of the database, which makes it safer to work with. They automatically generate and execute SQL queries, which reduces the likelihood of SQL injection. However, you should make sure that the ORM framework you use handles user input safely.

4) Secure programming and database configuration: When developing web applications, it is important to adhere to the principles of secure programming, namely: the principle of «least privilege» and proper database access management. In addition, an important step in securing web applications is to regularly check the site for SQL. It is necessary to regularly update and audit the database to minimize risks.

4. Using the created software application «SQL_Testing» in the educational process of the discipline «Databases». The program is written in the Python PyQt6 language to create a user interface, the menu of which is: 1.INJECTION (for executing the first part); 2.AUTH (for executing the second part); 3.LEAK (for executing the third part); 4.EXAM (without using comments).

The first part of the laboratory work: SQL injection vulnerability in the WHERE clause, which allows obtaining hidden data (Figure 1).

If we click «Search» and view the SYSTEM LOG, we will see what our SQL query looks like and which products are not «secret» (Figure 2).

This SQL query accesses the database to retrieve information about the corresponding products from the database, where *released=1* is used to hide products that have not yet been released. Let's try to create an attack using the truth condition: *Products' OR 1=1* -- Note that '--' is a comment indicator in SQL (this means that the rest of the query is interpreted as a comment, effectively deleting it). After execution, we get the product that was hidden and a secret FLAG, which is given to the lab report

as confirmation of its execution (Figure 3).

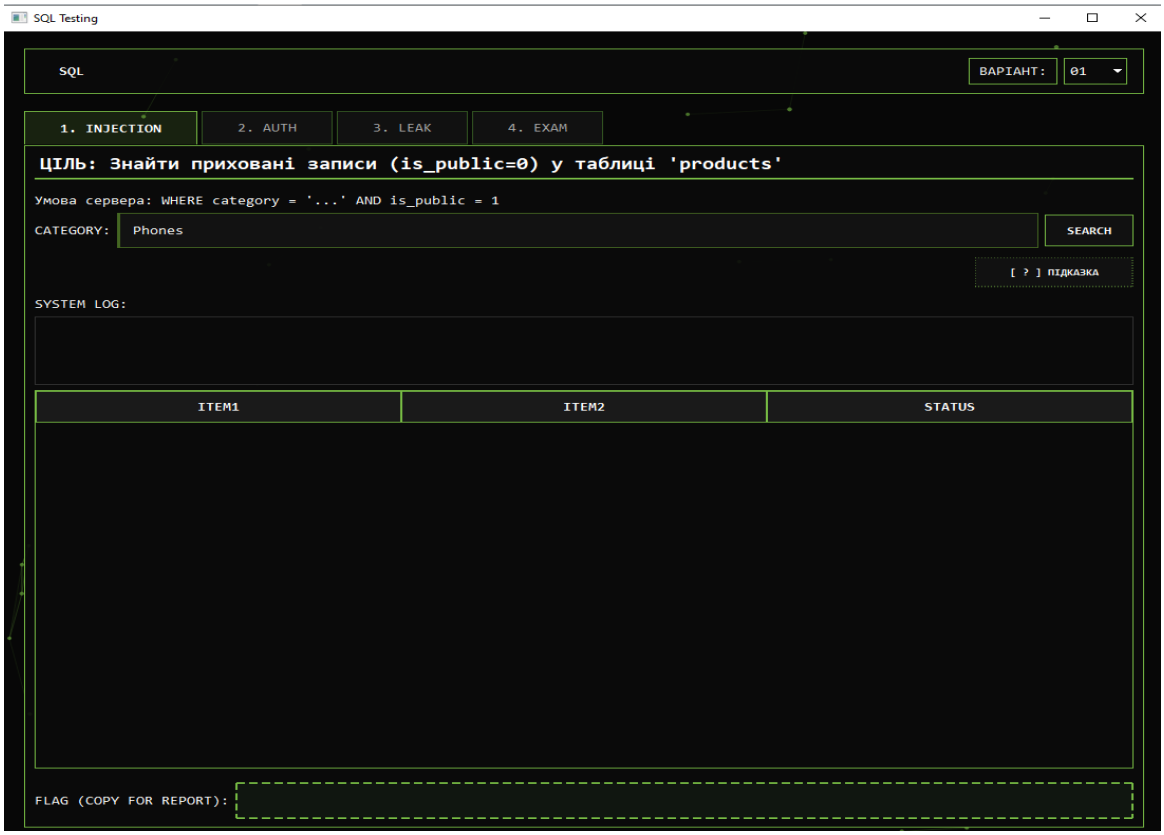

Figure 1 – «1. INJECTION»

Author's work

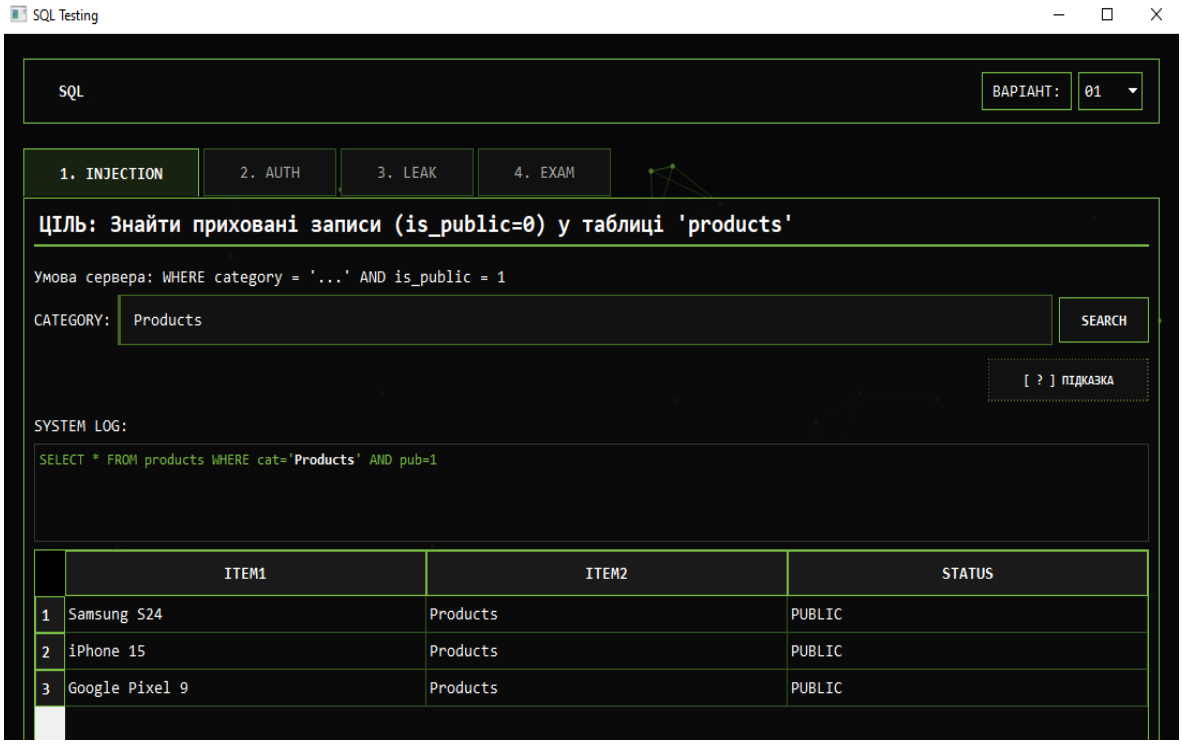

Figure 2 – «1. INJECTION»: after pressing SEARCH

Author's work

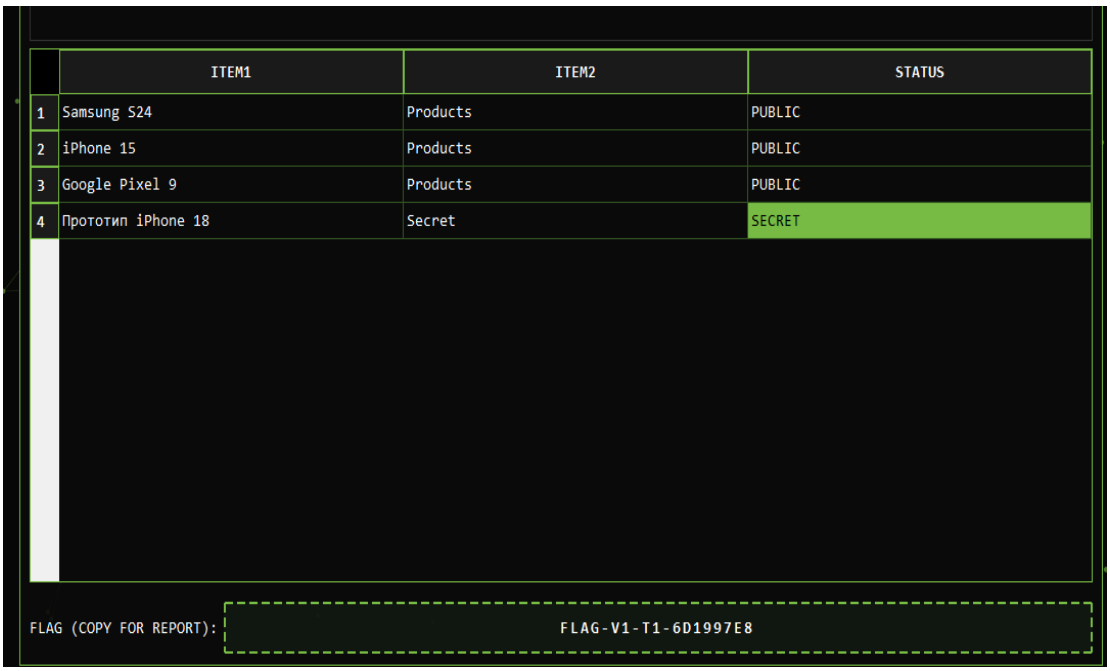

Figure 3 – «1. INJECTION»: successful «truth condition» attack

Author's work

***The second part of the laboratory work*:** SQLi vulnerability that allows you to bypass the login to the system. Click on the second part «2.AUTH» (Figure 4).

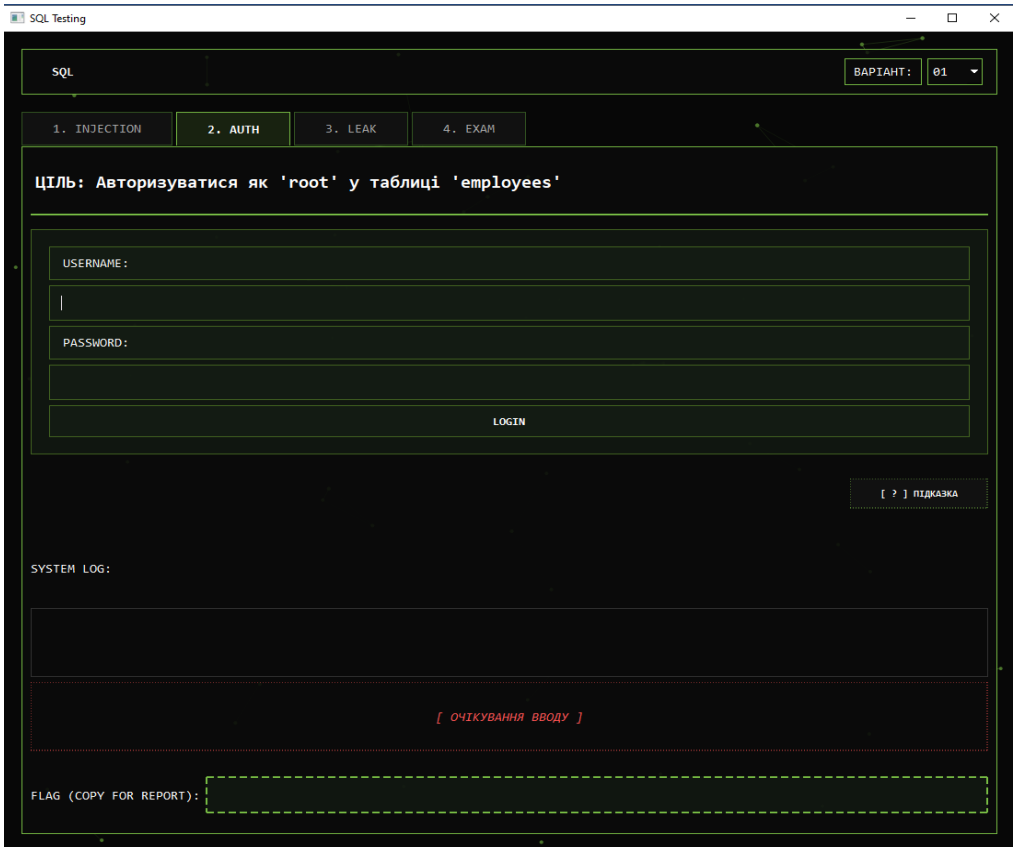

Figure 4 – «2. AUTH»

Author's work

Our goal is to log in to the system with the username root, but we don't know the correct password. We enter root in the «USERNAME» field and right-click on LOGIN, we get what the SQL query looks like:

*SELECT * FROM employees WHERE user='' ...*

We get information that first the system asks for a login, and then a password. Let's try to comment out the query after user: *root'--* The injection was successful, and we got access and a secret FLAG (Figure 5).

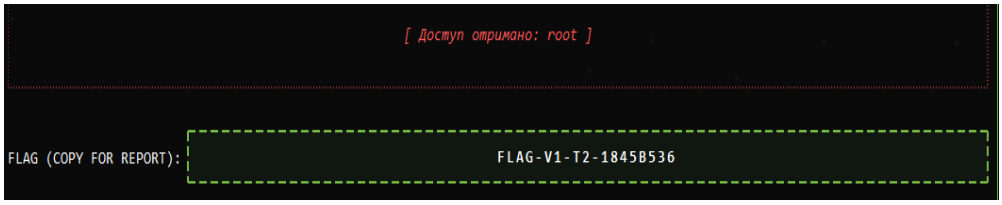

Figure 5 – «2. AUTH»: successful «truth condition» attack

Author's work

The third part of the laboratory work: SQLi vulnerability that allows unauthorized data leakage (Figure 6).

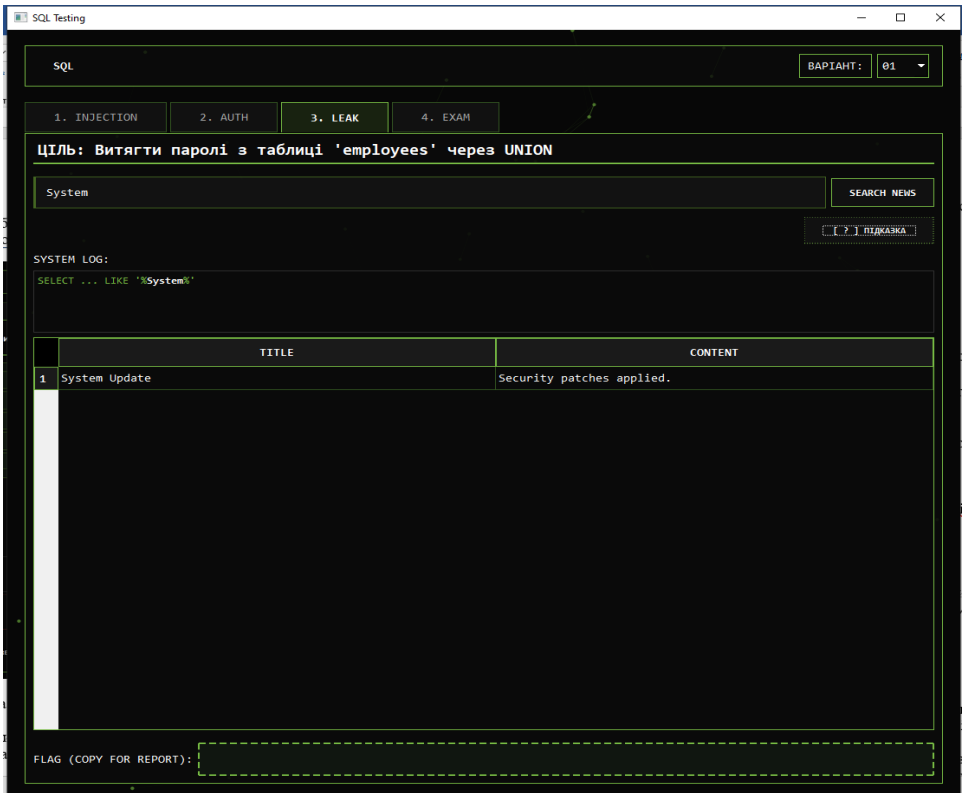

Figure 6 – «3. LEAK»

Author's work

The third part of the laboratory work is performed using prompts. Click «Hints» and get the required query:

' UNION SELECT username, password FROM

and add the table name:

' UNION SELECT username, password FROM employees

We get access to the database and the secret FLAG.

5. Creating tests according to the proposed list of questions based on current information [3-6].

Conclusions

In blended learning according to the proposed methodology «Blend_DB_SQLi», which is based on the use of the created software application «SQL_Testin», the bachelor's degree applicant: firstly, masters subject competencies in the discipline «Databases» (SQL injection and their classification); secondly, masters professional competencies in the specialty «Cybersecurity and information protection» (methods for detecting and preventing SQL injections); thirdly, «Soft skills» are formed (development of the ability to manage one's own time, the ability to work in a team, the development of team members).

References:

1. Гриневич Л. М., Морзе Н. В., Бойко М. А. Наукова освіта як основа формування інноваційної компетентності в умовах цифрової трансформації суспільства. Інформаційні технології і засоби навчання. 2020. т. 77. № 3. 1-26.

2. Дистанційний курс з дисципліни «Бази даних» для здобувачів ступеня «бакалавр» спеціальностей «Кібербезпека та захист інформації», «Комп'ютерна інженерія»; укладач доцент Пахомова В.М. Сертифікат №ДК0288 від 20.07.2018.

3. aCode. SQL-ін'єкції. URL: https://acode.com.ua/sql-injection/

4. FoxmindEd: SQL ін'єкції та захист від них. URL: https://foxminded.ua/sql-iniektsii/

5. PortSwigger. URL: https://portswigger.net

6. QATestLab training center. Тестування безпеки: SQL-ін'єкції. URL: https://training.qatestlab.com/blog/technical-articles/security-testing-sql-injection/