

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BỘ MÔN BẢO MẬT WEB**

 🙠🙟🕮🙝🙢

**BÁO CÁO BÀI TẬP**

**SỬ DỤNG SQLMAP ĐỂ KHAI THÁC**

**LỖ HỔNG SQL INJECTION**

**MÃ MÔN HỌC: WESE331479**

**GIẢNG VIÊN HƯỚNG DẪN: Lê Thị Minh Châu**

**SINH VIÊN THỰC HIỆN: – MSSV**

**VŨ HOÀNG ANH – 20110205**

**Tp. Hồ Chí Minh, tháng 3 năm 2023**

**MỤC LỤC**

[**1.** **Giới thiệu SQL MAP** 3](#_Toc129033853)

[**2.** **Các tính năng** 3](#_Toc129033854)

[**3.** **Các bước tải** 4](#_Toc129033855)

[**4.** **Demo** 9](#_Toc129033856)

# **Giới thiệu SQL MAP**

SQLMAP là công cụ khai thác những lổ hỏng của cơ sở dữ liệu SQL. Công cụ này được xem là công cụ khai thác SQL tốt nhất hiện nay. Được giới bảo mật và giới hacker sử dụng thường xuyên. Với người dùng Kali hoặc Back Track 5 thì SQLMAP đã được tích hợp sẵn vào hệ điều hành. Riêng Windows thì chúng ta phải cài đặt thêm python và SQLMAP để sử dụng

Đây là công cụ mã nguồn mở, tự động hóa quá trình phát hiện và khai thác lỗ hổng SQL. Nó đi kèm với một công cụ phát hiện mạnh mẽ, nhiều tính năng thích hợp cho trình kiểm tra thâm nhập cuối cùng

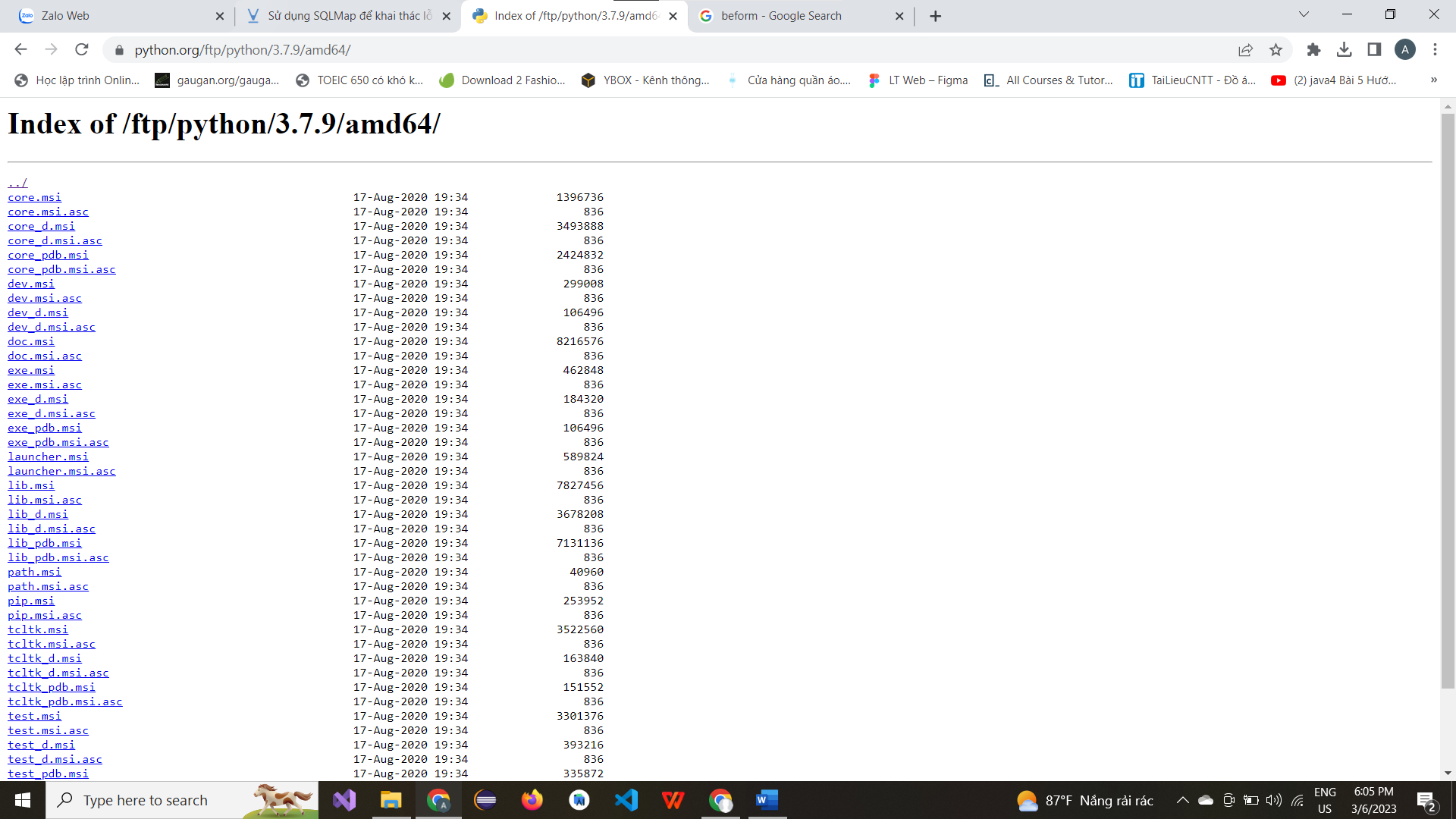
# **Các tính năng**

* Hỗ trợ đầy đủ làm việc với các hệ quản trị cơ sở dữ liệu MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, ...
* Hỗ trợ đầy đủ cho các kỹ thuật tấn công SQL Injection: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries và out-of-band.
* Kết nối trực tiếp với cơ sở dữ liệu mà không cần thông qua SQL SQL, bằng cách cung cấp thông tin đăng nhập DBMS, địa chỉ IP, cổng và tên cơ sở dữ liệu.
* Liệt kê người dùng, password hash, đặc quyền, vai trò, cơ sở dữ liệu, bảng và cột.
* Tự động nhận dạng các định dạng băm mật khẩu và hỗ trợ bẻ khóa chúng bằng cách sử dụng một cuộc tấn công dựa trên từ điển.
* Trích xuất hoàn toàn các bảng cơ sở dữ liệu, một loạt các mục hoặc các cột cụ thể theo lựa chọn của người dùng
* Tìm kiếm tên cơ sở dữ liệu cụ thể, các bảng cụ thể trên tất cả các cơ sở dữ liệu hoặc các cột cụ thể trên tất cả các bảng của cơ sở dữ liệu
* Tải xuống và tải lên bất kỳ tệp nào từ máy chủ cơ sở dữ liệu bên dưới hệ thống tệp khi phần mềm cơ sở dữ liệu là MySQL, PostgreQuery hoặc Microsoft SQL Server.
* Thực hiện các lệnh tùy ý và truy xuất đầu ra tiêu chuẩn của chúng trên máy chủ cơ sở dữ liệu bên dưới hệ điều hành khi phần mềm cơ sở dữ liệu là MySQL, PostgreQuery hoặc Microsoft SQL Server

# **Các bước tải**

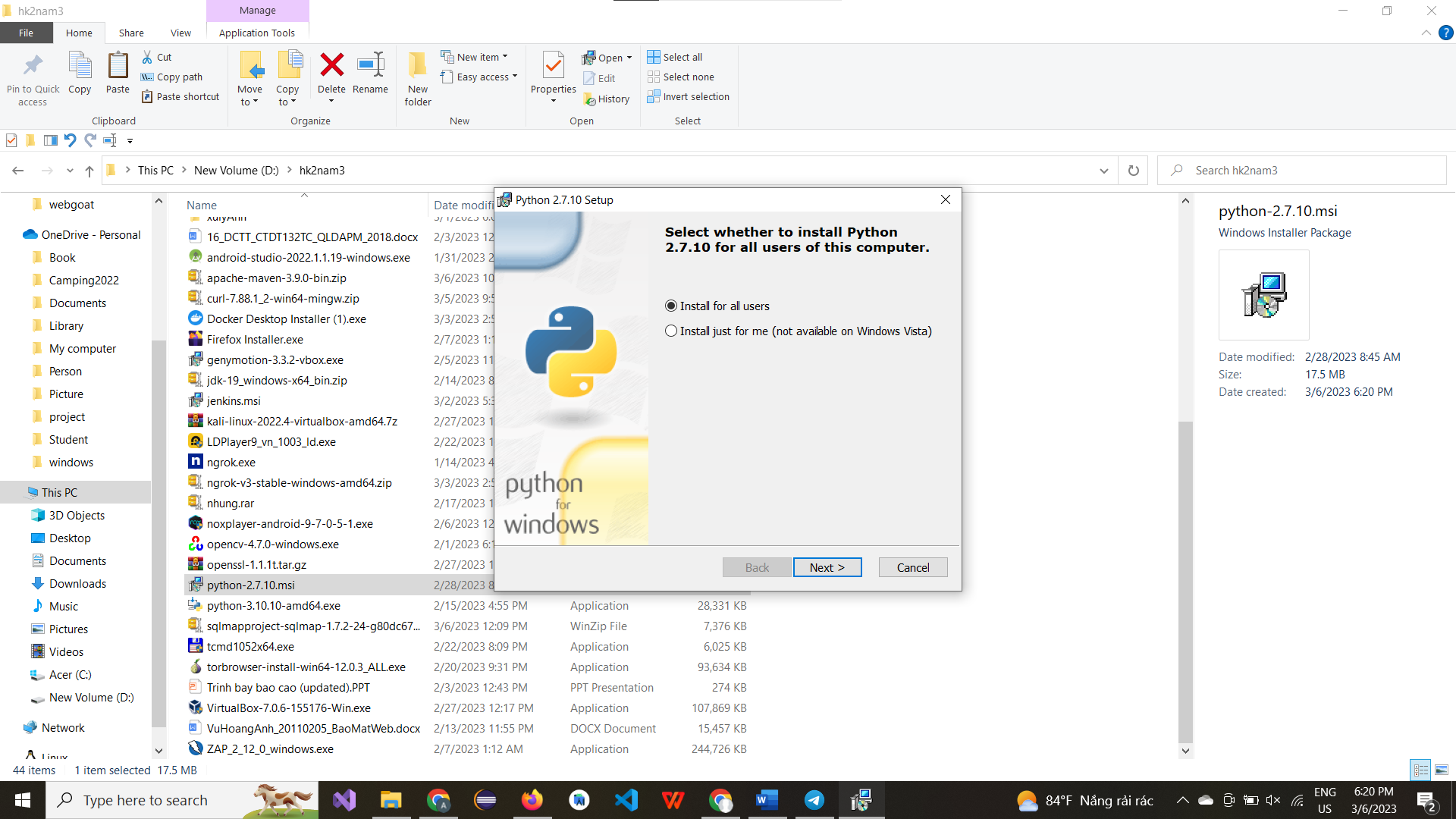
**Bước 1: Tải file cài đặt Python và SQLMap**

Link cài đặt Python: [https://www.python.org/ftp/python/2….hon-2.7.10.msi](https://www.python.org/ftp/python/2%E2%80%A6.hon-2.7.10.msi)

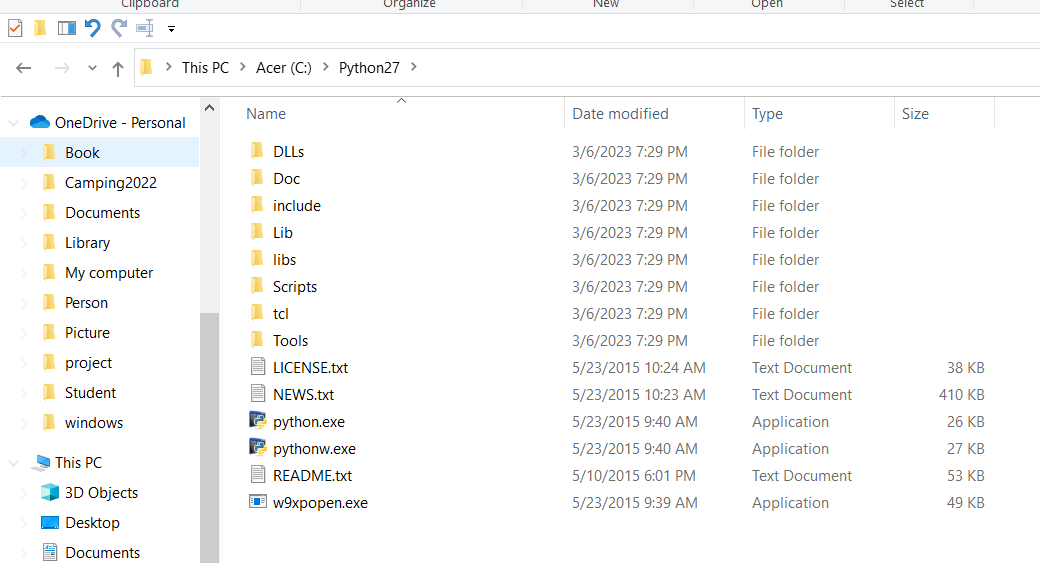


Link cài đặt SQLMap: <https://github.com/sqlmapproject/sqlmap/zipball/master>

**Bước 2: Cài đặt Python** Mở file python-2.7.10.msi và chọn “install for all users” sau đó click Next.



**Bước 3: Giải nén file sqlmap vừa tải sau đó copy toàn bộ thư mục sqlmap vào đường dẫn C:\Python27**



Tải SQL MAP về

Text

Description automatically generated

Giải nén SQL MAP

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text

Description automatically generated

Copy toàn bộ file của SQL MAP vào Python27

Table

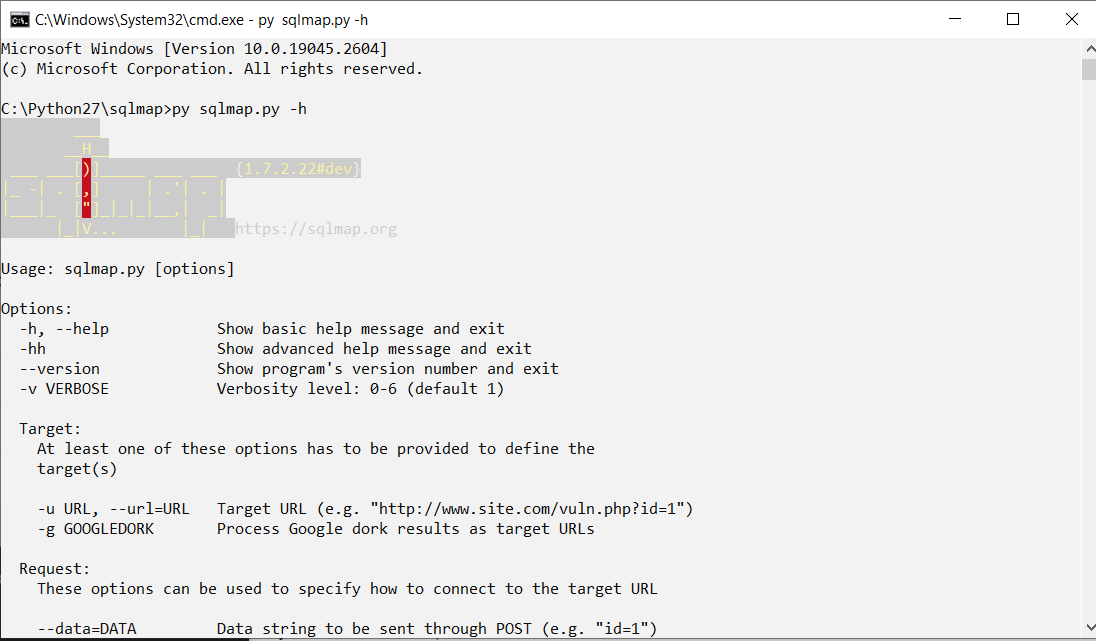
Description automatically generated

Mở CMD và điều hướng tới file sqlmap

Graphical user interface, text, application, email

Description automatically generated

Sử dụng câu lệnh **py sqlmap.py -h** để kiểm tra môi trường thực hiện được cài đặt thành công hay chưa.



Đã cài đặt thành công

# **Demo**

Bài học yêu cầu chúng ta tấn công trang web có địa chỉ là:

<http://testphp.vulnweb.com/>

Graphical user interface, text, application

Description automatically generated

Các bước thực hiện:

**Bước 1: Mở CMD, sử dụng câu lệnh:**

py sqlmap.py –u”[http://testphp.vulnweb.com/search.php?test=query”](http://testphp.vulnweb.com/search.php?test=query%E2%80%9D)

u: là url của mục tiêu

SQLMap sẽ phát hiện lỗ hổng của mục tiêu vào đưa ra thông tin về lỗ hổng.

Graphical user interface, text, application, email

Description automatically generated

Kết quả thực hiện

Graphical user interface

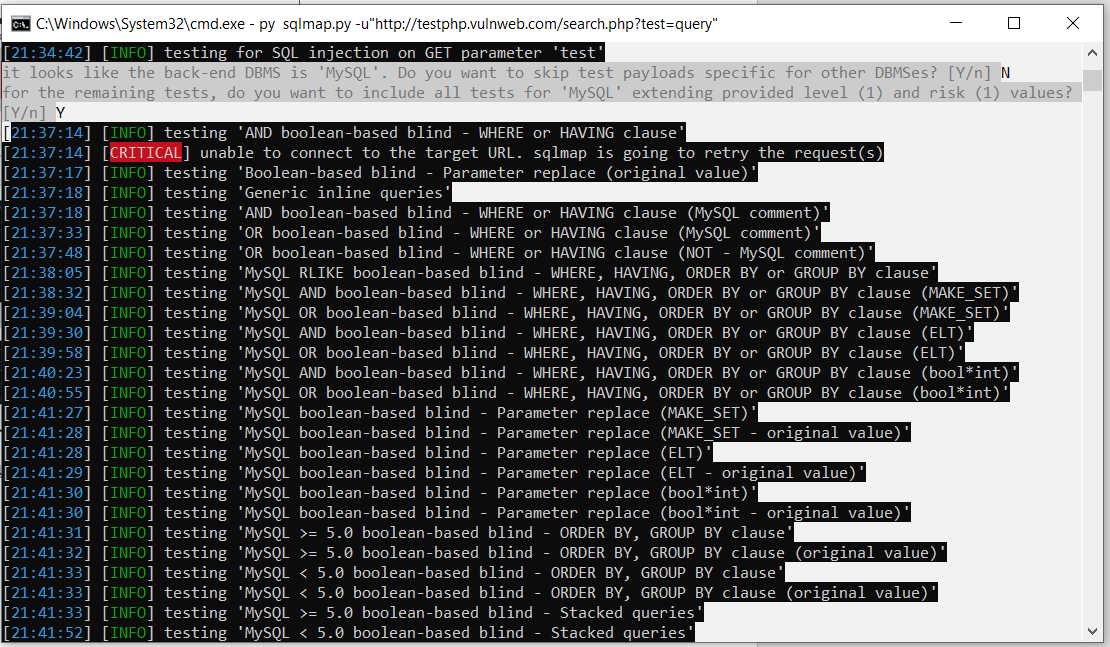
Description automatically generated

Chọn No, và tiếp tục thực hiện

Graphical user interface

Description automatically generated

Tiếp tục thực hiện Y (Yes) Và đợi khoảng 10 phút để hệ thống quét trang web xong.



Timeline

Description automatically generated with medium confidence

Thực hiện chọn Y và tiếp tục

Kết quả thực hiện

Graphical user interface, text

Description automatically generated with medium confidence

**Bước 2: Sau khi xác định được lỗi** **lỗ hổng SQL injection, ta tiến hành tìm tên cơ sở dữ liệu.**

**Sử dụng câu lệnh:**

**py** [**sqlmap.py**](sqlmap.py) **–u “**[**http://testphp.vulnweb.com/search.php?test=query”**](http://testphp.vulnweb.com/search.php?test=query%E2%80%9D) **–dbs**

Trong đó: -dbs là option để liệt kê các cơ sở dữ liệu của website.

**Graphical user interface, text, application, email

Description automatically generated**

Kết quả thực hiện.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Chúng ta xác định tên của CSDL là acuart

Graphical user interface, text

Description automatically generated

**Bước 3: Sau khi xác định được tên cơ sở dữ liệu, ta sẽ tìm tiếp tên các bảng có trong cơ sở dữ liệu**

**Sử dụng câu lệnh:**

py <sqlmap.py> -u"<http://testphp.vulnweb.com/search.php?test=query>" --tables -D acuart

Option – tables để liệt kê tất cả các bảng có trong cơ sở dữ liệu  
Option –D là tên cơ sở dữ liệu cần liệt kê bảng

**Graphical user interface, text, application

Description automatically generated**

Chúng ta xác định được tổng số bảng của CSDL

**Text

Description automatically generated**

Có 8 bảng

**A picture containing text

Description automatically generated**

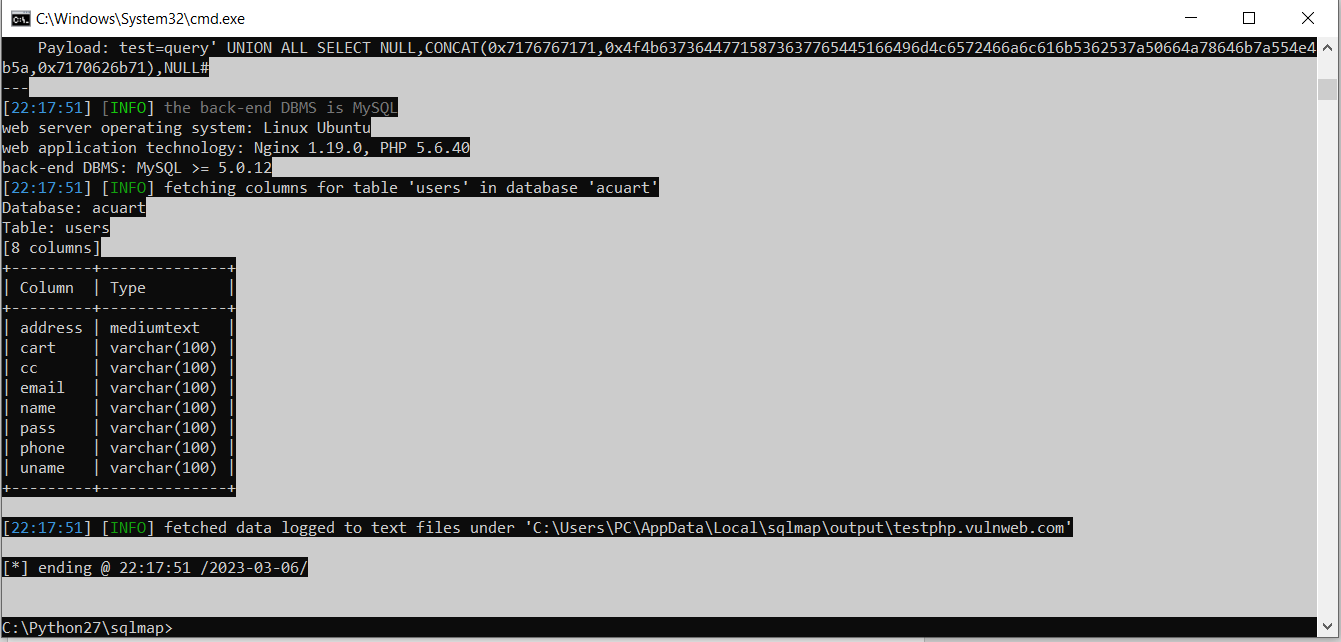
**Bước 4: Xác định tên các cột trong bảng**

**Ta lấy thông tin trong bảng user, thường sẽ có password và username.**

**Sử dụng câu lệnh:**

py <sqlmap.py> -u"<http://testphp.vulnweb.com/search.php?test=query>" --columns -D acuart -T users

Xác định được trong bảng user có 8 cột

****

**Bước 5: Lấy dữ liệu trong bảng user**

Chúng ta sử dụng câu lệnh:

**py** [**sqlmap.py**](sqlmap.py) **-u"**[**http://testphp.vulnweb.com/search.php?test=query**](http://testphp.vulnweb.com/search.php?test=query)**" --dump -D acuart -T users**

**Shape

Description automatically generated with medium confidence**

Câu lệnh sẽ lấy thông tin có trong bảng user, có thể chứa user và password của người dùng

Kết quả thực hiện:

Chúng ta lấy thông tin của John, có user và password

A picture containing graphical user interface

Description automatically generated

Qua bài học, chúng ta có thể thấy lỗ hổng SQL injection hết sức nguy hiểm, qua các lỗ hổng đó, người dùng có thể bị đánh mất thông tin quan trọng, gây thiệt hại cho doanh nghiệp, tổ chức, cá nhân.