



# PHÁT HIỆN TẤN CÔNG CHÈN MÃ SQL DỰA TRÊN PHÂN TÍCH CÚ PHÁP CÂU TRUY VẤN

SINH VIÊN THỰC HIỆN:

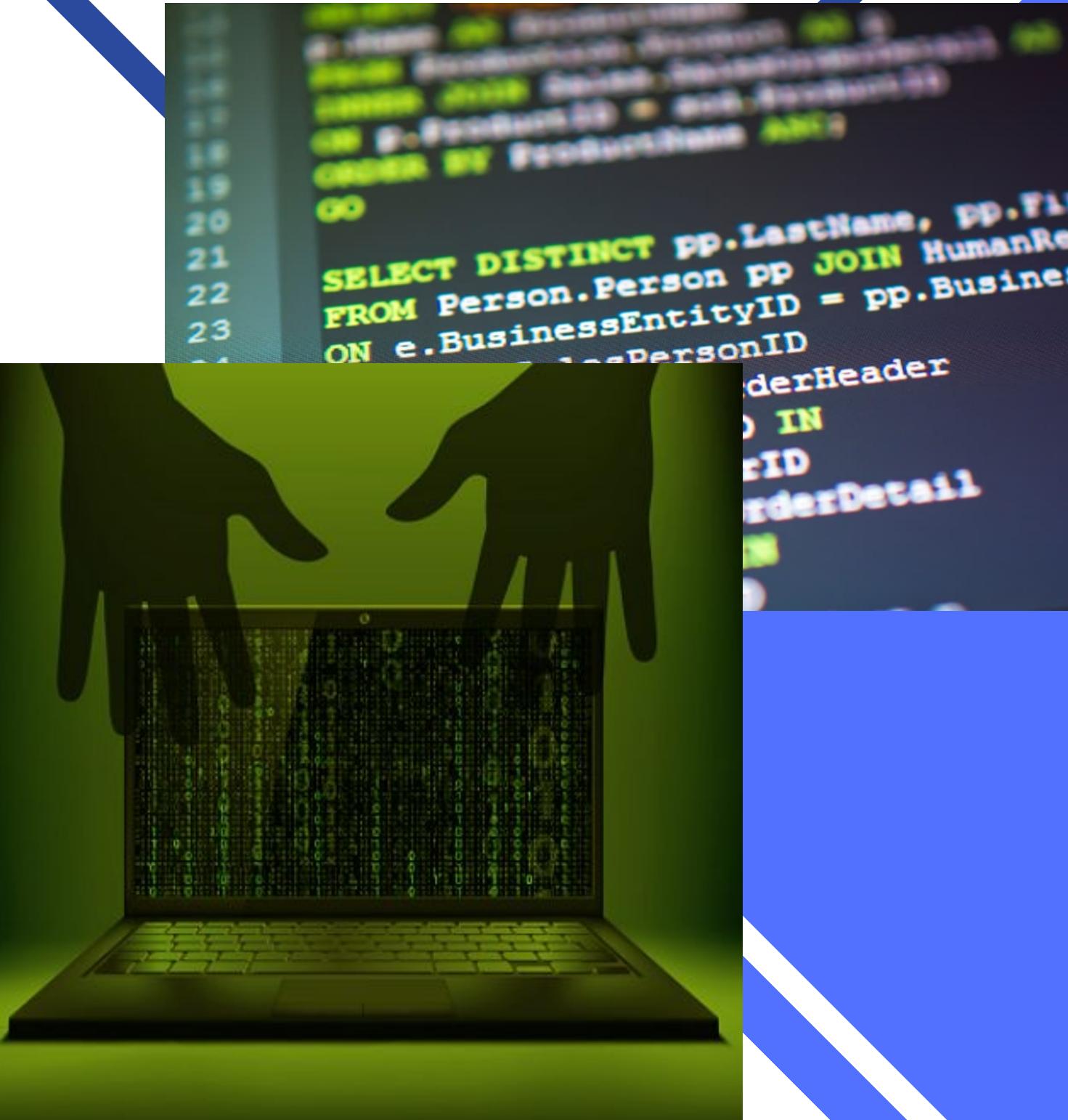
HỒ NHƯ PHONG 20TCLC\_DT3  
TRẦN GIA HUY 20TCLC\_DT1

GIẢNG VIÊN HƯỚNG DẪN:

THS. NGUYỄN VĂN NGUYÊN

# GIỚI THIỆU ĐỀ TÀI

Đề tài "Phát hiện tấn công chèn mã SQL dựa trên phân tích cú pháp câu truy vấn" tập trung vào nghiên cứu và phát triển các phương pháp hiệu quả để phát hiện và ngăn chặn tấn công chèn mã SQL, một trong những kỹ thuật phổ biến của các hacker nhằm tận dụng lỗ hổng bảo mật trong hệ thống quản lý cơ sở dữ liệu (DBMS).



# NỘI DUNG THUYẾT TRÌNH

1 **TỔNG QUAN ĐỀ TÀI**

2 **TRIỂN KHAI VÀ KẾT QUẢ ĐẠT ĐƯỢC**

3 **KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**



# 1

## TỔNG QUAN ĐỀ TÀI

TỔNG QUAN VỀ TẤN CÔNG CHÈN MÃ SQL VÀ  
CÁC BIỆN PHÁP PHÒNG CHỐNG



# NGÔN NGỮ SQL

SQL (Structured Query Language) là một ngôn ngữ lập trình sử dụng để quản lý và tương tác với cơ sở dữ liệu.

SQL được thiết kế để thực hiện các thao tác như truy vấn dữ liệu, cập nhật dữ liệu, chèn dữ liệu, xóa dữ liệu, và quản lý cấu trúc của cơ sở dữ liệu.

SQL được sử dụng để điều khiển tất cả các chức năng mà một hệ quản trị cơ sở dữ liệu cung cấp cho người dùng bao gồm:

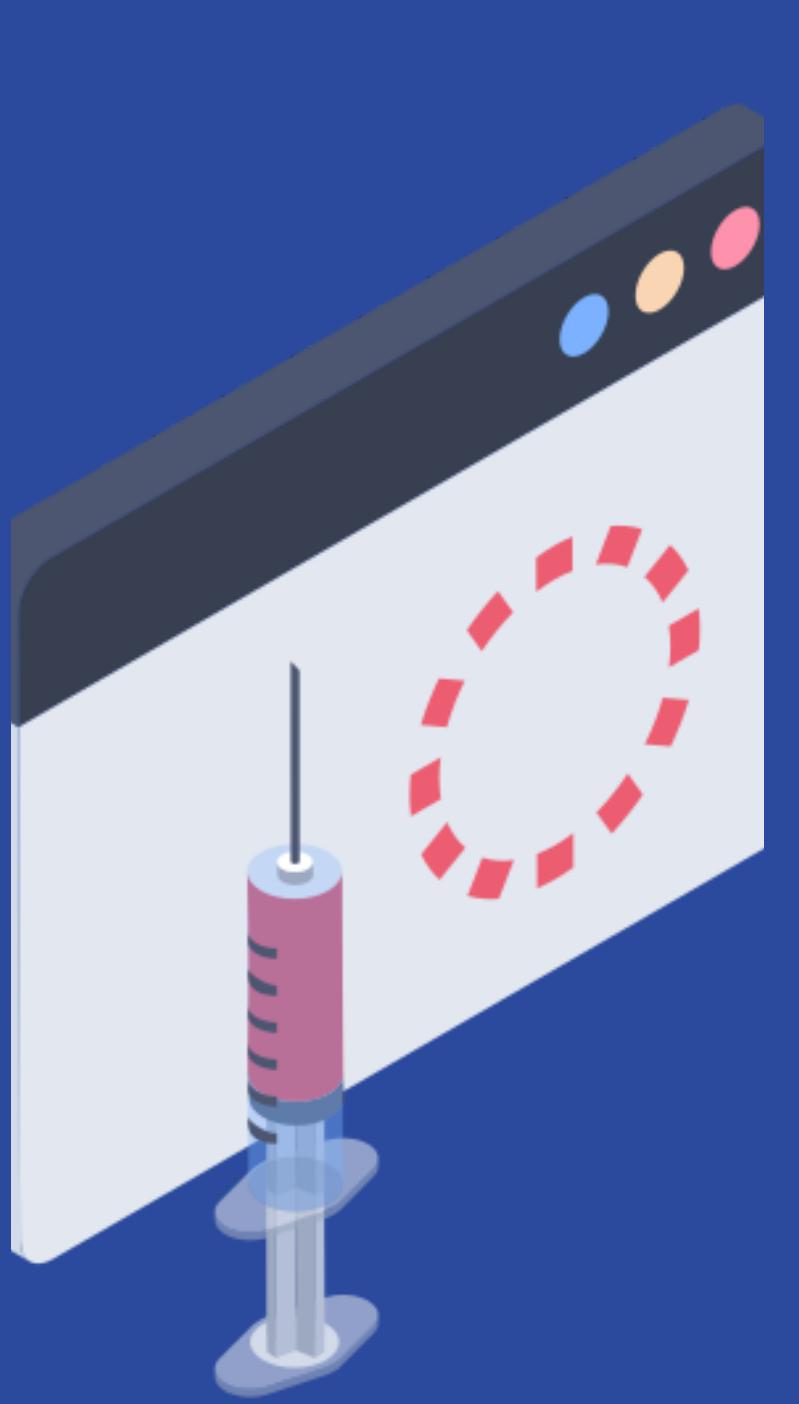
- Định nghĩa dữ liệu
- Truy xuất và thao tác dữ liệu
- Điều khiển truy cập
- Đảm bảo toàn vẹn dữ liệu



# TỔNG QUAN VỀ SQL INJECTION

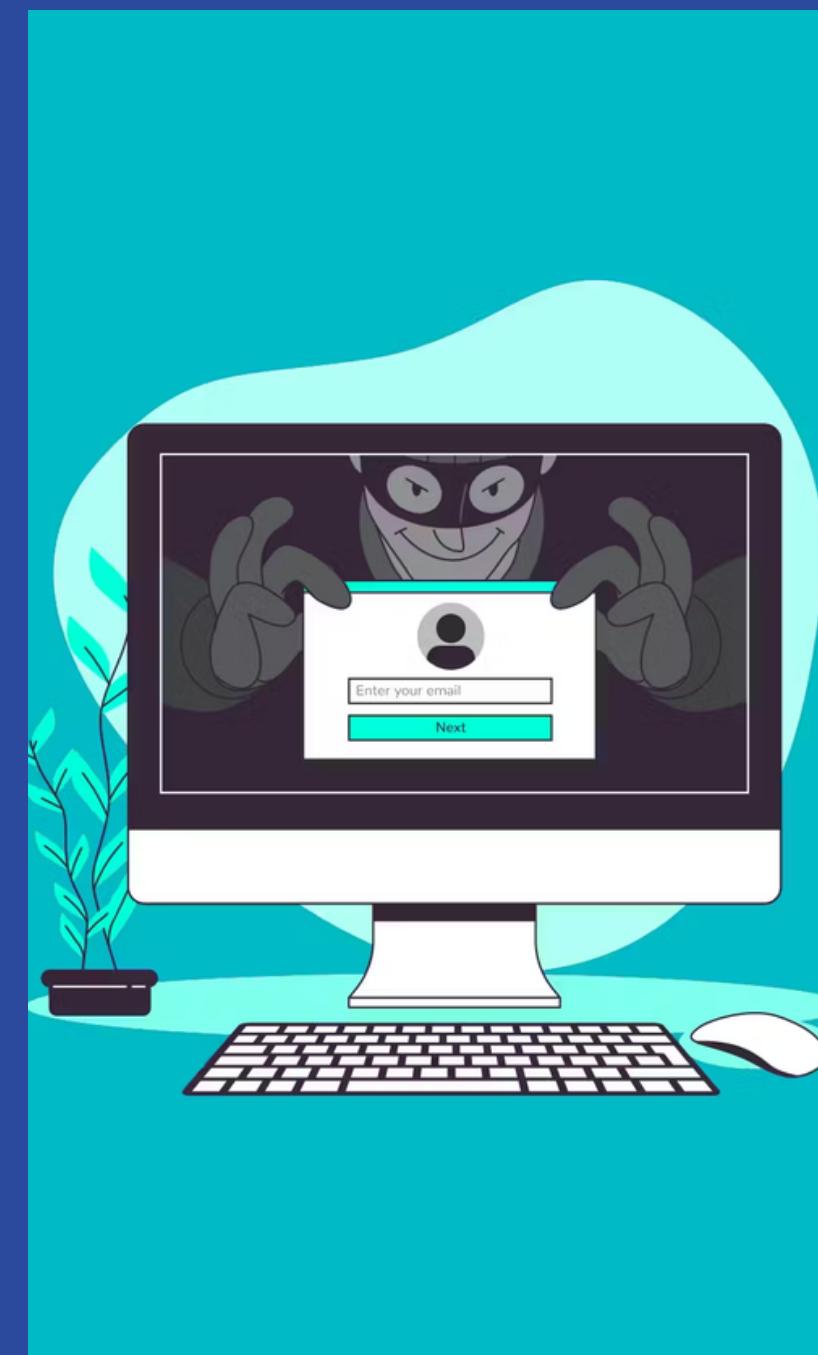
## SQL Injection

SQL Injection là một kỹ thuật tấn công phổ biến trong lĩnh vực bảo mật web, mục tiêu chính là tận dụng lỗ hổng trong xử lý dữ liệu đầu vào của các ứng dụng web để thực hiện các câu lệnh SQL độc hại.

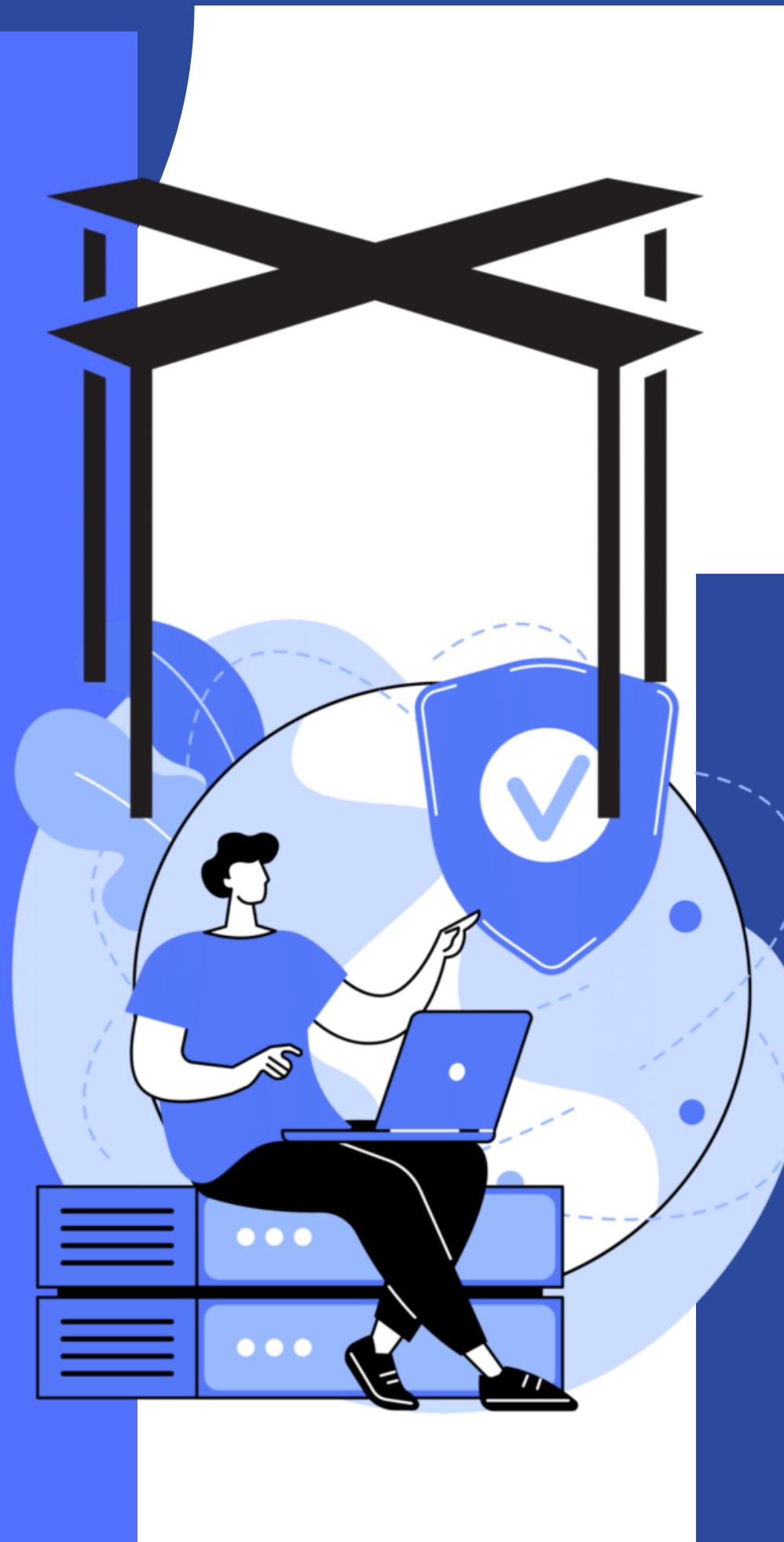


## Hậu quả

- Trích xuất dữ liệu nhạy cảm của hệ thống
- Thay đổi dữ liệu của hệ thống
- Sửa đổi cấu trúc của cơ sở dữ liệu



# MỤC ĐÍCH TẤN CÔNG SQL INJECTION



Mục đích chính của tấn công SQL Injection là lợi dụng các lỗ hổng bảo mật trong ứng dụng web hoặc trang web để thực hiện các hành động không được phép đối với cơ sở dữ liệu. Một số mục đích phổ biến của tấn công SQL Injection là:

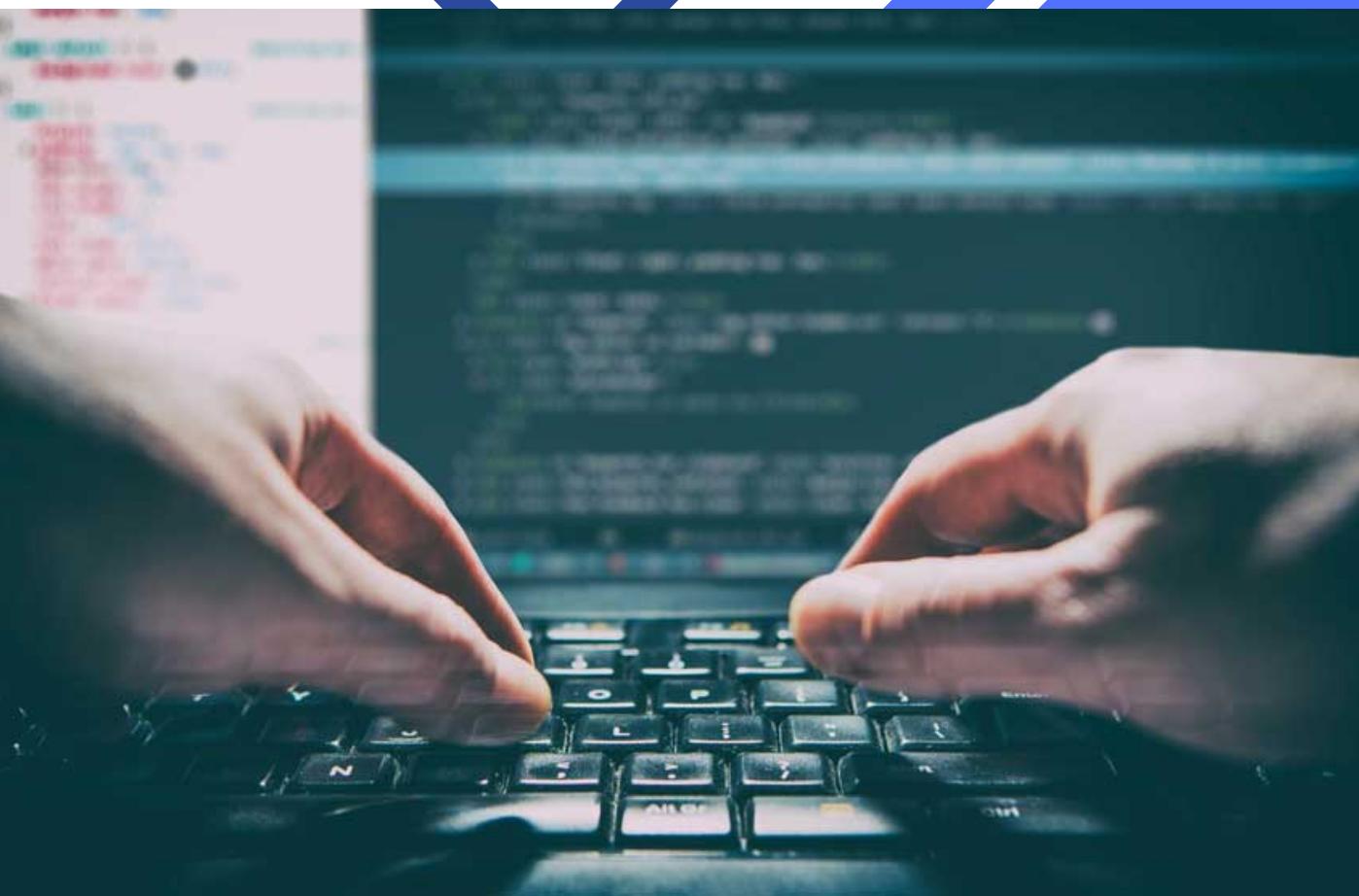
- Thu thập thông tin về cơ sở dữ liệu.
- Thay đổi dữ liệu.
- Thực hiện các thao tác không hợp pháp.
- Kiểm thử bảo mật.

# CƠ CHẾ TẤN CÔNG CHÈN MÃ SQL

Tấn công chèn mã SQL (SQL Injection) thường được thực hiện bằng cách chèn các đoạn mã SQL độc hại vào các trường nhập liệu hoặc tham số của ứng dụng web.

Một số cơ chế phổ biến mà kẻ tấn công sử dụng để thực hiện SQL Injection:

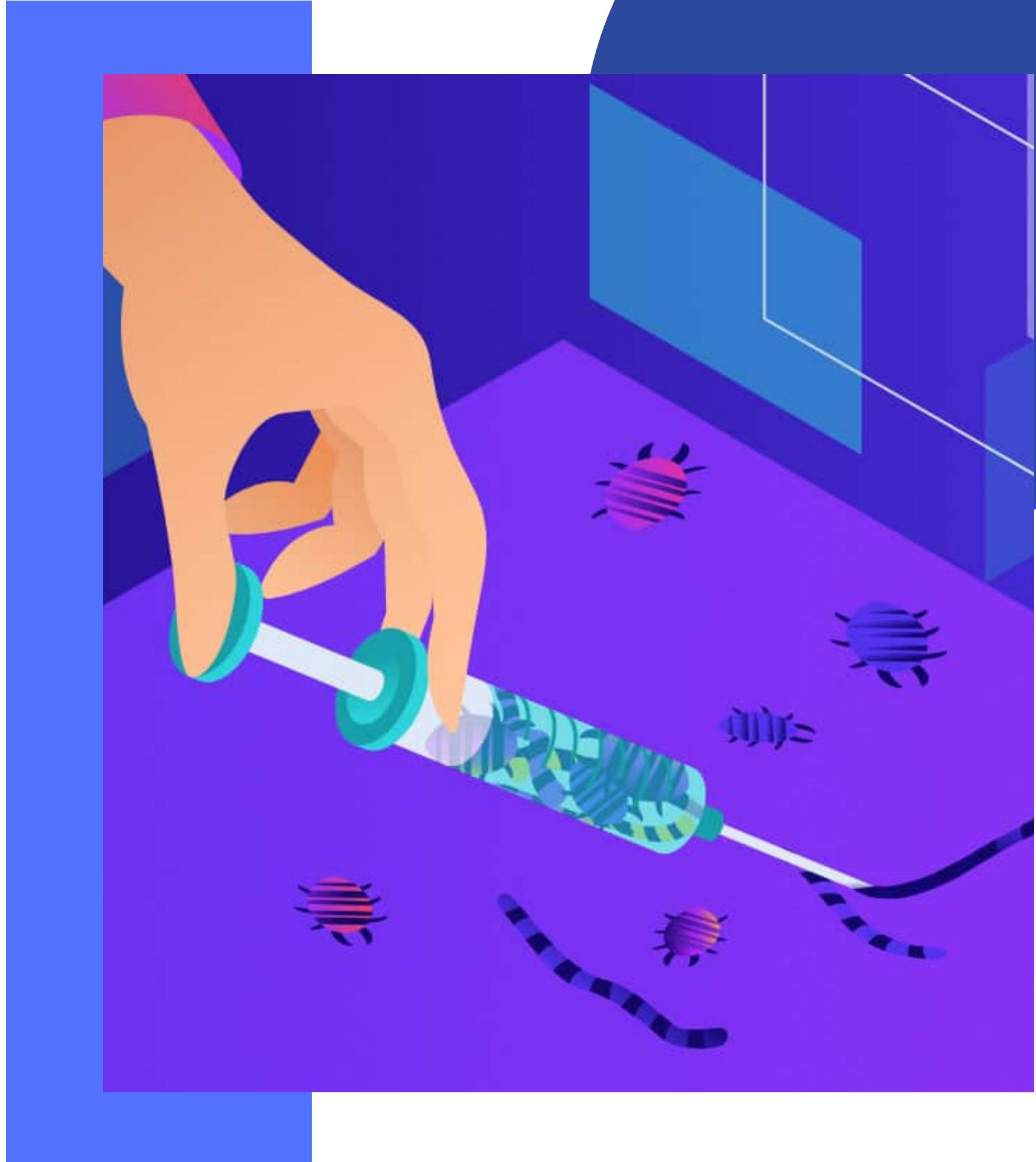
- Chèn vào trường nhập liệu
- Chèn mã thông qua Cookie
- Chèn vào câu lệnh SQL trực tiếp



# CÁC DẠNG TẤN CÔNG BẰNG SQL INJECTION

Có bốn dạng tấn công thông thường:

- Classic SQL Injection
- Tấn công sử dụng câu lệnh SELECT
- Tấn công khai thác dữ liệu thông qua toán tử UNION
- Tấn công sử dụng câu lệnh INSERT



# CLASSIC SQL INJECTION

Kẻ tấn công chèn đoạn mã SQL vào các trường nhập liệu của ứng dụng web, chẳng hạn như ô tìm kiếm, biểu mẫu đăng nhập, hoặc trường khác.

Ví dụ: '**OR '1'='1'; --**



# TẤN CÔNG SỬ DỤNG CÂU LỆNH SELECT

Kiểu tấn công này cho phép kẻ tấn công thu thập các thông tin quan trọng về kiểu và cấu trúc của hệ thống cơ sở dữ liệu đầu cuối của ứng dụng web.

```
20
21
22
23
24
25
26
27
28
```

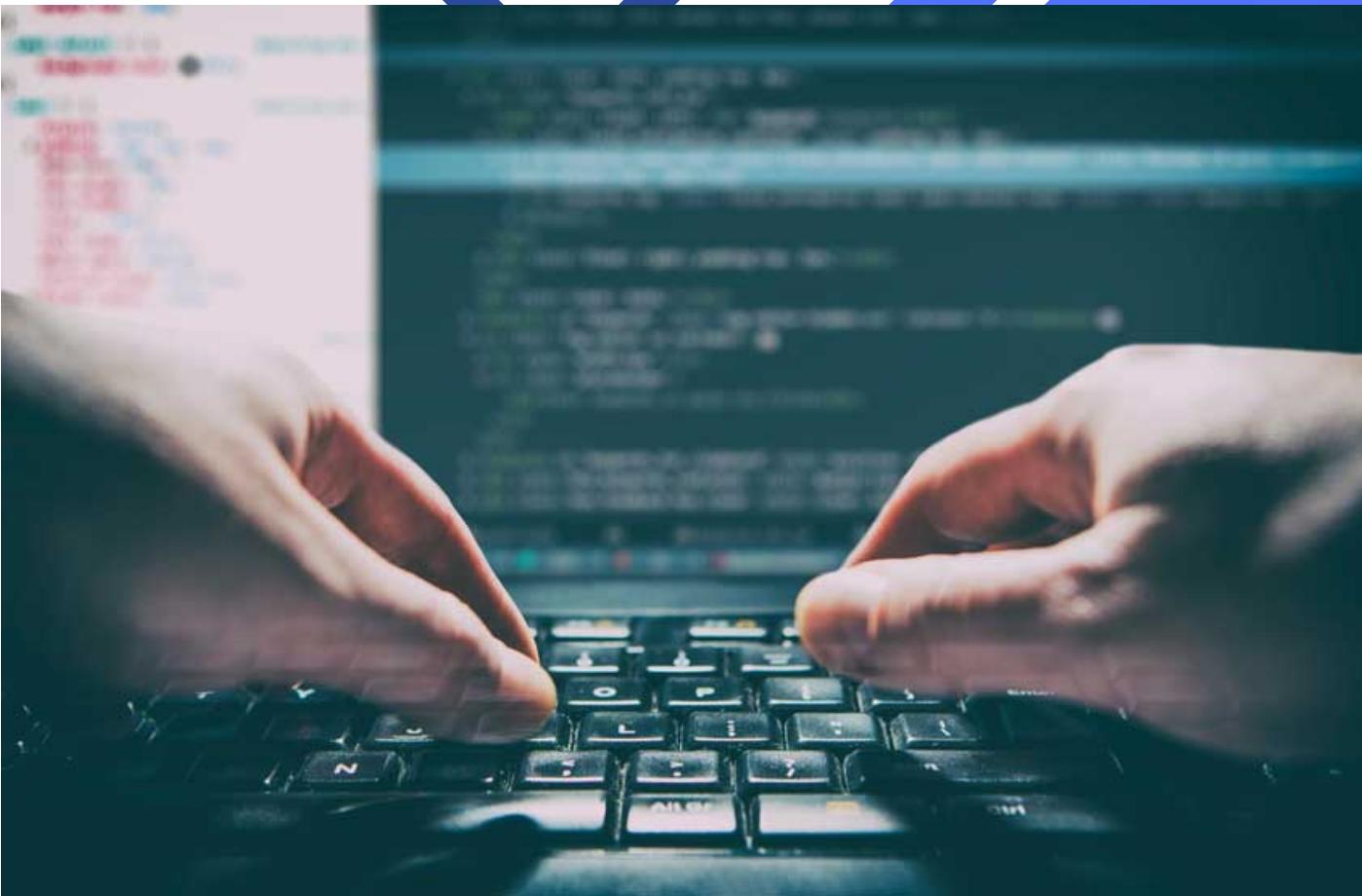
SELECT DISTINCT pp.LastName, pp....
FROM Person.Person PP JOIN HumanRe
ON e.BusinessEntityID = pp.Business
(SLECT SalesPersonID
FROM Sales.SalesOrderHeader
WHERE SalesOrderID IN
(SLECT SalesOrderID
FROM Sales.SalesOrderDetail

**Ví dụ:** Trang đăng nhập có 3 trường đầu vào là username, password và mã pin với đoạn truy vấn sau để thực hiện việc đăng nhập:  
**SELECT accounts FROM users WHERE login=**" AND pass=" AND pin=  
Mục đích gây ra lỗi có thể tiết lộ thông tin dữ liệu. Để làm việc này kẻ tấn công sẽ chèn nội dung vào trường đầu vào chứa mã pin. Câu truy vấn trở thành:  
**SELECT accounts FROM users WHERE login=**" AND pass=" AND pin= convert (int, (select top 1 name from sys.objects where xtype='u'))

# TẤN CÔNG KHAI THÁC DỮ LIỆU THÔNG QUA TOÁN TỬ UNION

Trong kiểu tấn công này, kẻ tấn công khai thác một tham số dễ bị tổn thương để thay đổi các thiết lập dữ liệu trả về với một câu truy vấn, từ đó lừa ứng dụng trong việc trả về dữ liệu từ bảng dữ liệu khác.

Ví dụ: Với bảng Credit Cards, kẻ tấn công sẽ chèn đoạn mã “**‘UNION SELECT cardNo FROM CreditCards WHERE acctNo=10032--’** vào trong trường login. Khi đó câu query sẽ trở thành:  
**SELECT accounts FROM users WHERE login=“UNION SELECT cardNo from CreditCards WHERE acctNo=10032-- AND pass=“ AND pin=**



# TẤN CÔNG SỬ DỤNG CÂU LỆNH INSERT

Trong loại tấn công này, kẻ tấn công cố gắng chèn hoặc thay đổi dữ liệu trong cơ sở dữ liệu bằng cách sử dụng câu lệnh INSERT.

Ví dụ: Giả sử có một ứng dụng web có chức năng thêm mới người dùng và câu lệnh INSERT được sử dụng như sau:

```
INSERT INTO Users (username, password)
VALUES ('$username', '$password');
```

Kẻ tấn công có thể chèn dữ liệu độc hại:  
“ ' OR '1'='1'; -- ”

Kết quả là câu lệnh SQL trở thành:

```
INSERT INTO Users (username, password)
VALUES (" OR '1'='1'; -- ', '$password');
```



# CÁC BIỆN PHÁP PHÒNG CHỐNG



## CÁC BIỆN PHÁP PHÒNG CHỐNG Ở MỨC ĐỘ LẬP TRÌNH

- Làm sạch dữ liệu đầu vào
- Xây dựng truy vấn theo mô hình tham số hóa
- Chuẩn hóa dữ liệu
- Sử dụng ORM (Object-Relational Mapping)

## CÁC BIỆN PHÁP PHÒNG CHỐNG Ở MỨC ĐỘ NỀN TẢNG

- Các biện pháp bảo vệ tức thời
- Các ứng dụng tường lửa Web (WAF)
- Sử dụng hệ thống phát hiện xâm nhập

# 2

TRIỂN KHAI VÀ KẾT QUẢ ĐẠT  
ĐƯỢC



# XÂY DỰNG BỘ LỌC CÂU LỆNH SQL

## BƯỚC 1

Xử lý dữ liệu đầu vào. Dữ liệu đầu vào ở đây là dữ liệu người dùng nhập vào để đăng nhập. Sẽ được gửi từ web qua bộ lọc

## BƯỚC 2

Kiểm tra địa chỉ ip của người dùng có nằm trong danh sách đen hay không sau đó, lọc dữ liệu so sánh dữ liệu người dùng với list từ khóa nguy hiểm .

## BƯỚC 3

Đây là quá trình kiểm tra tính đúng đắn của câu truy vấn được gửi đến máy chủ cơ sở dữ liệu. Nếu câu truy vấn là đúng đắn nó sẽ được gửi đến máy chủ cơ sở dữ liệu để thực hiện ngược lại nó sẽ bị loại bỏ và gây ra lỗi máy chủ không hồi đáp phía máy chủ ứng dụng web.

# XÂY DỰNG MÔ ĐUN PROXY



Mô đun proxy giữ chức năng chặn gói tin chuyển từ máy chủ ứng dụng web sang máy chủ cơ sở dữ liệu sau đó chuẩn hóa lại dữ liệu làm đầu vào cho các mô đun kiểm tra.

Mô đun thực hiện một số chức năng sau:

- Lọc các từ khóa nguy hiểm trong form đăng nhập
- Kiểm tra xem tên người dùng hoặc mật khẩu có chứa từ khóa nguy hiểm nào không.
- Lưu trữ địa chỉ IP và thời gian hiện tại khi đăng nhập

# KẾT QUẢ ĐẠT ĐƯỢC



## QUẢN LÝ NHÂN VIÊN

NHÂN VIÊN    ĐIỂM DANH    TIỀN LƯƠNG    LỊCH CÔNG TÁC    BÁO CÁO    SỰ KIỆN    Tài Khoản ▾

Họ và tên	Giới tính	Ngày sinh	Số điện thoại	Địa chỉ	Chức vụ
Hồ Như Phong	Nam	2002-08-08	388202337	87 Nguyễn Lương Bằng	Trưởng phòng nhân sự
Trần Huy	Nam	2002-12-09	356789009	89 Đồng Kè, Hòa Khánh Bắc	Nhân viên maketing
Dương Trí Đức	Nam	2004-09-05	344234333	23 Âu cơ, Hòa Khánh Bắc	Nhân viên tiếp thị
Nguyễn Văn A	Nam	2023-12-05	889927272	01, Ngô Văn Sở	Nhân viên thu ngân
Nguyễn Thị B	Nữ	2002-07-05	889933372	01, Ngô Thị Nhậm	Nhân viên tư vấn
Nguyễn Văn A	Nam	2004-03-03	889927272	01, Ngô Văn Sở	Nhân viên bán hàng
Nguyễn Ngọc B	Nữ	2003-06-05	889927272	01, Ngô Văn Sở	Nhân viên bán hàng
Nguyễn Thị N	Nữ	2002-11-05	889927272	01, Ngô Văn Sở	Nhân viên bán hàng
Nguyễn Văn E	Nam	2005-12-05	889927272	01, Ngô Văn Sở	Nhân viên bán hàng
Nguyễn Văn D	Nam	2007-10-06	889927272	01, Ngô Văn Sở	Nhân viên bán hàng
Nguyễn Văn C	Nam	2002-12-08	889927272	01, Ngô Văn Sở	Nhân viên bán hàng
Nguyễn Văn B	Nam	2003-09-05	889927272	01, Ngô Văn Sở	Nhân viên thu ngân

Giao diện quản lý



Mô phỏng tấn công chèn mã



Phát hiện và chặn tấn công khi đăng nhập

```
proxy_server.py login_ip.txt login_log.txt  
login_ip.txt  
46 2023-12-05 16:00:53 - IP Address: 127.0.0.1  
47 2023-12-05 16:01:08 - IP Address: 127.0.0.1  
48 2023-12-05 16:01:22 - IP Address: 127.0.0.1  
49 2023-12-05 16:01:26 - IP Address: 127.0.0.1  
50 2023-12-05 16:02:02 - IP Address: 127.0.0.1  
51 2023-12-05 16:02:05 - IP Address: 127.0.0.1  
52 2023-12-05 16:14:43 - IP Address: 127.0.0.1  
53 2023-12-05 16:14:46 - IP Address: 127.0.0.1  
54 2023-12-05 16:14:47 - IP Address: 127.0.0.1  
55 2023-12-05 16:14:51 - IP Address: 127.0.0.1  
56 2023-12-05 16:16:31 - IP Address: 127.0.0.1  
57 2023-12-05 16:16:36 - IP Address: 127.0.0.1  
58 2023-12-05 16:16:42 - IP Address: 127.0.0.1  
59 2023-12-05 16:21:33 - IP Address: 127.0.0.1  
60 2023-12-05 16:21:42 - IP Address: 192.168.1.11  
61 2023-12-05 16:21:45 - IP Address: 192.168.1.6  
62 A
```

Danh sách địa chỉ ip và thời gian đăng nhập

```
E: > proxy > login_log.txt  
1 127.0.0.1  
2
```

Danh sách địa chỉ ip bị chặn

# 3

## KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

NHẬN XÉT VỀ KẾT QUẢ ĐẠT ĐƯỢC VÀ  
HƯỚNG PHÁT TRIỂN



# KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

## KẾT QUẢ ĐẠT ĐƯỢC

- Đồ án trình bày được khái quát về tấn công chèn mã SQL, chi tiết về cơ chế và các dạng tấn công chèn mã SQL.
- Đưa ra các biện pháp phát hiện và ngăn chặn tấn công chèn mã SQL.
- Xây dựng và thử nghiệm thành công bộ lọc cơ sở dữ liệu sử dụng trong phát hiện tấn công chèn mã.

## HẠN CHẾ

- Chỉ mới triển khai được trên một mô hình nhỏ, chưa thể mở rộng mô hình.
- Chưa đáp ứng được đầy đủ điều kiện yêu cầu.
- Chương trình cần được tối ưu hóa để tận dụng tối đa hiệu năng của hệ thống phần cứng máy tính và mạng.

## HƯỚNG PHÁT TRIỂN

- Tiếp tục thử nghiệm bộ lọc trên với nhiều ứng dụng web cùng kết nối đến một máy chủ cơ sở dữ liệu.
- Sử dụng phương pháp học truy vấn cho ứng dụng để khả năng phát hiện tấn công chèn mã của ứng dụng đạt hiệu quả cao nhất.

Thank You

