ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN THANH LIÊM

CHỐNG TẤN CÔNG TIÊM NHIỄM SQL SỬ DỤNG CÁC KHUÔN MẪU HỢP LỆ THEO BỐI CẢNH

Ngành: Công nghệ Thông tin

Chuyên ngành: Truyền dữ liệu và Mạng máy tính

Mã số: Chuyên ngành đào tạo thí điểm

TÓM TẮT LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Hà Nội - Năm 2017

TÓM TẮT LUẬN VĂN THẠC SĨ

Đề tài: Chống tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh

Tác giả luận văn: Nguyễn Thanh Liêm..... Khóa 21

Người hướng dẫn: TS. Nguyễn Đại Thọ.....

Từ khóa: SQL injection, SDriver, Chống tấn công tiêm nhiễm SQL .....

Tóm tắt: Luận văn giới thiệu tổng quan về tấn công tiêm nhiễm SQL, cách thức tấn công và phương pháp ngăn chặn. Nghiên cứu kỹ thuật chống tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh, SDriver. Chỉ ra được vấn đề còn tồn tại của SDriver và đưa ra được đề xuất cải tiến.

1. Lý do chọn đề tài.

Tiêm nhiễm SQL 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 nhiễm (inject) và thi hành các câu lệnh SQL trái phép (không được người phát triển ứng dụng lường trước). Hậu quả của nó rất tai hại vì nó cho phép những kẻ tấn công có thể thực hiện các thao tác xóa, hiệu chỉnh, … do có toàn quyền trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy. Đã có nhiều kỹ thuật ngăn chặn tấn công tiêm nhiễm SQL được giới thiệu. Trong đó, kỹ thuật chông tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh, SDriver, là kỹ thuật ngăn chặn đơn giản, hiệu quả và chi phí triển khai thấp. Tuy vậy, SDriver vẫn tồn tại những vấn đề cần được khắc phục. Tuy vậy phương pháp này vẫn tồn tại vấn đề khiến kẻ tấn công có thể tiêm nhiễm thành công.

Xuất phát từ thực tế đó, luận văn tập trung nghiên cứu*: "Chống tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh".*

2. Mục tiêu nghiên cứu của đề tài.

Tìm hiểu tấn công tiêm nhiễm SQL, cách thức tấn công và phương pháp ngăn chặn.

Tìm hiểu kỹ thuật chống tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh, SDriver.

Phân tích hoạt động của SDriver và chỉ ra được vấn đề còn tồn tại của SDriver.

Đưa ra được đề xuất cải tiến.

Chạy mô phỏng đề xuất và đánh giá.

3. Đối tượng và phạm vi nghiên cứu.

Đối tượng nghiên cứu: Kỹ thuật chống tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh, SDriver.

Phạm vi nghiên cứu: Cách thức tấn công tiêm nhiễm SQL và các phương pháp ngăn chặn.

4. Nội dung chính

CHƯƠNG 1 TỔNG QUAN VỀ TẤN CÔNG TIÊM NHIỄM SQL VÀ CÁC PHƯƠNG PHÁP PHÒNG CHỐNG.

Nội dung toàn chương 1 đã nêu lên được các kiến thức cơ bản về Tấn công tiêm nhiễm SQL, khái niệm về Tấn công tiêm nhiễm SQL, các cách thức của Tấn công tiêm nhiễm SQL và các phương pháp ngăn chặn Tấn công tiêm nhiễm SQL.

1.1. Khái niệm tấn công tiêm nhiễm SQL.

Tấn công tiêm nhiễm SQL là một dạng tấn công tiêm nhiễm mã độc mà kẻ tấn công sẽ cố gắng khai thác lỗ hổng của chính ứng dụng web để tiến hành tiêm nhiễm mã độc vào câu truy vấn SQL của ứng dụng web nhằm truy cập trái phép vào cơ sở dữ liệu đằng sau ứng dụng web.

Tấn công tiêm nhiễm SQL vô cùng nguy hiểm vì kẻ tấn công không chỉ có thể ăn cắp được dữ liệu chứa thông tin nhạy cảm mà chúng còn có thể thay đổi dữ liệu, thậm chí là kiểm soát cả máy chủ mà CSDL đang chạy. Tấn công tiêm nhiễm SQL xảy ra trên các hệ quản trị CSDL quan hệ như MySQL, MS SQL, DB2, Oracle…

1.2. Phân loại tấn công tiêm nhiễm SQL.

Tấn công tiêm nhiễm SQL có thể phân loại theo các tiêu chí như cơ chế tiêm nhiễm, mục đích tấn công và kỹ thuật tấn công.

Cơ chế tiêm nhiễm gồm: tiêm nhiễm thông qua nhập liệu người dùng, tiêm nhiễm thông qua cookies, tiêm nhiễm second-order.

Mục đích tấn công của kẻ tấn công có thể là xác định các tham số có thể tiêm nhiễm, thực hiện tìm vết CSDL, xác định lược đồ CSDL, trích xuất dữ liệu, thêm hoặc thay đổi dữ liệu, thực hiện từ chối dịch vụ, Tránh né phát hiện, vượt qua xác thực, thực thi câu lệnh từ xa, thực hiện leo thang đặc quyền.

Kỹ thuật tấn công phổ biến gồm: tautologies, chú thích cuối dòng, truy vấn Union, truy vấn Piggy-Backed, suy luận.

1.3. Các phương pháp ngăn chặn tấn công tiêm nhiễm SQL.

Các phương pháp ngăn chặn chủ yếu gồm mã phòng thủ và phát hiện và ngăn chặn.

Phương pháp mã phỏng thủ có một số kỹ thuật điển hình sau: thực hành mã phòng thủ, tham số hóa truy vấn, SQL DOM.

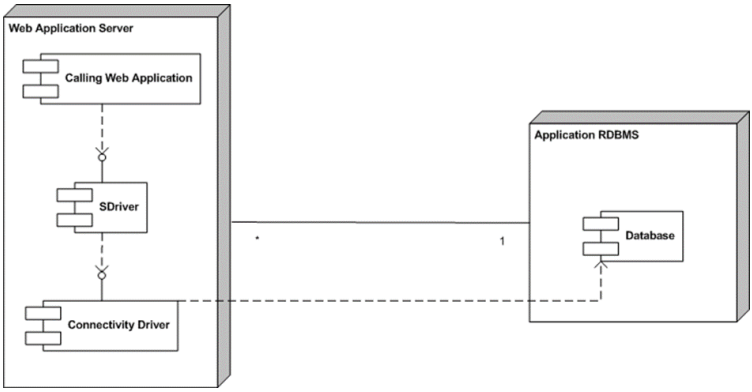
Phương pháp phát hiện và ngăn chặn được phân thành 3 loại sau: signature based, anomaly based, code analysis.

CHƯƠNG 2 PHƯƠNG PHÁP SDRIVER TRONG CHỐNG TẤN CÔNG TIÊM NHIỄM SQL

2.1. Phương pháp chống tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh, SDriver.

SDriver là trình điều khiển được chèn vào giữa ứng dụng web và trình điều khiển kết nối. Bản thân SDriver không phải là một trình điều khiển kết nối mà nó đóng vai trò như một bộ lọc.

Kiến trúc của SDriver:

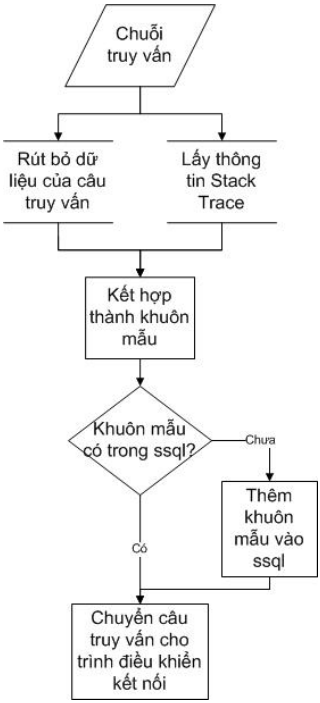


Hình 2.1 – Kiến trúc đề xuất của SDriver

2.2. Cách thức hoạt động của SDriver.

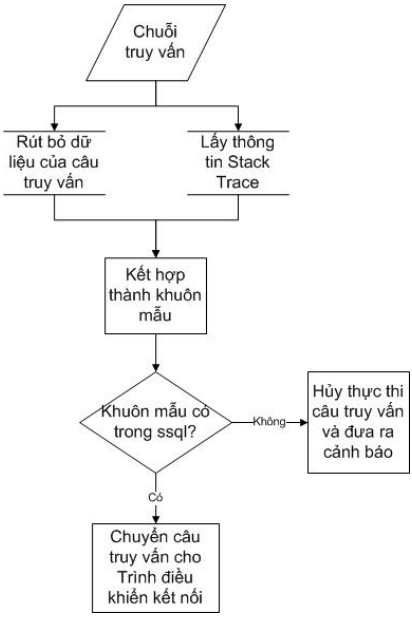
SDriver có hai chế độ hoạt động là chế độ huấn luyện và chế độ thực thi. Trong chế độ huấn luyện, SDriver sẽ xây dựng CSDL về các khuôn mẫu hợp lệ. Trong chế độ thực thi, SDriver sẽ đóng vai trò phát hiện và ngăn chặn tấn công tiêm nhiễm SQL.

Chế độ huấn luyện:



Hình 2.2 – Chế độ huấn luyện của SDriver

Chế độ thực thi:



Hình 2.3 – Chế độ thực thi của SDriver

SDriver sẽ rút bỏ dữ liệu của câu truy vấn và thu thập thông tin về stack strace của câu truy vấn. Kết hợp hai đặc trưng trên sẽ thu được khuôn mẫu hợp lệ tương ứng của câu truy vấn.

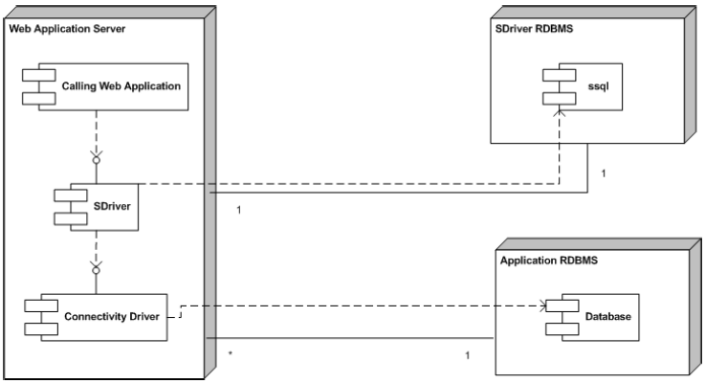
2.3. Stack trace.

Stack trace gồm thông tin chi tiết về tất cả phương thức và vị trí gọi (vị trí dòng lệnh), từ phương thức của ứng dụng nơi câu truy vấn được thực thi cho đến phương thức mục tiêu của trình điều khiển kết nối. Mỗi câu truy vấn sẽ có thông tin về stack trace riêng biệt.

Stack trace khiến việc giả mạo câu truy vấn hợp lệ trở nên khó khăn.

2.4. Mô phỏng hoạt động của SDriver.

Môi trường mô phỏng: ứng dụng web được sử dụng để mô phỏng được xây dựng trên nền tản JSP & Servlet. Sử dụng Eclipse để biên dịch và chạy ứng dụng web, máy chủ web là tomcat 8.0, CSDL là MySQL 5.7.



Hình 2.5 – Kiến trúc thực tế của SDriver.

Chế độ huấn luyện: SDriver tiếp nhận các câu truy vấn từ ứng dụng web, thu thập thông tin stack trace và rút bỏ dữ liệu của câu truy vấn. Kết hợp hai đặc trưng trên của câu truy vấn và sử dụng hàm băm MD5 để tạo ra khuôn mẫu hợp lệ tương ứng. Nếu trong CSDL ssql chưa có khuôn mẫu hợp lệ tương ứng với câu truy vấn thì tiến hành chèn vào ssql, nếu đã có thì không thực hiện gì.

Chế độ thực thi: Tương tự như ở chế độ huấn luyện, chỉ khác biệt ở chỗ nếu không tìm thấy khuôn mẫu hợp lệ tương ứng với câu truy vấn thì SDriver sẽ coi câu truy vấn là độc hại và ngăn chặn, nếu tìm thấy khuôn mẫu hợp lệ tương ứng thì

SDriver sẽ chuyển tiếp câu truy vấn cho trình điều khiển kết nối.

Thử nghiệm một số kỹ thuật tấn công tiêm nhiễm SQL để quan sát. Các cuộc tấn công đều bị phát hiện và ngăn chặn.

CHƯƠNG 3 ĐỀ XUẤT CẢI TIẾN CHỐNG TẤN CÔNG TIÊM NHIỄM SQL SỬ DỤNG KHUÔN MẪU HỢP LỆ THEO BỐI CẢNH

3.1. Phân tích hoạt động của SDriver.

Cũng giống như các kỹ thuật chống tấn công tiêm nhiễm SQL sử dụng khuôn mẫu hợp lệ khác, SDriver cần phải trích xuất ra được các đặc trưng của câu truy vấn. Trong SDriver thì đặc trưng của câu truy vấn gồm có thông tin về stack trace và câu truy vấn rút bỏ dữ liệu. Trong quá trình rút bỏ dữ liệu của câu truy vấn, SDriver có thể để lọt mã độc. Kẻ tấn công có thể lợi dụng lỗ hổng này tiêm nhiễm SQL.

Một vài ví dụ về kỹ thuật tấn công tiêm nhiễm SQL lợi dụng lỗ hổng của SDriver. Các cuộc tấn công đều vượt qua được SDriver.

3.2. Đề xuất cải tiến.

Các ký tự thông thường hay chuỗi chú thích cũng có thể coi là những đặc trưng riêng của câu truy vấn, bản thân chúng mang phong cách lập trình riêng của nhà phát triển.

Khi loại bỏ các chuỗi đầu vào nằm trong cặp ngoặc đơn thì thay thế bằng một ký tự đặc biệt. Tác dụng của điều này là xác định vị trí và số lượng của chuỗi bị xóa bỏ. Bất kỳ sự khác

biệt nào về vị trí, số lượng chuỗi bị xóa bỏ giữa câu truy vấn được gửi từ ứng dụng web với khuôn mẫu hợp lệ đều sẽ được coi là câu truy vấn độc hại, trong chế độ thực thi của SDriver.

Chuỗi đầu vào sau khi bị loại bỏ vẫn sẽ phải trải qua một lần kiểm tra mã độc để đảm bảo không bỏ lọt mã độc.

CHƯƠNG 4 KẾT QUẢ THỰC NGHIỆM ĐÁNH GIÁ.

4.1. Mô phỏng thực nghiệm SDriver với cơ chế rút bỏ dữ liệu mới.

Môi trường thử nghiệm hoạt động của SDriver đề xuất như sau:

Các bước chạy mô phỏng thực nghiệm:

1. Đặt chế độ hoạt động của SDriver là huấn luyện. Chuyển dòng đầu tiên của file mode.txt thành "training mode".
2. Lần lượt thực thi các câu truy vấn bằng cách chạy các chức năng của ứng dụng web. Tiến hành quan sát các câu truy vấn được rút bỏ dữ liệu.
3. Khi toàn bộ câu truy vấn đã có được khuôn mẫu hợp lệ tương ứng trong CSDL ssql thì dừng chế độ huấn luyện.
4. Chuyển chế độ hoạt động của SDriver sang thực thi. Chuyển dòng đầu tiên của file mode.txt thành "production mode".

5. Lần lượt thực thi các câu truy vấn bằng đầu vào hợp lệ. Tiến hành quan sát kết quả.
6. Lần lượt thử nghiệm các kỹ thuật tấn công đã vượt qua được SDriver. Quan sát kết quả.

4.2. Đánh giá hoạt động của SDriver đề xuất

Đánh giá SDriver đề xuất theo hai tiêu chí là hiệu năng và độ chính xác.

Đánh giá hiệu năng của hệ thống:

Bảng 4.1 Thời gian thực thi truy vấn của 2 phiên bản SDriver.

Chế độ	SDriver cũ (ms)	SDriver đề xuất (ms)	Tỷ lệ mới/cũ (%)
Huấn luyện	15.9375	15.5625	97.64706
Thực thi	3.8125	4.3125	113.1148

Bảng 4.1 trên thể hiện thời gian thực thi câu truy vấn, đơn vị mili giây (ms), của SDriver cũ và SDriver đề xuất ở cả hai chế độ huấn luyện và thực thi. Cột "Tỷ lệ mới/cũ" thể hiện so sánh tỷ lệ thời gian thực thi câu truy vấn của SDriver đề xuất với SDriver cũ.

Đánh giá độ chính xác:

Sử dụng hai cách thức đánh giá là đánh giá bằng công cụ sqlmap và đánh giá qua trang web thực tế.

Công cụ sqlmap: cả SDriver cũ và SDriver đề xuất đều phát hiện và ngăn chặn thành công các cuộc tấn công tiêm nhiễm SQL.

Bảng 4.2 Kết quả ngăn chặn tấn công tiêm nhiễm SQL.

Ứng dụng web	Tấn công tiêm nhiễm SQL	SDriver cũ		SDriver đề xuất	
		Ngăn chặn	Tỷ lệ (%)	Ngăn chặn	Tỷ lệ (%)
EMusic	110	101	91,8 %	110	100%
Book store	130	124	95,4 %	130	100%
Document Manager System	151	145	96%	151	100%

Bảng 4.2 trên đây thể hiện kết quả phát hiện và ngăn chặn tấn công tiêm nhiễm SQL của SDriver cũ và SDriver đề xuất. Cột "tấn công tiêm nhiễm SQL" thể hiện số cuộc tấn công đã được thực hiện. Cột "ngăn chặn" thể hiện số cuộc tấn công mà SDriver ngăn chặn thành công, cột "tỷ lệ" là tỷ lệ % ngăn chặn thành công.

5. Phương pháp nghiên cứu

Nghiên cứu lý thuyết, tiến hành mô phỏng thực nghiệm để tìm kiếm vấn đề, cách giải quyết vấn đề, từ đó đưa ra được đề xuất cải tiến.

6. Kết luận và hướng phát triển tiếp theo.

Sau thời gian tìm hiểu và thực hiện đề tài: "Chống tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh". Nội dung bài luận văn đã đạt được các kết quả như sau:

- ✓ Hiểu được tổng quan về tấn công tiêm nhiễm SQL, các cách thức tấn công và các phương pháp ngăn chặn.
- ✓ Hiểu được cơ chế hoạt động của kỹ thuật chống tấn công tiêm nhiễm SQL sử dụng các khuôn mẫu hợp lệ theo bối cảnh SDriver, áp dụng thực hiện mô phỏng hoạt động của SDriver.
- ✓ Phân tích hoạt động của SDriver và tìm ra được vấn đề còn tồn tại của SDriver.
- ✓ Đưa ra được đề xuất cải tiến.
- ✓ Chạy mô phỏng SDriver với đề xuất cải tiến và đưa ra được đánh giá.

Nhìn chung, luân văn đã đạt được các mục tiêu nghiên cứu đã đề ra. Tuy nhiên luận văn vẫn cần phải đưa ra được những đánh giá có tính thuyết phục hơn, như mở rộng ứng dụng web, mở rộng số lượng câu truy vấn, thực thi các câu truy vấn có độ phức tạp cao…Hướng phát triển tiếp theo: Nội dung luận văn có thể phát triển theo các hướng sau:

- ✓ Tiếp tục nghiên cứu cải tiến hiệu năng của kỹ thuật này.
- ✓ Nghiên cứu để triển khai trên nhiều nền tảng khác nhau.