

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра кібербезпеки

**Звіт до лабораторної роботи № 12-13
на тему “ Пошук та експлуатація SQL-ін'єкцій ”**

Виконав студент(ка)

Борщ Дмитро

Група

КБ-01

Перевірила

Лаврик Т.В.

Суми 2023

«Пошук та експлуатація SQL-ін'єкцій»

Мета роботи:

- 1) ознайомитися з функціональними можливостями утиліти Sqlmap;
- 2) провести дослідження веб-ресурсу за допомогою Sqlmap.

I. Загальні відомості.

SQLmap – одна з найпотужніших відкритих утиліт для пентестера, яка автоматизує процес пошуку і експлуатації SQL-ін'єкцій з метою отримання даних або захоплення віддаленого хоста. Що робить SQLmap відмінним від інших утиліт для виявлення SQL-ін'єкцій, так це можливість експлуатувати кожну знайдену уразливість. Це означає, що SQLmap здатна не тільки знаходити «дірку», але ще і застосувати її. А коли вже в якості завдання ставиться саме експлуатація уразливості, то сканеру доводиться бути особливо уважним до деталей: він не буде видавати мільйон помилкових спрацьовувань «так, про всяк випадок».

Будь-яка потенційна вразливість додатково перевіряється на можливість експлуатації. Сканер має величезний функціонал, починаючи від можливості визначення системи управління базою даних, створення дампа (копії) даних і закінчуючи отриманням доступу до системи з можливістю звертатися до довільних файлів на хості та виконувати на сервері довільні команди. І все-таки головне – це виявлення можливості зробити ін'єкцію SQL-коду.

Завдання до роботи:

Завдання 1 (платформа Range Force). Виконати модулі:

- «Web Application Security Foundations / SQL Injection: Overview»
- SQL Injection: Prelude
- SQL Injection: Authentication Bypass
- SQL Injection: Union Select
- Blind SQL Injection: Find & Exploit (PHP)

Завдання 2.

1. За результатами проведення сканування цільового ресурсу сканером OWASP ZAP обрати перелік параметрів для перевірки їх на вразливість до sql ін'єкцій та внести їх до таблиці (обрати для перевірки 2-4 параметри).

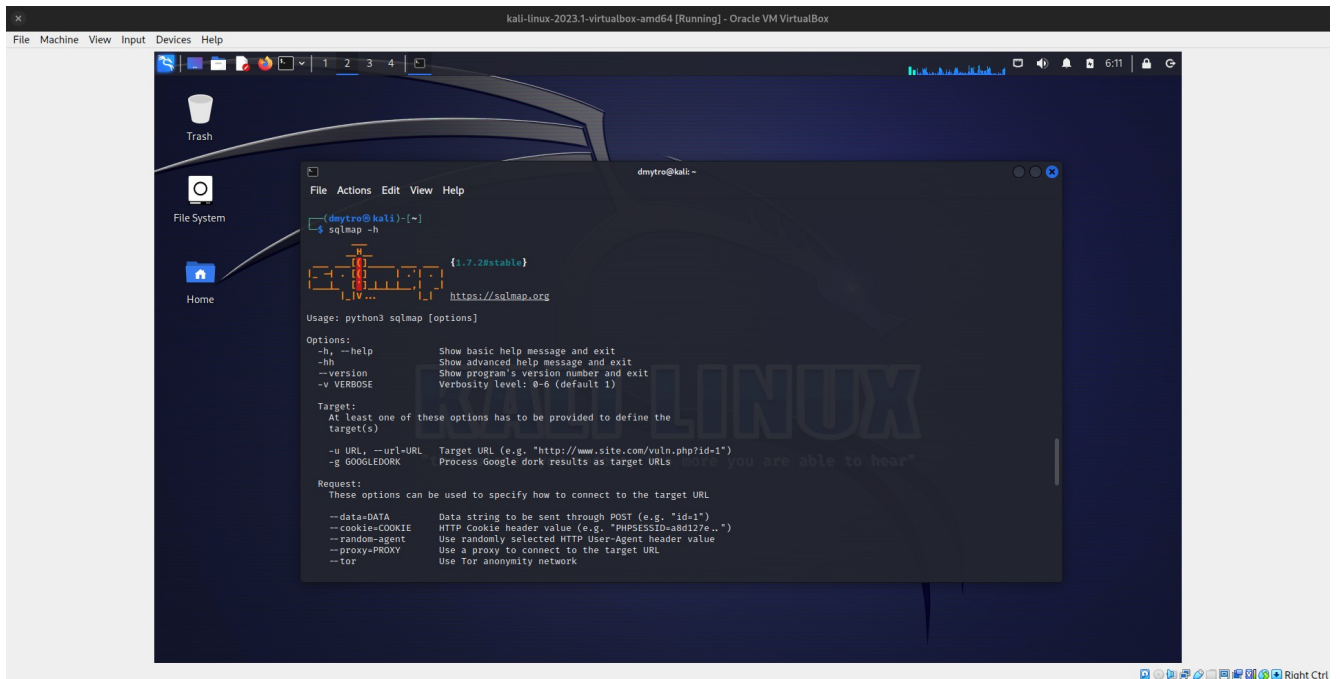
№	Посилання з параметром
1	http://www.humor.co.il/kiki/kikipedia.php?wakka=Home
2	http://www.humor.co.il/adventure/banner.php?action=show&id=15

Завдання 3. Вивчення SQLmap

3.1 Ознайомтеся зі статтею [2]. Випишіть всі основні опції SQLmap, які можуть бути корисними для тестування (виведення заголовка Cookie, списку таблиць, баз даних тощо).

Опція sqlmap	Опис
- -dbs	Визначити наявні бази даних в СКБД
- -tables	Визначити таблиці у вказаній за допомогою параметру -D базі
- -columns	Визначити колонки у вказаній за допомогою параметру -T таблиці
- -dump	Зняти дамп записів, необхідно вказати базу даних(-D) та таблицю (-T)
- D	Вказати базу даних з визначених за допомогою параметра --dbs
- T	Вказати таблицю з визначених зв допомогою параметра --tables
- C	Вказати колонку визначену за допомогою параметра --columns. Може використовуватися разом з --dump

3.2 Запустіть Kali Linux. Запустіть утиліту SQLmap на віртуальній машині Kali Linux.

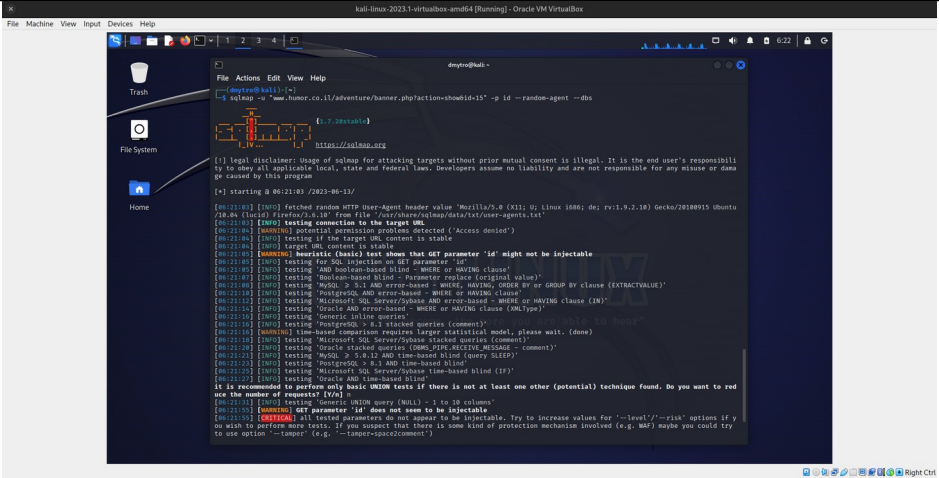
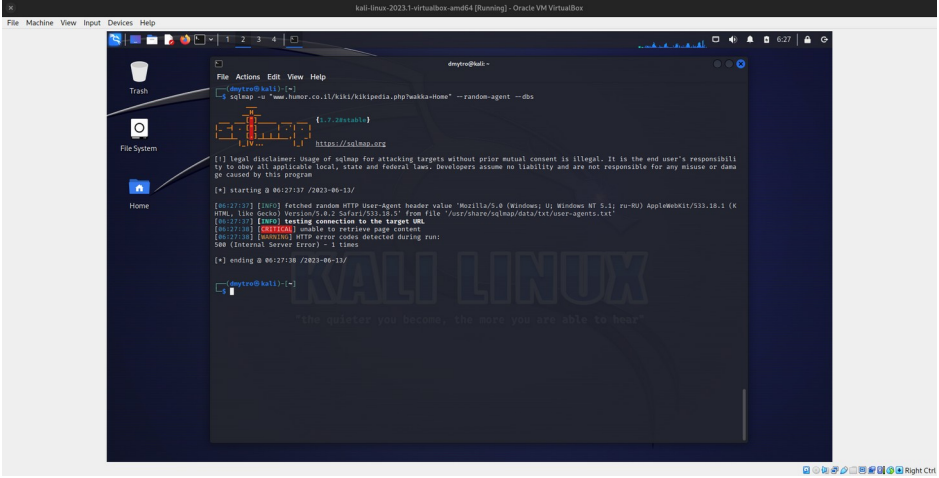


3.3 Для заданого цільового ресурс проведіть дослідження за допомогою SQLmap.

Застосуйте необхідні опції для того, щоб:

- a) перевірити обрану ціль на наявність sql-ін'єкцій;
- b) отримати список баз даних;
- c) отримати список таблиць однієї з баз даних (бажано з цінною інформацією, наприклад, з користувачами);
- d) дізнатися список колонок з обраної таблиці;
- e) вивести вміст всієї таблиці.

Заповніть таблицю з командами і скріншотами.

Команда	Результат	Скріншот
<pre>sqlmap -u "www.humor.co.il/adventure/b anner.php?action=show&id=15" -p id --random-agent --dbs</pre>	Параметр не вразливий	
<pre>sqlmap -u "www.humor.co.il/kiki/kikipedia.php?wakka=home" --random-agent --dbs</pre>	Внутрішня помилка серверу. Схоже що ця сторінка просто зламана та Active Scan помилково позначив її як вразливу.	

Рекомендація: в командах використовувати параметр --random-agent

Висновок:

Яка версія бази даних?

-

Який параметр(и) виявився уразливим до sql ін'єкцій?

-

Яку ще інформацію можна вивести, використовуючи SQLmap?

Інформацію про структуру бази даних, вміст таблиць, що за достатніх привілеїв користувача дозволяє дізнатися всю інформацію про СКБД.

Які існують способи захисту від SQL ін'єкцій?

Використання підготовлених операторів і параметризованих запитів.

Фільтрація та валідація вхідних даних. Екранування спеціальних символів

Використання обмежень доступу до бази даних. Частково захищає, дозволяє знизити шкоду при отриманні несанкціонованого доступу.

Використання вбудованих механізмів безпеки бази даних.

Моніторинг і аудит бази даних для виявлення некоректних запитів.

Основні ресурси:

1. Відео «Як встановити Sqlmap на Windows OS» - https://www.youtube.com/watch?v=CdR7pw_FBj8
2. Sqlmap - інструменти Kali Linux (англійською мовою) - <https://en.kali.tools/?p=1>