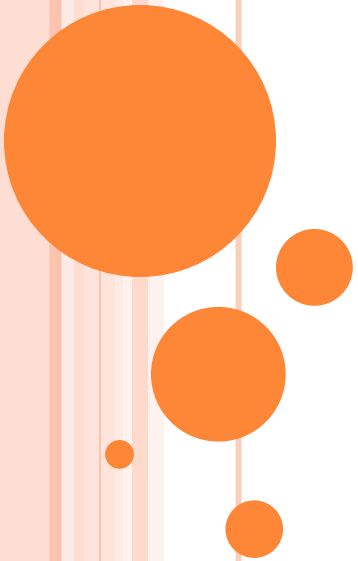
HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

CHƯƠNG 4: AN TOÀN ỨNG DỤNG



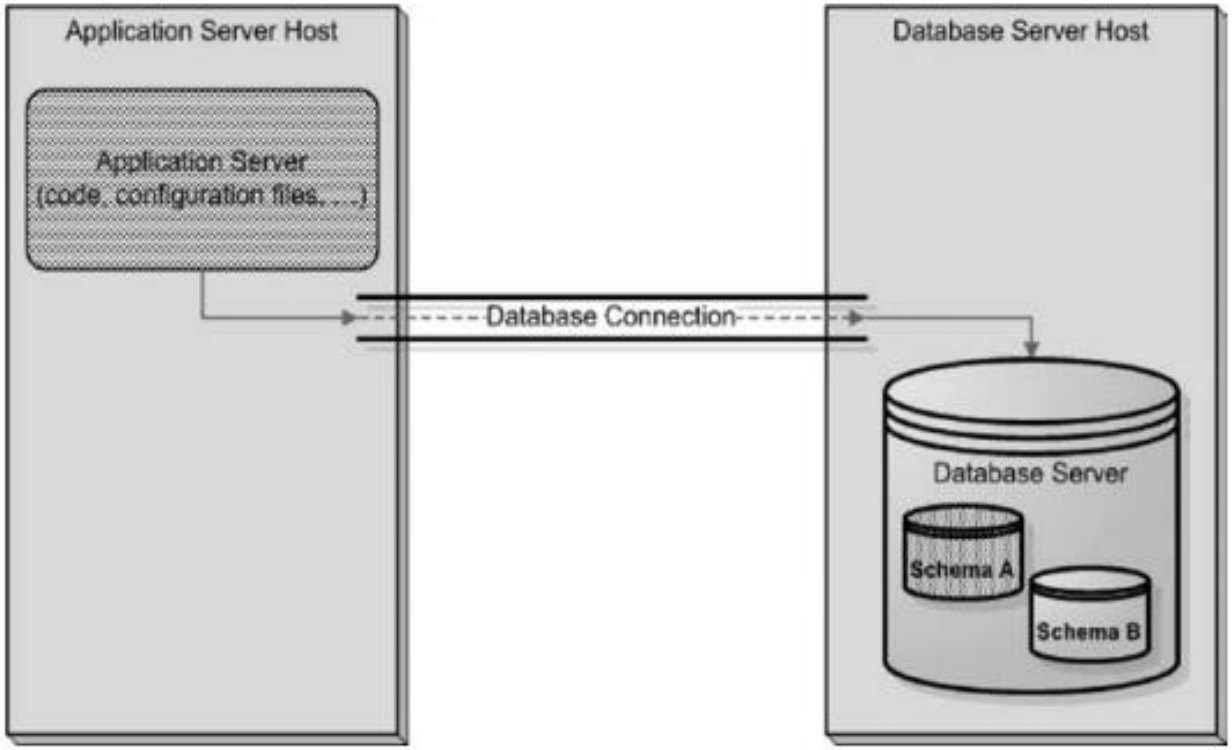
Giảng viên: TS. Trần Thị Lượng

Giới thiệu

- Mục đích của an toàn ứng dụng chính là đảm bảo an toàn cho dữ liệu của ứng dụng, như: dữ liệu tài chính, hồ sơ bệnh nhân, và thông tin khách hàng, v.v.
- Việc đảm bảo an toàn cho dữ liệu của ứng dụng thực chất là đảm bảo an toàn cho việc truy nhập vào cơ sở dữ liệu

GIỚI THIỆU

Mô hình ứng dụng cơ sở dữ liệu



VẤN ĐỀ QUẢN LÝ TÀI KHOẢN VÀ MẬT KHẨU NGƯỜI DÙNG

- **Lỗ hổng trong quản lý mật khẩu cơ sở dữ liệu:**
  - Lỗ hổng này đề cập đến vấn đề tên và mật khẩu của cơ sở dữ liệu được sử dụng và lưu trữ không an toàn: thường là do tên và mật khẩu được lưu trữ dưới dạng rõ trong tệp cấu hình
  - Đây là một lỗ hổng bảo mật nghiêm trọng vì định danh được sử dụng bằng ứng dụng để truy nhập vào trong cơ sở dữ liệu thường có toàn quyền đối với lược đồ cơ sở dữ liệu, thậm chí là toàn quyền với cơ sở dữ liệu.

VẤN ĐỀ QUẢN LÝ TÀI KHOẢN VÀ MẬT KHẨU NGƯỜI DÙNG

- **Kiểm soát việc truy nhập vào CSDL:**
  - Giám sát xem ai đang truy nhập vào dữ liệu. Bắt đầu bằng việc tạo báo cáo về các tải khoản nào đang hoạt động, tài khoản đó đang dùng địa chỉ IP nào kết nối tới CSDL, và ứng dụng nào được dùng để truy nhập vào CSDL.
  - Tăng cường an toàn bằng sử dụng tường lửa:

VẤN ĐỀ QUẢN LÝ TÀI KHOẢN VÀ MẬT KHẨU NGƯỜI DÙNG

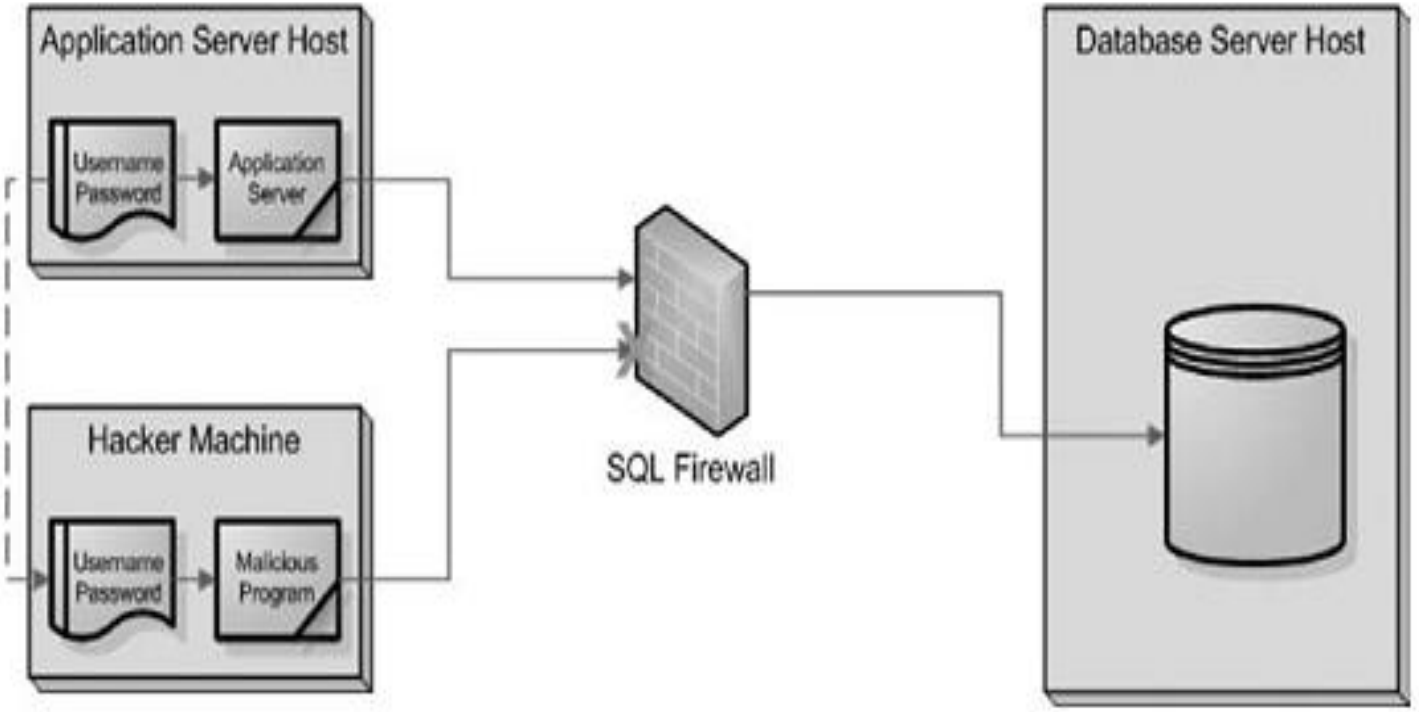
- Tăng cường an toàn bằng sử dụng tường lửa:

(1) Sử dụng tường lửa chuẩn, cho phép thực hiện kiểm soát truy nhập dựa trên IP và Port;

(2) Sử dụng tường lửa SQL, cho phép việc xây dựng các tập luật không chỉ dựa trên IP mà còn dựa trên tên truy nhập, ứng dụng truy nhập, đối tượng CSDL được truy nhập. Nó cũng cho phép xác định chính xác tài khoản nào hay ứng dụng nào, máy tính nào được phép truy nhập vào CSDL.

VẤN ĐỀ QUẢN LÝ TÀI KHOẢN VÀ MẬT KHẨU NGƯỜI DÙNG

Sử dụng một tường lửa SQL giữa ứng dụng và cơ sở dữ liệu



XÁO TRỘN MÃ ỨNG DỤNG

- Một loại lỗ hổng bảo mật trong ứng dụng phổ biến ngày nay là mã nguồn ứng dụng thường quá lộ liễu, dễ tiếp cận.
- Tùy thuộc vào ngôn ngữ lập trình được sử dụng để viết nên ứng dụng, một kẻ tấn công có thể trích xuất mã nguồn để phát hiện xem làm thế nào để ứng dụng đó có thể truy nhập vào cơ sở dữ liệu.

=> Một phương pháp để hạn chế các tấn công khai thác lỗ hổng dựa trên phân tích mã nguồn là sử dụng các kỹ thuật mã hóa ứng dụng gồm:

- *Mã hóa giao diện*
- *Mã hóa dữ liệu*

TẤN CÔNG SQL INJECTION

- SQL injection là một kĩ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng trong việc kiểm tra dữ liệu nhập trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu để "tiêm vào" (inject) và thi hành các câu lệnh SQL bất hợp pháp (không được người phát triển ứng dụng lường trước).
- Sql injection có thể cho phép những kẻ tấn công thực hiện các thao tác: delete, insert, update,… trên cơ sở dữ liệu của ứng dụng, thậm chí là máy chủ mà ứng dụng

Tấn công SQL injection

- Hậu quả của loại tấn công này là rất nghiêm trọng vì nó cho phép những kẻ tấn công có thể thực hiện các thao tác xóa, hiệu chỉnh, hoặc có toàn quyền trên cơ sở dữ liệu của ứng dụng, thậm chí là máy chủ mà ứng dụng đó đang chạy.
- Lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như: SQL Sever, My SQL, Oracle, DB2, Sysbase...

Tấn công SQL injection

- Một số cách phòng tránh SQL Injection như:
  - Giới hạn quyền người dùng
  - Loại bỏ dấu, ký tự đặc biệt như : ‘ :’, ‘--‘, ‘/’,...
  - Giới hạn những Textbox và Input
  - Mã hóa cơ sở dữ liệu ở các trường hoặc các bản ghi quan trọng.
  - + ...

Lỗ hổng tràn bộ đệm

- SV tham khảo trong giáo trình…