# **HỌC VIỆN KỸ THUẬT MẬT MÃ**

**KHOA AN TOÀN THÔNG TIN**

-----\*\*\*-----

A red circle with a white and yellow circle with a key and a book

Description automatically generated

**BÀI TẬP LỚN MÔN HỌC**

**AN TOÀN CƠ SỞ DỮ LIỆU**

**Tìm hiểu về tấn công leo thang đặc quyền trên Oracle và thực nghiệm**

**Giảng viên hướng dẫn:Nguyễn Thị Thu Thủy**

**Nhóm sinh viên thực hiện:**

* Tăng Hoàng Quí AT190243
* Vũ Đức Trường AT190250
* Phạm Quang Minh AT190233
* Nguyễn Hùng Cường AT190510

**HÀ NỘI 12/2024**

**MỤC LỤC**

[DANH MỤC TỪ VIẾT TẮT iv](#_Toc183274694)

[DANH MỤC HÌNH VẼ VÀ BẢNG BIỂU v](#_Toc183274695)

[Lời mở đầu vi](#_Toc183274696)

[CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN CƠ SỞ DỮ LIỆU 1](#_Toc183274697)

[1.1. Tổng quan về Cơ sở dữ liệu 1](#_Toc183274698)

[1.1.1. Khái niệm 1](#_Toc183274699)

[1.1.2.Ưu điểm của CSDL 1](#_Toc183274700)

[1.1.3. Vấn đề đặt ra 2](#_Toc183274701)

[1.2. Vai trò của an toàn cơ sở dữ liệu 2](#_Toc183274702)

[CHƯƠNG 2. TỔNG QUAN VỀ TẤN CÔNG LEO THANG ĐẶC QUYỀN 4](#_Toc183274703)

[2.1. Giới thiệu về tấn công leo thang đặc quyền 4](#_Toc183274704)

[2.2. Các dạng leo thang đặc quyền 5](#_Toc183274705)

[2.2.1. Khái quát 5](#_Toc183274706)

[2.2.2. Leo thang đặc quyền dọc 5](#_Toc183274707)

[2.2.3. Leo thang đặc quyền ngang 8](#_Toc183274708)

[2.3. Các biện pháp bảo vệ hệ thống giảm thiểu leo thang đặc quyền 9](#_Toc183274709)

[CHƯƠNG 3. TẤN CÔNG LEO THANG ĐẶC QUYỀN TRÊN ORACLE 12](#_Toc183274710)

[3.1. Giới thiệu về hệ quản trị cơ sở dữ liệu Oracle 12](#_Toc183274711)

[3.1.1. Tổng quan về hệ quản trị cơ sở dữ liệu 12](#_Toc183274712)

[3.1.2. Tổng quan về hệ quản trị cơ sở dữ liệu Oracle 13](#_Toc183274713)

[3.1.3. Ngôn ngữ PL/SQL 15](#_Toc183274714)

[3.2. Các loại tấn công leo thang đặc quyền trong Oracle 16](#_Toc183274715)

[3.2.1. PL/SQL Injection 16](#_Toc183274716)

[3.2.2. Leo thang đặc quyền DBA bằng CREATE ANY VIEW 20](#_Toc183274717)

[3.2.3. Leo thang đặc quyền DBA bằng CREATE, EXECUTE PROCEDURE 21](#_Toc183274718)

[3.2.4. Leo thang đặc quyền DBA bằng INDEX 22](#_Toc183274719)

[3.2.5. Sử dụng công cụ ODAT 23](#_Toc183274720)

[CHƯƠNG 4. THỰC NGHIỆM 25](#_Toc183274721)

[4.1. Khai thác PL/SQL Injection (19c) 25](#_Toc183274722)

[4.2. Create Index (19c) 26](#_Toc183274723)

[4.3. Create và Execute Procedure (11gR2) 27](#_Toc183274724)

[4.4. Create view (11gR2) 28](#_Toc183274725)

[KẾT LUẬN 31](#_Toc183274726)

[TÀI LIỆU THAM KHẢO 32](#_Toc183274727)

# 

# **DANH MỤC TỪ VIẾT TẮT**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Ký hiệu | Chữ viết đầy đủ | Ý nghĩa |
| 1 | CSDL |  | Cơ sở dữ liệu |
| 2 | DBA | Database Administrator | Quản trị viên cơ sở dữ liệu |
| 3 | DBMS | Database Management System | Hệ quản trị cơ sở dữ liệu |
| 4 | DDL | Data Definition Language | Ngôn ngữ định nghĩa kiểu dữ liệu |
| 5 | DML | Data Manipulation Language | Ngôn ngữ thao tác dữ liệu |
| 6 | ODAT | Oracle Database Attacking Tool | Công cụ kiểm thử xâm nhập Oracle |
| 7 | OS / HĐH | Operating System | Hệ điều hành |
| 8 | PL/SQL | Procedural Language extensions to SQL | Ngôn ngữ truy vấn theo cấu trúc hướng thủ tục |
| 9 | RDBMS | Relational Database Management System | Hệ quản trị cơ sở dữ liệu quan hệ |
| 10 | SQL | Structured Query Language | Ngôn ngữ truy vấn có cấu trúc |

# **DANH MỤC HÌNH VẼ VÀ BẢNG BIỂU**

|  |  |
| --- | --- |
| **Hình 1** Các thành phần của một CSDL | Trang 1 |
| **Hình 2** Minh họa diễn biến của leo thang đặc quyền trong Oracle | Trang 4 |
| **Hình 3** Minh họa tấn công tràn bộ đệm | Trang 6 |
| **Hình 4** Minh họa tấn công Cross Site Scripting | Trang 7 |
| **Hình 5** Minh họa tấn công Command Injection | Trang 7 |
| **Hình 6** Leo thang đặc quyền bằng CREATE ANY VIEW | Trang 13 |
| **Hình 7** Minh họa chỉ mục (INDEX) | Trang 15 |
| **Hình 8** Kiến trúc ODAT | Trang 18 |

# **Lời mở đầu**

Trong thế giới công nghệ thông tin hiện đại, bảo mật dữ liệu đã trở thành một ưu tiên hàng đầu của các tổ chức và doanh nghiệp. Hệ quản trị cơ sở dữ liệu Oracle, với vai trò là một trong những hệ thống quản trị dữ liệu được sử dụng phổ biến trên thế giới, đóng vai trò quan trọng trong việc quản lý và bảo vệ thông tin. Tuy nhiên, như bất kỳ hệ thống phần mềm phức tạp nào khác, Oracle không tránh khỏi các lỗ hổng bảo mật, trong đó đáng chú ý nhất là vấn đề leo thang đặc quyền (privilege escalation).

Có rất nhiều loại tấn công khác nhau vào cơ sở dữ liệu và chúng có thể được sử dụng kết hợp với nhau để tăng sức mạnh. Leo thang đặc quyền là một trong những phương pháp tấn công nghiêm trọng nhất, cho phép kẻ xâm nhập khai thác các lỗ hổng hoặc cấu hình sai để nâng cấp quyền truy cập của mình lên mức cao hơn so với được cấp phép, cụ thể là từ cấp độ người dùng bình thường (User) lên tới cấp độ quản trị viên (Administrator). Những cuộc tấn công này thường nhằm vào mục đích đánh cắp thông tin của các doanh nghiệp và tập đoàn, gây rủi ro lớn cho dữ liệu nhạy cảm và làm suy giảm niềm tin của người dùng vào hệ thống bảo mật của họ.

Từ những vấn đề thực tiễn nêu trên, nhóm 12 đã quyết định lựa chọn đề tài “Tìm hiểu về tấn công leo thang đặc quyền trong hệ quản trị Oracle” làm đề tài báo cáo trong môn học An toàn cơ sở dữ liệu.

Nội dung báo cáo gồm 4 phần:

Chương 1. Tổng quan về an toàn cơ sở dữ liệu

Chương 2. Tổng quan về tấn công leo thang đặc quyền

Chương 3. Tấn công leo thang đặc quyền trên Oracle

Chương 4: Thực nghiệm

Bài báo cáo này nhằm cung cấp cái nhìn tổng quan về vấn đề leo thang đặc quyền trong Oracle, từ khái niệm, cơ chế hoạt động, đến các lỗ hổng phổ biến và cách thức tấn công. Đồng thời, báo cáo cũng trình bày các phương pháp phòng chống và khuyến nghị để giảm thiểu rủi ro liên quan. Cuối cùng là thực nghiệm minh họa.

Nhóm 12 xin chân thành cảm ơn cô Nguyễn Thị Thu Thủy đã tận tình giảng dạy để nhóm có thể hoàn thành tốt đề tài báo cáo này. Mặc dù đã cố gắng, song do còn hạn chế về mặt kiến thức cũng như năng lực nên đề tài khó tránh khỏi thiếu sót và khuyết điểm. Nhóm rất mong được nhận sự thông cảm và sự đánh giá, nhận xét của cô và sự góp ý của các bạn để giúp đề tài được hoàn thiện hơn.

**Hà Nội, tháng 12 năm 2024**

**NHÓM SINH VIÊN THỰC HIỆN**

**Tăng Hoàng Quí**

**Vũ Đức Trường**

**Phạm Quang Minh**

**Vũ Hùng Cường**

# **CHƯƠNG 1. TỔNG QUAN VỀ AN TOÀN CƠ SỞ DỮ LIỆU**

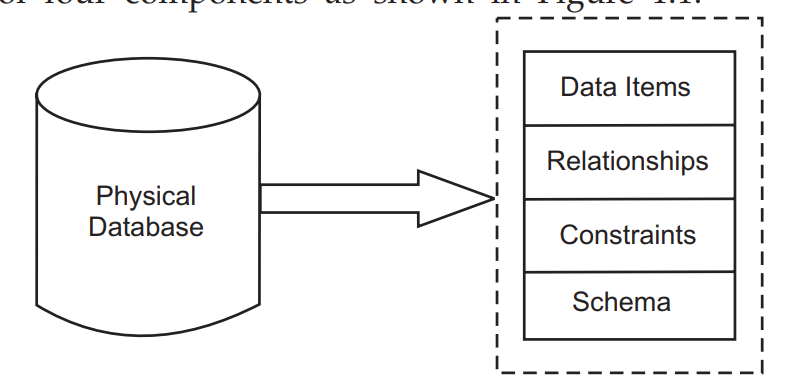
## **1.1. Tổng quan về Cơ sở dữ liệu**

### **1.1.1. Khái niệm**

*Cơ sở dữ liệu* (Database, viết tắt làCSDL) là một tập hợp các dữ liệu có cấu trúc và một tập các quy tắc tổ chức dữ liệu chỉ ra các mối quan hệ giữa chúng. Tập các dữ liệu này có mức độ dư thừa được kiểm soát để phục vụ một hay nhiều chương trình một cách tối ưu. Dữ liệu được lưu trữ sao cho chúng độc lập với các chương trình được sử dụng để truy vấn dữ liệu. CSDL cũng được định nghĩa là tập các dữ liệu có liên quan đến nhau được lưu trữ tập trung và được thiết kế để phù hợp với yêu cầu của các tổ chức và doanh nghiệp. Ngoài ra, có thể định nghĩa CSDL như một hệ thống hồ sơ điện tử.

CSDL là tập hợp các thông tin có tính chất hệ thống, không phải là các thông tin rời rạc. Các thông tin này phải có cấu trúc và tập hợp các thông tin này phải có khả năng đáp ứng nhu cầu khai thác thông tin đồng thời của nhiều người sử dụng hay nhiều chương trình ứng dụng với những mục đích khác nhau.

CSDL là dữ liệu, nhưng dữ liệu chưa chắc đã là CSDL.



**Hình 1** Các thành phần của một CSDL

### **1.1.2.Ưu điểm của CSDL**

*-* ***Tránh dư thừa, trùng lặp dữ liệu*** xuống mức thấp nhất, do đó đảm bảo được tính nhất quán và toàn vẹn dữ liệu.

- ***Đảm bảo sự độc lập* *giữa dữ liệu và chương trình ứng dụng***: Cho phép thay đổi cấu trúc, dữ liệu trong CSDL mà không cần thay đổi chương trình ứng dụng.

- ***Đảm bảo tính an toàn và bảo mật dữ liệu***: Trừu tượng hóa dữ liệu (Data Abstraction) là một nguyên tắc của lý thuyết mô hình hóa dữ liệu, nhằm ẩn lưu trữ vật lý chi tiết của dữ liệu, chỉ biểu diễn mức khái niệm của CSDL.

- ***Đa khung nhìn* *(multi-view)****:* Đảm bảo dữ liệu có thể được truy xuất theo nhiều cách khác nhau vì nhu cầu của mỗi đối tượng sử dụng CSDL là khác nhau.

- ***Đa người dùng* *(multi-user)****:* Khả năng chia sẻ thông tin cho nhiều người sử dụng và nhiều ứng dụng khác nhau một cách đồng thời.

### **1.1.3. Vấn đề đặt ra**

Do tính chia sẻ và có nhiều người được phép truy cập, khai thác CSDL với những mục đích khác nhau, CSDL đặt ra những vấn đề cần giải quyết để phát huy tối đa được các ưu điểm trên của mình. Đó là:

- ***Tính chủ quyền của dữ liệu***: Chủ quyền của CSDL dễ bị xâm phạm.

- ***Tính bảo mật và quyền khai thác thông tin của người sử dụng***: Cần có cơ chế bảo mật và phân quyền hạn khai thác CSDL.

- ***Tranh chấp dữ liệu***: Cần có cơ chế ưu tiên truy cập dữ liệu hoặc giải quyết tình trạng xung đột trong quá trình khai thác cạnh tranh. Cơ chế ưu tiên có thể được thực hiện bằng việc cấp quyền (hay mức độ) ưu tiên cho từng người khai thác.

-***Đảm bảo dữ liệu khi có sự cố***: Việc quản lý dữ liệu tập trung có thể làm tăng nguy cơ mất mát hoặc sai lệnh thông tin khi có sự cố mất điện đột xuất hoặc đĩa lưu trữ bị hỏng. Nên cần có cơ chế khôi phục dữ liệu khi sự cố xảy ra.

## **1.2. Vai trò của an toàn cơ sở dữ liệu**

Hơn hai thập kỷ gần đây, sự phát triển vượt bậc cả về số lượng lẫn chất lượng của các ứng dụng dựa trên CDSL đã khiến chúng ngày càng đóng vai trò quan trọng trong hoạt động của tổ chức, doanh nghiệp hay cá nhân. Ở thời đại thế giới phẳng, khi mà ai cũng có thể tiếp cận với tin tức toàn cầu, việc sở hữu dữ liệu đã là vấn đề sống còn của các doanh nghiệp trong việc phân tích chiến lược thị trường và từ đây việc bảo mật thông tin lại càng trở nên quan trọng và cấp bách hơn.

Tin tặc (hacker) đã không còn tấn công chỉ để thỏa mãn sự tò mò, hay chỉ để gia tăng danh tiếng, khẳng định bản thân. Nó đã trở thành một ngành công nghiệp thực sự. Tin tặc được trả tiền hậu hĩnh cho việc ăn cắp và bán đi những thông tin độc quyền. Trong thời đại Big Data, quyền truy cập thông tin là một yếu tố thay đổi cuộc chơi và người nắm được thông tin mới có tính bảo mật cao là người làm chủ. CSDL rất dễ bị tấn công bởi thông tin trên CSDL luôn được thể hiện ở dạng bản rõ, còn những thông tin truyền theo đường truyền thì lại bị mã hóa bằng nhiều thuật toán phức tạp. Không chỉ thế, các CSDL còn tồn tại nhiều vấn đề bảo mật như: quản trị mật khẩu kém, không cập nhật thường xuyên các chương trình phần mềm hiện đại, cấu hình CSDL không đạt tiêu chuẩn hay duy trì các plug-in dưới quyền sử dụng hoặc không được sử dụng,.....

Do đó, việc bảo mật CSDL là vô cùng cần thiết, nhằm mục đích:

- ***Bảo vệ dữ liệu khỏi truy cập trái phép***: Đảm bảo rằng chỉ những người hoặc hệ thống được ủy quyền mới có thể truy cập, sửa đổi hoặc xóa dữ liệu.

- ***Đảm bảo tính toàn vẹn của dữ liệu***: Đảm bảo dữ liệu luôn chính xác và đáng tin cậy trong mọi tình huống.

- ***Duy trì tính sẵn sàng của dữ liệu***: Đảm bảo hệ thống cơ sở dữ liệu luôn hoạt động, cung cấp dữ liệu một cách liên tục và không bị gián đoạn. Phòng tránh các cuộc tấn công gây từ chối dịch vụ (DDoS) hoặc các lỗi hệ thống khiến cơ sở dữ liệu không khả dụng.

-***Ngăn chặn đe dọa nội bộ***: Giảm thiểu rủi ro từ các nhân viên, nhà quản trị hệ thống hoặc người dùng nội bộ có thể lợi dụng quyền hạn để xâm phạm dữ liệu.

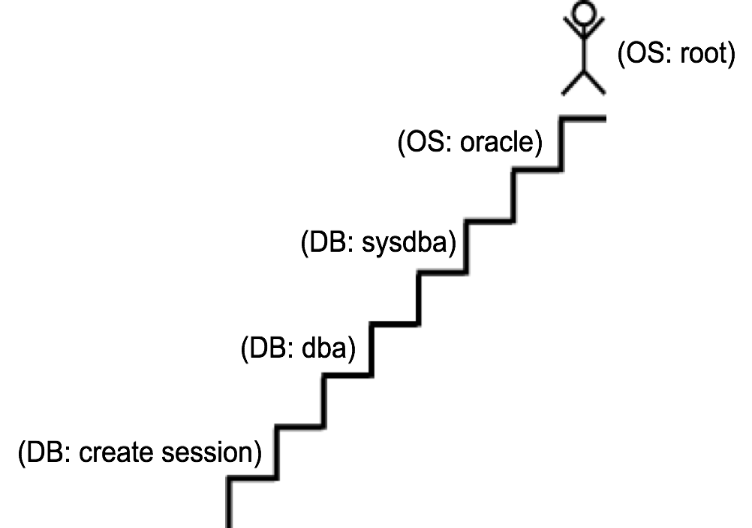
- ***Xây dựng niềm tin cho người dùng và tổ chức***: Tăng cường uy tín của tổ chức bằng cách đảm bảo dữ liệu khách hàng và doanh nghiệp được bảo vệ an toàn.

# **CHƯƠNG 2. TỔNG QUAN VỀ TẤN CÔNG LEO THANG ĐẶC QUYỀN**

## **2.1. Giới thiệu về tấn công leo thang đặc quyền**

*Leo thang đặc quyền*(Escalating Privilege) về cơ bản có định nghĩa là thêm nhiều quyền hơn hoặc cho phép một tài khoản người dùng thêm quyền. Ở mức độ cao nhất, leo thang đặc quyền làm cho một tài khoản người dùng có quyền như là tài khoản quản trị.

Các tài khoản quản trị viên thường có yêu cầu mật khẩu nghiêm ngặt hơn, và mật khẩu của họ được bảo vệ chặt chẽ hơn. Nếu không thể tìm thấy một tên người dùng và mật khẩu của một tài khoản với quyền quản trị viên, một hacker có thể chọn sử dụng một tài khoản với quyền thấp hơn. Tại trường hợp này, các hacker sau đó phải leo thang đặc quyền để có nhiều quyền như quyền của quản trị.

Một khi tin tặc đã có thể truy cập tài khoản với quyền quản trị, điều tiếp theo cần làm là thực thi các ứng dụng trên hệ thống đích. Mục tiêu của việc thực thi ứng dụng có thể cài đặt một cửa sau trên hệ thống, cài đặt một keylogger để thu thập thông tin bí mật, sao chép các tập tin, hoặc chỉ gây thiệt hại cơ bản cho hệ thống, bất cứ điều gì hacker muốn làm trên hệ thống. Lúc này, hacker có thể thực thi các ứng dụng, họ có thể chiếm toàn quyền trên hệ thống hệ thống. Vì vậy vấn đề về leo thang đặc quyền là rất quan trọng.

**Hình 2** Minh họa diễn biến của leo thang đặc quyền trong Oracle

## **2.2. Các dạng leo thang đặc quyền**

### **2.2.1. Khái quát**

Kẻ tấn công bắt đầu bằng cách khai thác lỗ hổng leo thang đặc quyền trong một hệ thống hoặc ứng dụng mục tiêu, cho phép chúng ghi đè các giới hạn của tài khoản người dùng hiện tại. Sau đó, họ có thể truy cập chức năng và dữ liệu của người dùng khác *(leo thang đặc quyền ngang)* hoặc có được các đặc quyền nâng cao, thường là của quản trị viên hệ thống hoặc người dùng quyền lực khác *(leo thang đặc quyền dọc)*. Sự leo thang đặc quyền như vậy thường chỉ là một trong những bước được thực hiện để chuẩn bị cho cuộc tấn công chính.

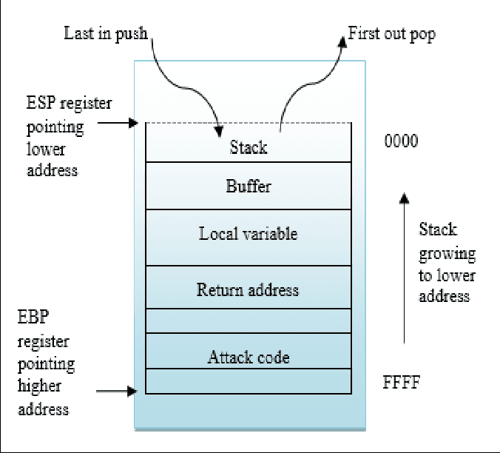
### **2.2.2. Leo thang đặc quyền dọc**

*Leo thang đặc quyền dọc*(Vertical privilige escalation) còn gọi là độ cao đặc quyền, trong đó người dùng hoặc ứng dụng đặc quyền thấp hơn truy cập vào các chức năng hoặc nội dung dành cho người dùng hoặc ứng dụng có đặc quyền cao hơn. Ví dụ: người dùng Internet Banking có chức năng quản trị hệ thống và sửa đổi cơ sở dữ liệu.

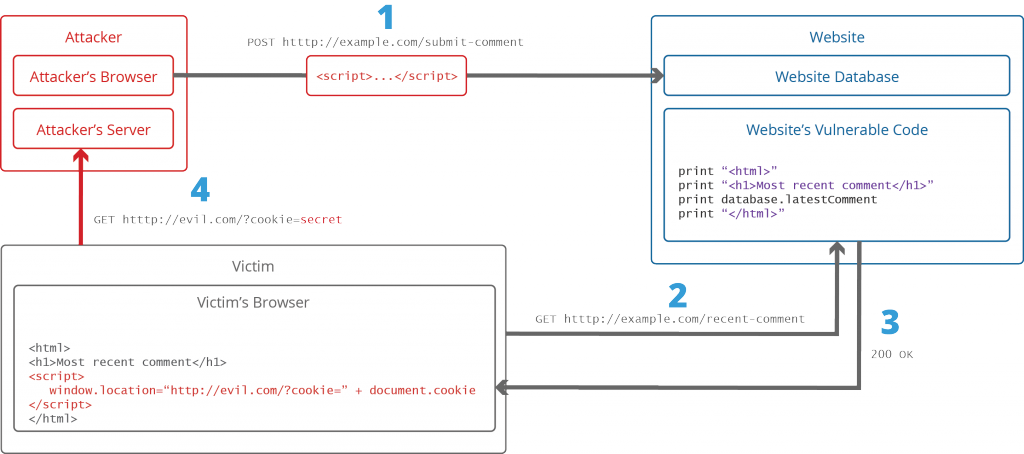
Thông qua tấn công leo thang đặc quyền dọc, kẻ tấn công sẽ được cấp cho các đặc quyền nâng cao. Với các đặc quyền nâng cao này, kẻ tấn công có thể phá hủy tất cả các tài nguyên trong hệ thống máy tính và ứng dụng của người dùng: đánh cắp thông tin truy cập và thông tin nhạy cảm khác, tải xuống và thực thi phần mềm độc hại, xóa dữ liệu hoặc thực thi mã tùy ý.

Tệ hơn nữa, những kẻ tấn công có thể sử dụng các đặc quyền nâng cao để che dấu vết của chúng bằng cách xóa nhật ký truy cập và bằng chứng khác về hoạt động của chúng. Điều này có khả năng khiến nạn nhân không biết rằng một cuộc tấn công đã xảy ra. Bằng cách đó, tội phạm mạng có thể ngấm ngầm đánh cắp thông tin hoặc cài đặt phần mềm độc hại trực tiếp trong hệ thống.

Trong một số trường hợp, một ứng dụng đặc quyền cao giả định rằng nó sẽ chỉ được cung cấp với đầu vào khớp vớp đặc tả giao diện của nó. Kẻ tấn công có thể khai thác giả định này để chạy mã trái phép với đặc quyền của ứng dụng:

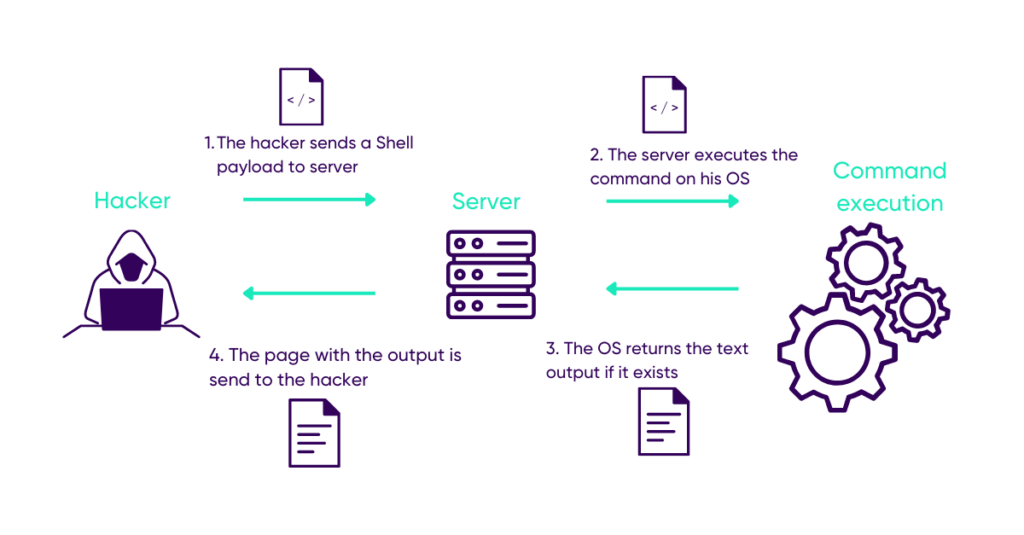
- **Buffer Overflow**: về bản chất cuộc tấn công tràn bộ đệm là gửi quá nhiều thông tin cho một biến nào đó trong ứng dụng, có thể gây lỗi ứng dụng. Một lỗ hổng như tràn bộ đệm có thể được sử dụng để thực thi mã tùy ý với đặc quyền được nâng lên quyền Administrator.

**Hình 3** Minh họa tấn công tràn bộ đệm

- **Cross Site Scripting (XSS)**: là một kiểu tấn công leo thang đặc quyền trong đó một trang web thay đổi mô hình bảo mật của trình duyệt web, cho phép chạy mã độc trên máy khách.

**Hình 4** Minh họa tấn công Cross Site Scripting

- **Command Injection**: Một ứng dụng có thể thực thi các dòng lệnh Command Line hoặc Shell có thể có lỗ hổng Shell Injection nếu nó sử dụng đầu vào không có giá trị giống như một phần của lệnh được thực thi, kẻ tấn công sau đó có thể chạy các lệnh hệ thống bằng các đặc quyền ứng dụng.



**Hình 5** Minh họa tấn công Command Injection

- **IOS Jailbreaking**: là sự leo thang đặc quyền của thiết bị Apple với mục đich xóa bỏ các hạn chế phần mềm do Apple áp đặt lên có hệ điều hành iOS, iPadOS, tvOS và watchOS. Jailbreak cho phép truy cập root trong hệ điều hành di động của Apple, cho phép cài đặt phần mềm không được Apple chấp thuận, như tùy chỉnh và chỉnh sửa giao diện người dùng.

- **Root trên Android**: là quá trình cho phép người dùng điện thoại thông minh, máy tính bảng hay các thiết bị sử dụng hệ điều hành Android để đạt được quyền truy cập root. Vì android sử dụng nhân linux, việc root thiết bị Android cho phép truy cập tương tự các quyền quản trị như trên linux hoặc bất kì hệ điều hành nào giống như Unix (FreeBSD, macOS). Root cung cấp quyền thay đổi hoặc thay thế ứng dụng và cài đặt hệ thống, các ứng dụng chuyên dụng yêu cầu quyền cấp quản trị viên hoặc các hoạt động khác mà người dùng Android không thể truy cập được.

- **Rootkit**: là một loại chương trình thường được sử dụng để che dấu các tiện ích trên hệ thống bị xâm nhập. Rootkit bao gồm cái gọi là back door, nó giúp cho kẻ tấn công đó truy cập vào hệ thống sẽ dễ dàng hơn trong lần sau. Ví dụ, các rootkit có thể ẩn một ứng dụng, ứng dụng này có thể sinh ra một lệnh kết nối vào một cổng mạng cụ thể trên hệ thống. Back door cho phép các quá trình bắt đầu bởi một người không có đặc quyên, dùng để thực hiện chức năng thường dành cho các quản trị viên.

### **2.2.3. Leo thang đặc quyền ngang**

*Leo thang đặc quyền ngang*(Horizontal privilige escalation) là khi một người dùng bình thường có thể truy cập các chức năng hoặc nội dung dành riêng cho những người dùng bình thường khác (ví dụ: người dùng Internet Banking A truy cập vào tài khoản Internet Banking của người dùng B)

Leo thang đặc quyền theo chiều ngang thường có tính thách thức hơn, vì nó thường đòi hỏi sự hiểu biết nhiều và đa dạng hơn về các lỗ hổng của hệ thống và sử dụng nhiều hơn các công cụ hack như Metasploit,…

Một số nguyên nhân dẫn đến leo thang đặc quyền ngang:

*- Đoán được session ID trong HTTP cookie của người dùng.*

*- Session fixation.*

*- Cross-site scripting.*

*- Mật khẩu dễ đoán.*

*- Trộm cắp hoặc chiếm quyền điều khiển.*

*- Keystroke logging.*

## **2.3. Các biện pháp bảo vệ hệ thống giảm thiểu leo thang đặc quyền**

Những kẻ tấn công sử dụng nhiều kĩ thuật leo thang đặc quyền để đạt được mục tiêu của họ. Nhưng trước tiên, họ thường cần có quyền truy cập vào tài khoản người dùng ít đặc quyền hơn. Điều này có nghĩa là tài khoản người dùng thông thường cần bảo vệ đầu tiên, do đó cần thực hiện các biện pháp để kiểm soát truy cập như:

- ***Thực thi chính sách mật khẩu***: mật khẩu cần phải đủ mạnh và thay đổi mật khẩu thường xuyên để bảo mật, nhưng không gây bất tiện cho người dùng.

- ***Tạo người dùng và nhóm chuyên biệt với quyền truy cập và quyền truy cập tệp tối thiểu cần thiết***: áp dụng quy tắc quyền tối thiều cần thiết để giảm thiểu rủi ro khi bất kỳ tài khoản người dùng bị xâm phạm.

Các ứng dụng cung cấp điểm vào dễ dàng nhất cho bất kỳ cuộc tấn công nào, vì vậy điều quan trọng là giữ an toàn cho chúng:

- ***Tránh các lỗi lập trình ứng dụng phổ biến thường bị kẻ tấn công nhắm tới như***: tràn bộ dệm, code injection và đầu vào của người dùng không được xác thực

- ***Bảo mật cơ sở dữ liệu và lọc đầu vào của người dùng***: các hệ thống cơ sở dữ liệu thường là mục tiêu tấn công vì nhiều ứng dụng web hiện nay và frameworks lưu trữ tất cả dữ liệu của chúng trong cơ sở dữ liệu bao gồm cài đặt cấu hình, thông tin đăng nhập và dữ liệu người dùng. Chỉ với một cuộc tấn công SQL injection, kẻ tấn công có thể có quyền truy cập vào tất cả thông tin này và sử dụng nó cho cuộc tấn công tiếp theo.

Không phải tất cả các cuộc tấn công leo thang đặc quyền đều nhắm trực tiếp vào tài khoản người dùng mà đặc quyền của quản trị viên cũng có thể có được bằng cách khai thác lỗi ứng dụng và hệ điều hành hay lỗi cấu hình. Để giảm thiểu ta cần:

- ***Giữ cho hệ thống và ứng dụng được vá và cập nhật***: Nhiều cuộc tấn công dựa vào khai thác lỗi đã biết, vì vậy ta cần giữ cập nhật để hạn chế tấn công.

- ***Đảm bảo quyền chính xác cho tất cả các tệp và thư mục***: cũng như tài khoản người dùng, các tệp và thư mục cần tuân theo quy tắc quyền tối thiểu, nếu có gì đó không cần ghi hãy giữ ở chế độ đọc.

- ***Đóng các cổng không cần thiết và xóa tài khoản người dùng không sử dụng***: cấu hình hệ thống mặc định thường bao gồm các dịch vụ không cần thiết chạy trên các cổng mở và mỗi cổng là một lỗ hổng tiềm năng. Bạn có thể xóa hoặc đổi tên tài khoản người dùng mặc định để tránh kẻ tấn công bắt đầu dễ dàng.

- ***Xóa và hạn chế tất các các chức năng truyền tệp***: kẻ tấn công thường cần một cách để tải xuống tập lệnh khai thác và mã độc, vì vậy hãy xem kĩ tất cả các công cụ, tiện ích hệ thống cho phép truyền tập như: FTP, wget, curl... Xóa các công cụ bạn không cần và khóa những công cụ còn lại, hạn chế sử dụng chúng cho các thư mục, người dùng và ứng dụng cụ thể.

- ***Thay đổi thông tin đăng nhập mặc định trên tất cả các thiết bị bao gồm cả định tuyến và máy in***: chỉ cần bộ định tuyến có mật khẩu mặc định của quản trị viên hay một máy in mạng có cổng telnet đang mở có thể cung cấp cho kẻ tấn công một chỗ đứng.

- ***Thường xuyên quét các hệ thống và ứng dụng để tìm lỗ hổng.***

Ngoài ra, người dùng có thể sử dụng một vài biện pháp khác như:

*- Ngăn chặn thực thi dữ liệu*

*- Bố trí ngẫu nhiên không gian địa chỉ*

*- Dùng trình biên dịch bẫy tràn bộ đệm*

*- Mã hóa phần mềm hoặc các thành phần firmware*

*- Dùng hệ thống với kiểm soát truy nhập bắt buộc MAC*

# **CHƯƠNG 3. TẤN CÔNG LEO THANG ĐẶC QUYỀN TRÊN ORACLE**

## **3.1. Giới thiệu về hệ quản trị cơ sở dữ liệu Oracle**

### **3.1.1. Tổng quan về hệ quản trị cơ sở dữ liệu**

**Hệ quản trị cơ sở dữ liệu** (DBMS) là hệ thống phần mềm cho phép quản lý, thao tác trên CSDL, tạo ra sự trong suốt phân tán với người dùng. Hệ quản trị cơ sở dữ liệu hoạt động trên hệ điều hành, cung cấp chức năng tạo, sửa, xóa, lưu trữ, truy vấn và quản lý dữ liệu. Hệ quản trị đóng vai trò giao diện giữa ứng dụng và dữ liệu được lưu trữ trong CSDL.

Một hệ quản trị cơ sở dữ liệu gồm 3 thành phần chính:

- ***Ngôn ngữ định nghĩa dữ liệu* (DDL)**: dùng để định nghĩa cấu trúc dữ liệu và cấu trúc của các bảng như tạo (CREATE), sửa (ALTER) và xóa (DROP)

- ***Ngôn ngữ thao tác dữ liệu* (DML/SQL)**: dùng để thao tác lên dữ liệu như thêm (INSERT), sửa (UPDATE), xóa (DELETE) và các thao tác khai thác dữ liệu như chọn (SELECT).

- ***Phần mềm kiểm soát truy cập trên dữ liệu***: đứng trung gian giữa user và phần cứng, tạo lớp vỏ bọc phần cứng với user, kiểm soát các quyền được cấp cho user trên các thành phần tương ứng của CSDL và cung cấp khả năng back-up cho toàn bộ CSDL trong trường hợp xảy ra lỗi hệ thống hoặc sự cố phần cứng.

**\* Ưu điểm của DBMS:**

* Quản lý được dữ liệu dư thừa.
* Đảm báo tính nhất quán cho dữ liệu.
* Tạo khả năng chia sẻ dữ liệu nhiều hơn.
* Cải tiến tính toàn vẹn cho dữ liệu.

**\* Nhược điểm của DBMS:**

* DBMS tốt thì khá phức tạp.
* DBMS tốt thường rất lớn chiếm nhiều dung lượng bộ nhớ.
* Giá cả khác nhau tùy theo môi trường và chức năng.
* DBMS được viết tổng quát cho nhiều người dùng thì thường chậm.

### **3.1.2. Tổng quan về hệ quản trị cơ sở dữ liệu Oracle**

**Oracle Database** (thường gọi *Oracle DBMS* hoặc *Oracle*) là bộ phần mềm hệ thống quản lý CSDL quan hệ (RDBMS) được cung cấp bởi công ty Oracle, hỗ trợ nhiều nhiệm vụ khác nhau bao gồm xử lý giao dịch, kinh doanh thông minh (business intelligence) và các ứng dụng phân tích.

Oracle được xây dựng dựa trên 3 kiến trúc:

- ***Kiến trúc bộ nhớ***

- ***Kiến trúc process***

***- Kiến trúc lưu trữ***

\* Kiến trúc bộ nhớ (Memory Structure) bao gồm 2 phần:

* ***System Global Area* (SGA)**: phần bộ nhớ chia sẻ, bao gồm nhiều phần bộ nhớ nhỏ bên trong, chứa thông tin về hoạt động database, thông tin về các session, process, code thực thi, dữ liệu đọc từ phần lưu trữ lên…Một số thành phần chính: database buffer cache, redo log bufer, shared pool, ….
* ***Program Global Area*** **(PGA)**: phần bộ nhớ riêng cho mỗi server process (user session) hay background process.

\* Kiến trúc Process (Process Structure) bao gồm 2 phần:

* ***Server Process***: khi user mở 1 tool ứng dụng lên, chẳng hạng như sqlplus và kết nối với database ta gọi nó là user process. Server process là các tiến trình được sinh ra để phục vụ các yêu cầu từ user process.
* ***Background Process***: thực hiện các công việc nội tại của database: quản lý memory, process, quản lý I/O, giao tiếp giữa các thành phần, ….

\* Kiến trúc lưu trữ (Storage Structure) hay còn gọi là Database bao gồm 2 phần:

* ***Kiến trúc vật lý***: là các tập tin, những gì thấy được trên hệ điều hành được lưu trữ trong hệ thống lưu trữ.
* ***Kiến trúc logic***: phân bổ không gian logic cho tất cả dữ liệu trong database, lưu trữ logic tổ chức phức tạp, phân theo nhiều cấp.

#### **3.1.2.1. Phân loại người dùng**

Oracle là một hệ quản trị cơ sở dữ liệu lớn, chạy trên môi trường mạng. Để vận hành hệ thống được tốt, có thể có nhiều người sẽ tham gia vào hệ thống với vai trò khác nhau gọi là các user. Phân ra làm một số user chính:

* + - * Database Administrators (DBA)
      * Security Officers
      * Application Developers
      * Application Administrators
      * Database Users
      * Network Administrators

#### **3.1.2.2. Đặc quyền trong Oracle**

Người dùng Oracle sẽ được trao cho một số quyền thực hiện những thao tác nhất định với CSDL. Đặc quyền được trao có thể là gán (GRANT) hoặc thu hồi (REVOKE) với người dùng.

**Phân loại:**

* + - * Đặc quyền hệ thống: quyền thực hiện một tác vụ cơ sở dữ liệu cụ thể hoặc quyền thực hiện một loại hành động trên tất cả những đối tượng schema của hệ thống. Ví dụ: quyền ALTER SYSTEM, quyền CREATE TABLE, quyền DELETE ANY TABLE, …….
      * Đặc quyền đối tượng: quyền thực hiện một thao tác cụ thể lên một schema object cụ thể. Ví dụ như quyền thêm, xóa, sửa các hàng dữ liệu của bảng.

Có 2 user được gán sẵn quyền DBA là SYS và SYSTEM.

***Tài khoản SYS:***

* Là tài khoản sở hữu cơ sở dữ liệu và từ điển dữ liệu. User này được tạo tự động và được gán role DBA.
* Không nên tạo các table hay chỉnh sửa gì trong schema của user SYS.

***Tài khoản SYSTEM:***

* Là tài khoản được tạo khi tạo cơ sở dữ liệu, được gán role DBA, thường sở hữu các bảng do Oracle cung cấp. User SYSTEM có thể tạo thêm các table và view để cung cấp thông tin quản trị.
* Không nên tạo các đối tượng bằng tài khoản này.

***Quyền DBA***: Ngay khi tạo database, Oracel tạo sẵn 1 quyền gọi là DBA. Quyền này cho phép thực hiện các thao tác quản trị đối với database.

### **3.1.3. Ngôn ngữ PL/SQL**

Là một ngôn ngữ lâp trình hướng thủ tục sử dụng cho Oracle SQL. SQL dùng để truy nhập lấy dữ liệu từ cơ sở dữ liệu, không có sự đảm bảo về tính hiệu quả, không có vòng lặp… do đó PL/SQL (Procedural Language/Structured Query Language) được sử dụng để khắc phục những nhược điểm SQL và phát triển thêm những tính năng mới.

PL/SQL sử dụng cho việc tạo các procedure, fuction, trigger và object được lưu trữ trong Oracle và được tái sử dụng bởi các ứng dụng bất kỳ giao tiếp với ứng dụng Oracle.

## **3.2. Các loại tấn công leo thang đặc quyền trong Oracle**

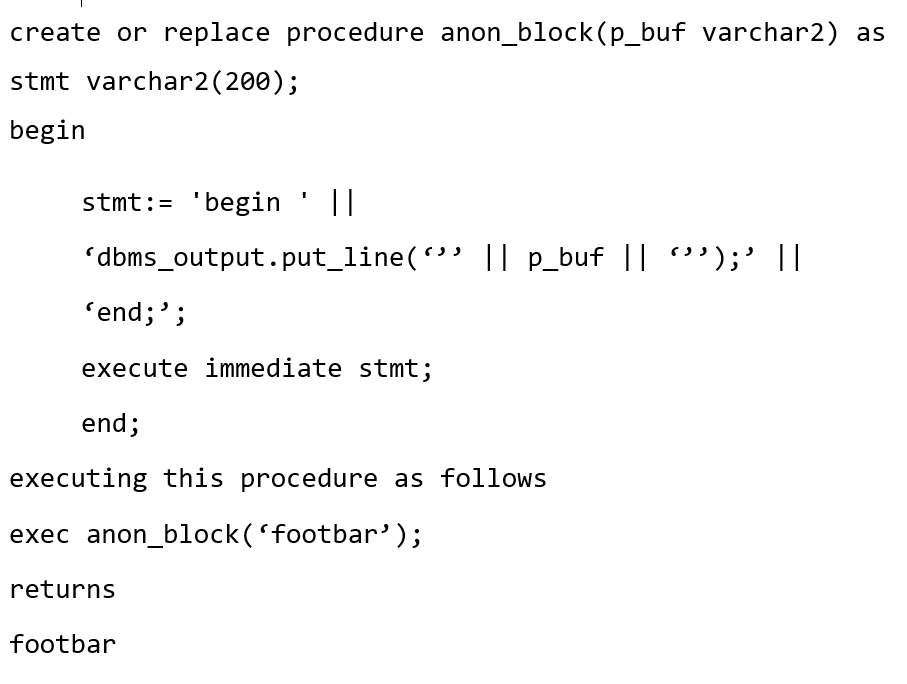
### **3.2.1. PL/SQL Injection**

**SQL injection** là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của DBMS trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update, v.v. trên CSDL của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy.

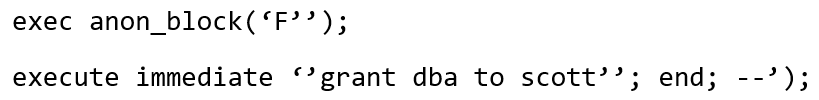
**PL/SQL**, giống như các thủ tục được lưu trữ, có thể dễ bị tấn công SQL injection. Khi mã PL/SQL tích hợp đầu vào của người dùng vào một truy vấn và thực thi nó, chúng tôi gặp chính xác vấn đề giống như chúng tôi gặp phải khi xây dựng một truy vấn động cổ điển. Trong hầu hết các trường hợp, cuộc tấn công khá giống với những cuộc tấn công được trình bày trong hướng dẫn.

***\* Chèn câu truy vấn vào Anonymous PL/SQL Blocks (Đưa vào các khối PL/SQL ẩn danh)***

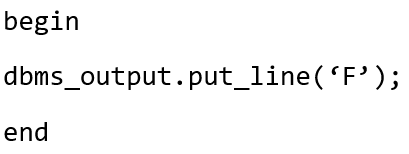
Mặc dù theo định nghĩa, một khối PL/SQL ẩn danh không được liên kết với bất kỳ thủ tục hoặc chức năng nào, các chương trình PL/SQL được lưu trữ có thể thực thi PL/SQL ẩn danh từ bên trong mã của chúng. Ví dụ, hãy xem xét đoạn mã sau:



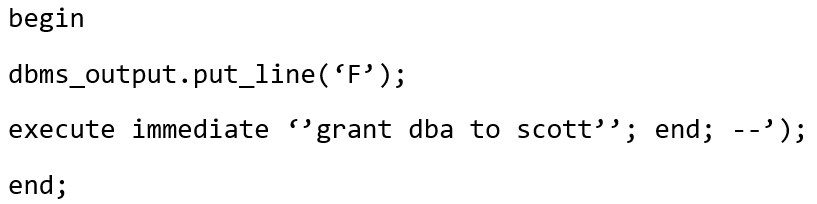
Nếu kẻ tấn công có thể đưa vào các khối PL/SQL ẩn danh, như có thể được thực hiện với thủ tục ANON\_BLOCK này, thì kẻ tấn công có thể làm những gì? Giả sử thủ tục ANON\_BLOCK này được xác định bởi người dùng SYS, kẻ tấn công có thể đưa vào câu lệnh GRANT này để trở thành **DBA**.



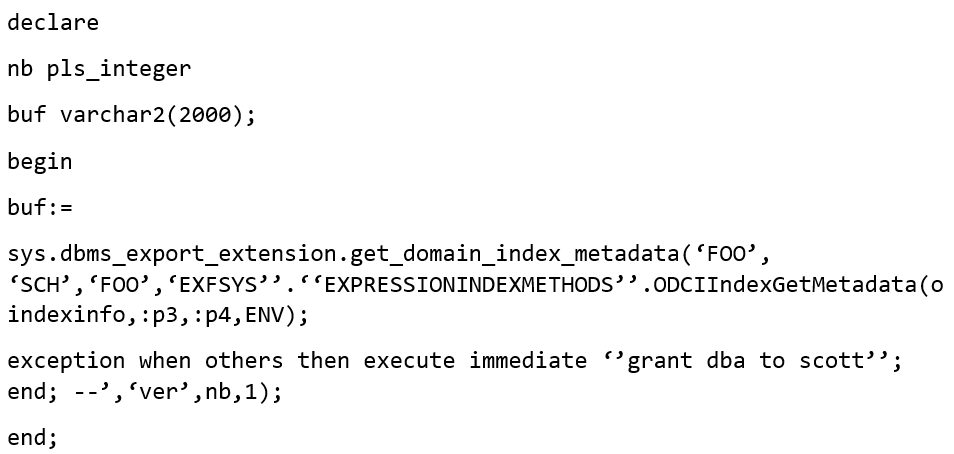
Điều này thay đổi khối PL/SQL ẩn danh ban đầu từ



thành

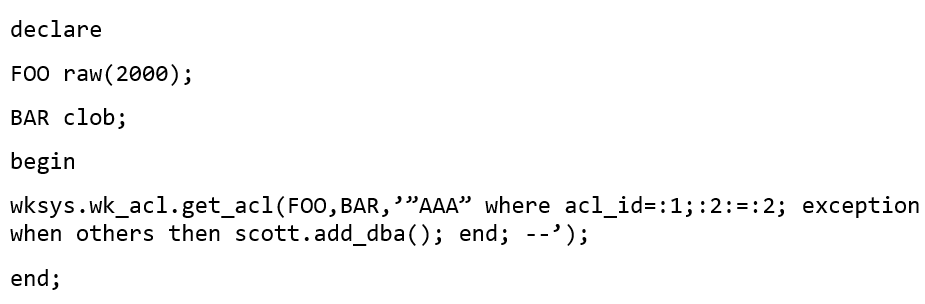


**Ví dụ thực tế**

Mặc dù ANON\_BLOCK trên là một ví dụ lý thuyết, nhưng điều này là tiền đề để xảy ra trong thế giới thực. Ví dụ, trong Oracle 10g, PUBLIC có thể thực thi thủ tục GET\_DOMAIN\_INDEX\_METADATA của gói DBMS\_EXPORT\_EXTENSION do SYS sở hữu. Gói này chưa được xác định bằng từ khóa AUTHID\_CURRENT\_USER và như vậy sẽ chạy với đầy đủ các đặc quyền của SYS. Thủ tục này thực thi một khối PL/SQL ẩn danh và nó có thể được đưa vào.

Tập lệnh này sẽ đưa vào thủ tục và cấp vai trò DBA cho SCOTT. Bằng cách nắm bắt tất cả các ngoại lệ với từ khóa WHEN OTHERS, khi ngoại lệ “no data” xảy ra, nó sẽ bị bắt và EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT' được kích hoạt.

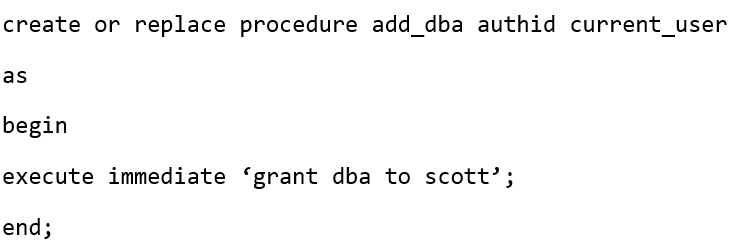
Một ví dụ khác là thủ tục GET\_ACL của gói WK\_ACL thuộc sở hữu của WKSYS trên Oracle 10g. Thủ tục này nhận tham số thứ ba của nó là giá trị varchar2. Giá trị này sau đó được chèn vào một khối PL/SQL ẩn danh trong quy trình để thực hiện lựa chọn từ một liên kết cơ sở dữ liệu từ xa. Bằng cách chèn SQL của riêng chúng ta vào tham số này, chúng ta có thể nâng cấp lên **DBA**. Ví dụ: hãy xem xét tập lệnh sau



Tham số thứ ba của GET\_ACL là '“AAA” WHERE ACL\_ID =: 1;: 2: =: 2; EXCEPTION WHEN OTHERS THEN SCOTT.ADD\_DBA (); END;--'. Ở đây “AAA” là một liên kết cơ sở dữ liệu. Chúng ta phải thêm “WHERE ACL\_ID =: 1;: 2: =: 2” để tránh lỗi “bind variable not present”. Sau đó, ta thiết lập một khối ngoại lệ:

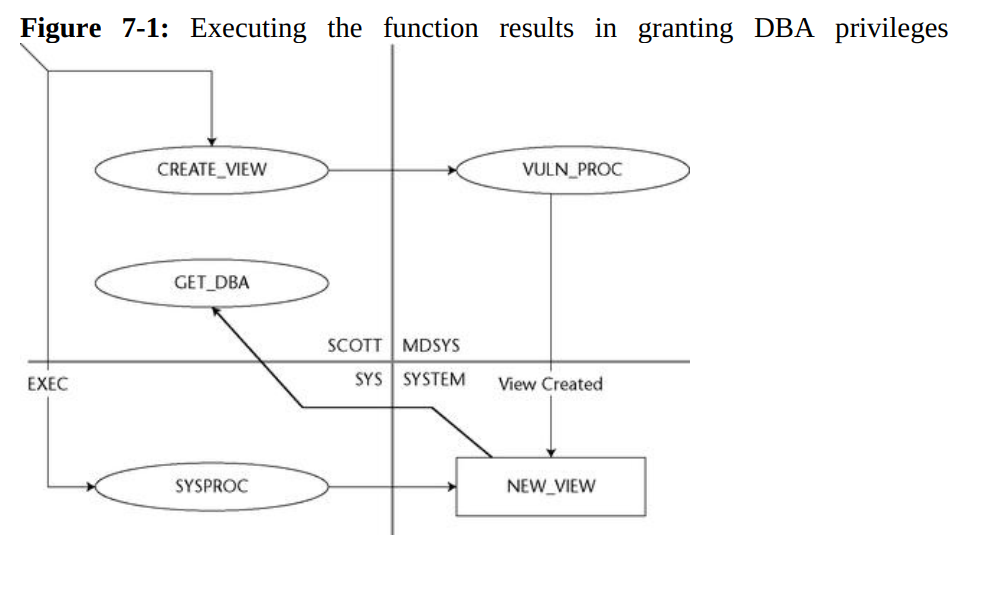
EXCEPTION WHEN OTHERS THEN SCOTT.ADD\_DBA();

Khi một ngoại lệ xảy ra - ví dụ: "no data" được trả về - thủ tục SCOTT.ADD\_DBA được thực thi. SCOTT tạo quy trình này như sau:



Nếu dữ liệu được trả về thì không cần khối ngoại lệ vì vậy '“AAA” WHERE ACL\_D =: 1;: 2: =: 2; SCOTT.ADD\_DBA (); END; - ' như tham số thứ ba sẽ thực hiện. Ràng buộc duy nhất là liên kết cơ sở dữ liệu “AAA” phải tồn tại và là công khai hoặc thuộc sở hữu của WKSYS.

### **3.2.2. Leo thang đặc quyền DBA bằng CREATE ANY VIEW**



**Hình 6** Leo thang đặc quyền bằng CREATE ANY VIEW

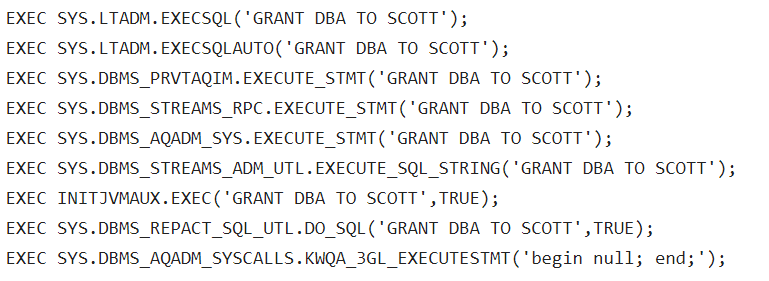
Đầu tiên cần có một thủ tục chứa lỗ hổng, một user với đặc quyền CREATE ANY VIEW.

Sau đó hacker cần tạo một view trong Schema của DBA và tiếp theo, bằng cách nào đó khiến user có đặc quyền cao hơn truy cập view này. Phần tấn công này nghe có vẻ khó hơn vì phụ thuộc vào việc user đặc quyền cao có truy cập view hay không. Tuy nhiên không phải vậy. Có hàng trăm trường hợp các thủ tục của SYS sử dụng tên của một bảng, hay một khung nhìn làm tham số và sau đó truy cập bảng, hay khung nhìn này. Nhưng với mục đích minh hoạ và tiết kiệm thời gian, chúng ta sẽ tạo một hàm (đảm bảo rằng hàm này không dễ bị chèn SQL injection bằng ASSERT.QUALIFIED\_SQL\_NAME)

Tiếp theo, chúng ta sẽ thực hiện lấy quyền DBA. Những gì chúng ta cần làm là đưa vào thủ tục của user hacker (HACKER.VPROC) - một thủ tục của chúng ta. Thủ tục này sẽ tạo một view trong Schema của SYSTEM. Ở ví dụ này chúng ta chọn Schema của SYSTEM vì đặc quyền CREATE ANY VIEW không cho phép tạo khung nhìn trong Schema của SYS. Khung nhìn được tạo sẽ gọi tới một hàm mà do chính hacker tạo ra. Hàm này chứa đoạn lệnh gán quyền cho ta để lấy được đặc quyền DBA. Khi chúng ta truy cập khung nhìn thông qua thủ tục SYS.SPROC, hàm này sẽ được thực thi và quyền DBA sẽ được gán.

### **3.2.3. Leo thang đặc quyền DBA bằng CREATE, EXECUTE PROCEDURE**

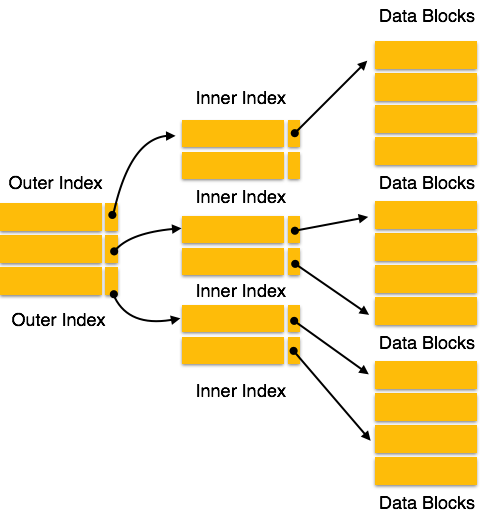
Hacker có thể lợi dụng đặc quyền EXCUTE ANY PROCEDURE và tìm ra một thủ tục của người dùng SYS cho phép chèn vào những đoạn mã SQL tuỳ ý để ngay lập tức lấy được đặc quyền DBA. Chỉ một số các thủ tục có thể được khai thác được liệt kê dưới đây:



Trong trường hợp chúng ta tìm ra một lỗ hổng SQL injection trong một package của một user có rất ít đặc quyền như OLAPSYS, MDSYS, DBSNMP và ORDSYS. Những tài khoản này thường được cấp quyền CREATE PROCEDURE. Do đó, nếu những user này thay đổi một trong các thủ tục mà họ sở hữu – có những thủ tục của user khác phụ thuộc lên những thủ tục này – thì họ sẽ có quyền thực thi những đoạn mã như những tài khoản sở hữu những thủ tục phụ thuộc kia. Nếu tài khoản user bị tấn công không phải người dùng DBA, thì bạn cũng đã tiến gần hơn một bước tới việc đạt được quyền hạn cao hơn.

Lấy ví dụ thủ tục VALIDATE\_CONTEXT do SYS sở hữu nhưng phụ thuộc vào gói DRUE của CTXSYS. Nếu CTXSYS thay đổi package này, chèn vào nó những đoạn mã tấn công, thì theo lí thuyết CTXSYS sẽ lấy được quyền DBA. Vì vậy, nếu CTXSYS sở hữu một thủ tục PUBLIC có thể bị tấn công SQL injection thì CTXSYS cũng có khả năng lấy được quyền DBA. Trong phiên bản 10g bản phát hành 2, CTXSYS đã bị gỡ bỏ đặc quyền này. Tuy nhiên chúng ta đã nắm được ý tưởng về cách thức tấn công. Vì vậy, có thể tham khảo những thủ tục nào phụ thuộc vào cái gì thông qua DBA\_DEPENDENCIES.

### **3.2.4. Leo thang đặc quyền DBA bằng INDEX**



**Hình 7** Minh họa chỉ mục (INDEX)

INDEX là một Object được tạo ra trên table với mục đích gia tăng tốc độ truy xuất dữ liệu. Với ý nghĩa như mục lục của cuốn sách, INDEX được tạo trên 1 hoặc nhiều column. Khi đó INDEX sẽ lưu giữ các giá trị trong các trường thuộc tính đó, cùng với rowId (địa chỉ vật lý trên disk) của từng hàng dữ liệu. Nhờ vậy khi truy vấn 1 lượng data nhỏ, Oracle có thể lấy được ngày dữ liệu nhờ việc truy xuất đúng vị trí row dữ liệu trên disk, thay vì phải dò toàn bộ bảng để tìm dữ liệu.

Trong Oracle, để có thể tạo chỉ mục trên bảng, user phải sở hữu bảng (owner) hoặc có đặc quyền đối tượng INDEX trên bảng hoặc có đặc quyền hệ thống CREATE ANY INDEX. Nếu user có một trong hai đặc quyền này, thì một lỗ hổng bảo mật sẽ lộ ra, mà theo đó họ có thể thực thi SQL tùy ý với tư cách là owner của bảng bằng cách tạo một chỉ mục dựa trên hàm. Nếu bảng được đề cập thuộc sở hữu của user có đặc quyền cao như SYS hoặc SYSTEM thì máy chủ CSDL sẽ bị lộ nguy hiểm vì nó cung cấp cho kẻ tấn công khả năng xâm phạm kiểm soát hoàn toàn hệ thống. Role PUBLIC (trước đây) đã được cấp đặc quyền INDEX sau:

* SYS.DUAL
* SYS.OLAPTABLEVELS
* SYS.OLAPTABLEVELTUPLES
* SYSTEM.OLAP\_SESSION\_CUBES
* SYSTEM.OLAP\_SESSION\_DIMS
* SYSTEM.PLAN\_TABLE
* FLOWS\_FILES.WWV\_FLOW\_FILE\_OBJECT$
* TOAD.TOAD\_PLAN\_TABLE

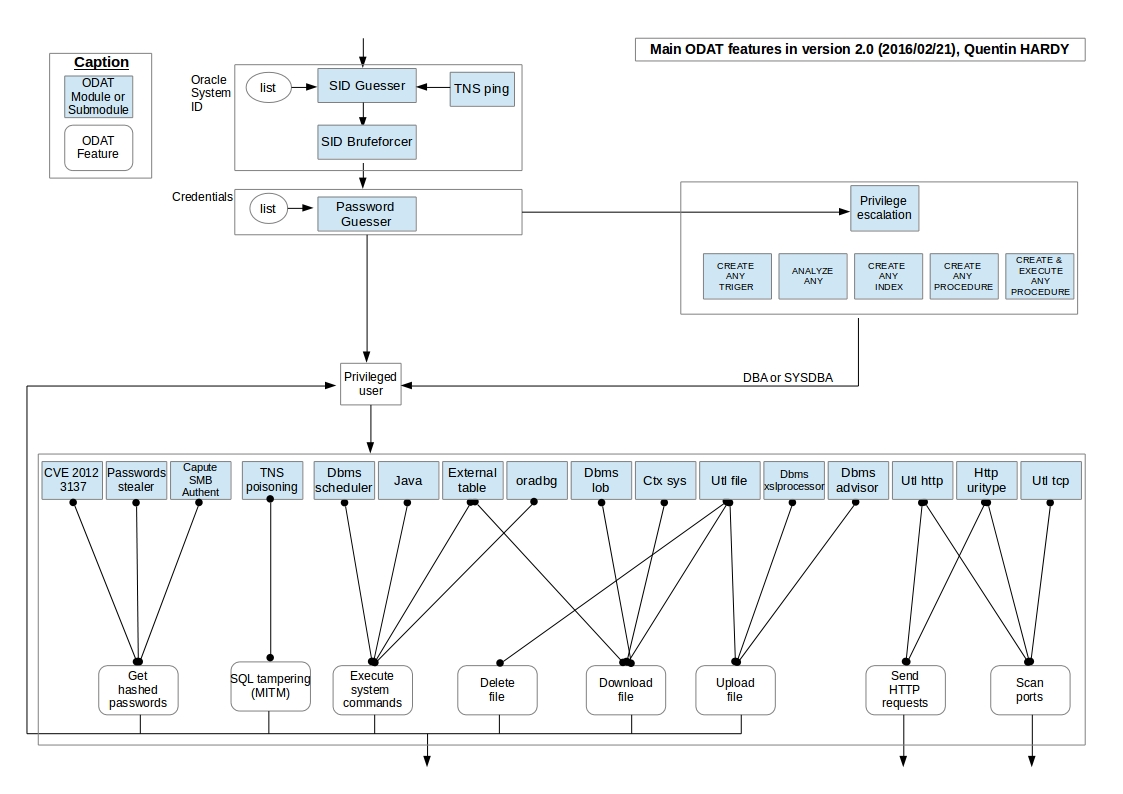
***\* Ví dụ minh họa:***

Giả sử có một bảng tên là FOO thuộc sở hữu của SYS và tất cả mọi users (PUBLIC) đã được cấp đặc quyền INDEX trên đó. User tên là TEST kết nối với máy chủ CSDL và cố gắng đặt role DBA nhưng không thành công vì TEST chưa được cấp thành viên của role này.

Đầu tiên, TEST tạo một hàm gọi là GETDBA sẽ thực hiện công việc khi được gọi sau này. Tiếp theo TSS tạo một chỉ mục có tên EXPLOIT\_INDEX trên bảng SYS.FOO gọi hàm GETDBA. Sau đó, TEST thực hiện SELECT từ bảng DUAL khiến chỉ mục EXPLOIT\_INDEX thực thi chức năng GETDBA với các đặc quyền SYS. Hàm GETDBA chứa câu lệnh SQL để cấp role DBA cho PUBLIC. Khi điều này đã được thực hiện, user TEST có thể đặt role DBA. Lúc này, user TEST đã có toàn quyền kiểm soát CSDL.

### **3.2.5. Sử dụng công cụ ODAT**

Phần mềm mã nguồn mở ODAT (Oracle Database Attacking Tool) là một công cụ pentest kiểm thử bảo mật cơ sở dữ liệu Oracle từ xa.



**Hình 8** Kiến trúc ODAT

Những trường hợp có thể sử dụng ODAT:

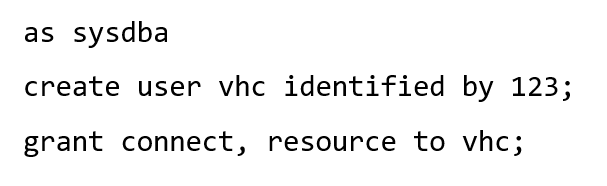
* Bạn có một CSDL Oracle từ xa và muốn tìm kiếm những nguy cơ từ hệ thống cũng như các xác thực hợp lệ để kết nối với CSDL.
* Nâng quyền trên CSDL Oracle, vượt quyền cho phép (Ví dụ: SYSDBA)
* Thực hiện các lệnh Command line trên HĐH lưu trữ thông qua CSDL Oracle này (Ví dụ: reverse shell)

Đã thử nghiệm / kiểm nghiệm trên Oracle 10g, 11g, 12c, 18c và 19c.

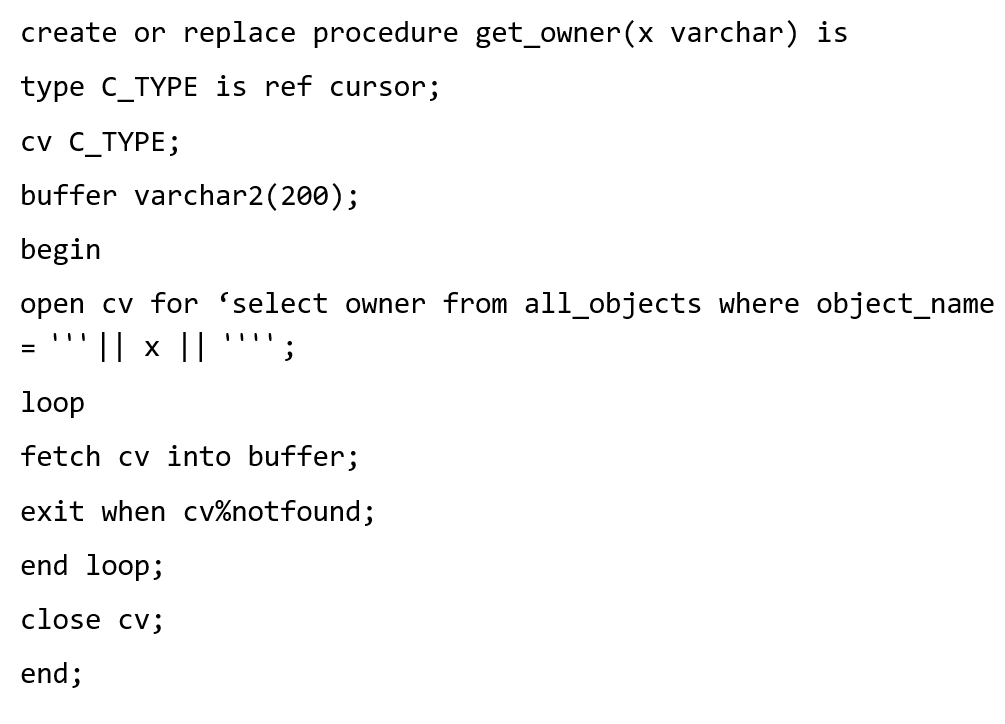
# **CHƯƠNG 4. THỰC NGHIỆM**

## **4.1. Khai thác PL/SQL Injection (19c)**

Kết nối vào CSDL bằng tài khoản SYS và tạo lập tài khoản user VHC



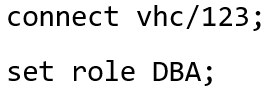
Tạo 1 thủ tục có tên GET\_OWNER với tham số truyền vào X



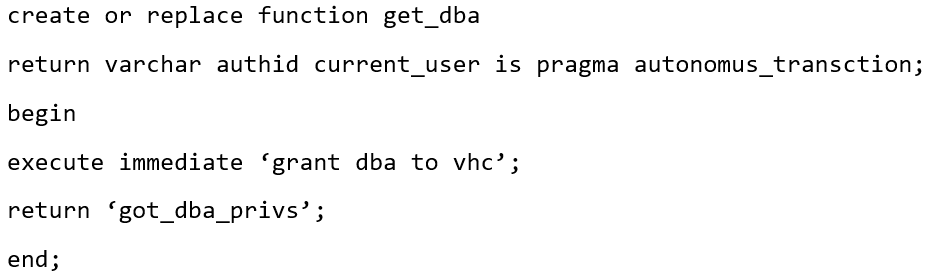
A close up of black text

Description generated with high confidenceGán 1 số quyền thực thi trên thủ tục cho user VHC

Kết nối vào tài khoản user VHC



Tạo 1 hàm tên GET\_DBA để gán quyền DBA cho user DBA



Thực thi bảng GET\_OWNER của tài khoản SYS với hàm GET\_DBA được tiêm vào

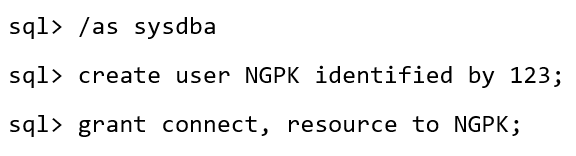


Cài đặt role DBA thành công

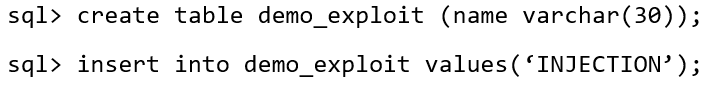


## **4.2. Create Index (19c)**

Kết nối vào CSDL bằng tài khoản SYS và tạo lập tài khoản user NGPK



Tạo 1 bảng có tên DEMO\_EXPLOIT với 1 cột NAME, sau đó chèn vào bảng 1 bản ghi có nội dung là “INJECTION”



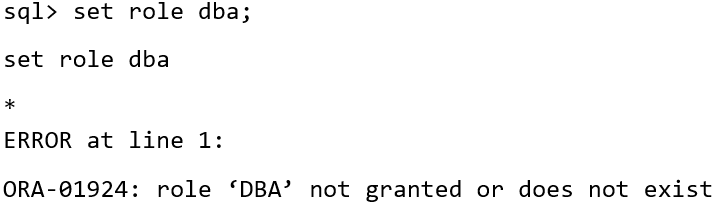
Black text on a white background

Description generated with very high confidenceGán 1 số quyền thực thi trên bảng cho user NGPK

Kết nối vào tài khoản user NGPK



Thử đặt role DBA và bị báo lỗi



Tạo 1 hàm có tên DEMO nhằm thực thi gán quyền DBA cho user NGPK

A computer code with black text

Description generated with high confidence

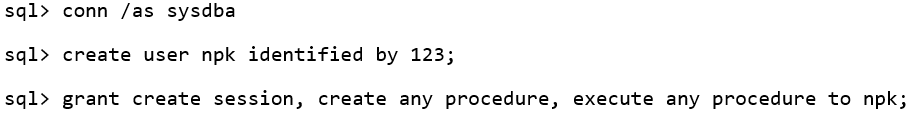
Tạo 1 INDEX lên bảng DEMO\_EXPLOIT



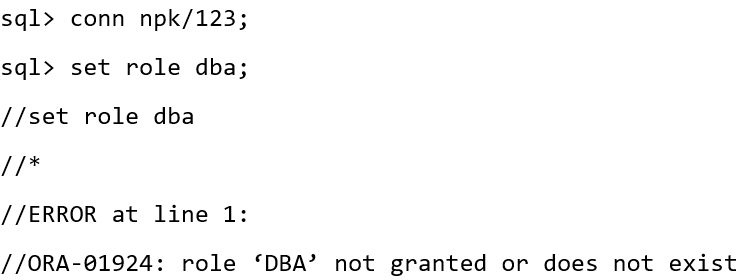
Cài đặt role DBA thành công

## **4.3. Create và Execute Procedure (11gR2)**

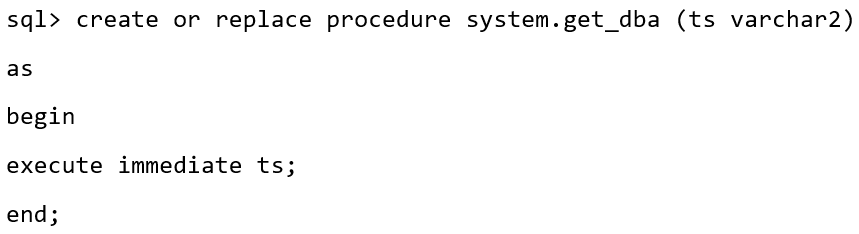
Kết nối vào CSDL bằng tài khoản SYS, tạo lập tài khoản user NPK và gán 1 số quyền procedure cho user NPK



Kết nối vào tài khoản user NGPK, thử đặt role DBA và bị báo lỗi



Tạo 1 thủ tục có tên SYSTEM.GET\_DBA với tham số truyền vào TS



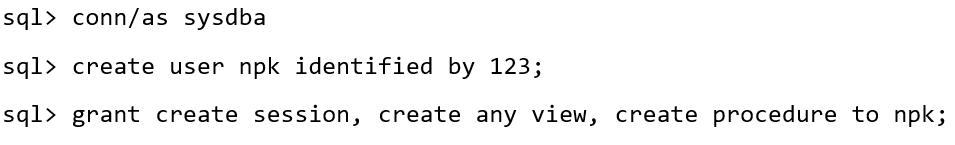
Thực thi hàm với tham số truyền vào là lệnh cấp quyền DBA cho user NPK



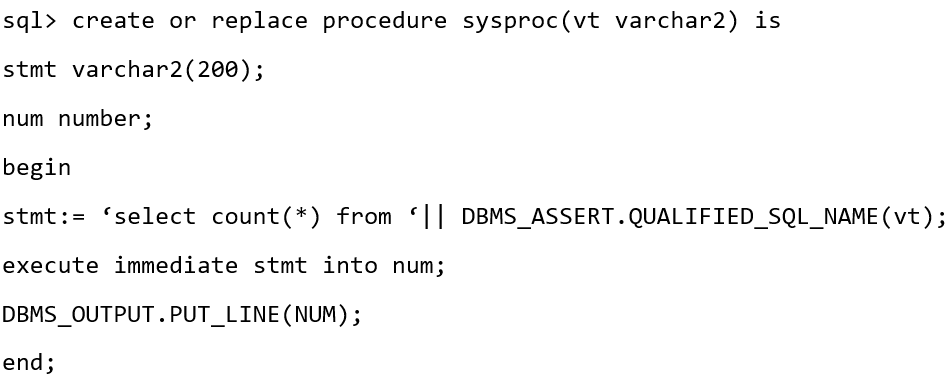
Cài đặt role DBA thành công

## **4.4. Create view (11gR2)**

Kết nối vào CSDL bằng tài khoản SYS, tạo lập tài khoản user NPK và gán 1 số quyền cho user NPK



Tạo 1 thủ tục có tên SYSPROC với tham số truyền vào VT

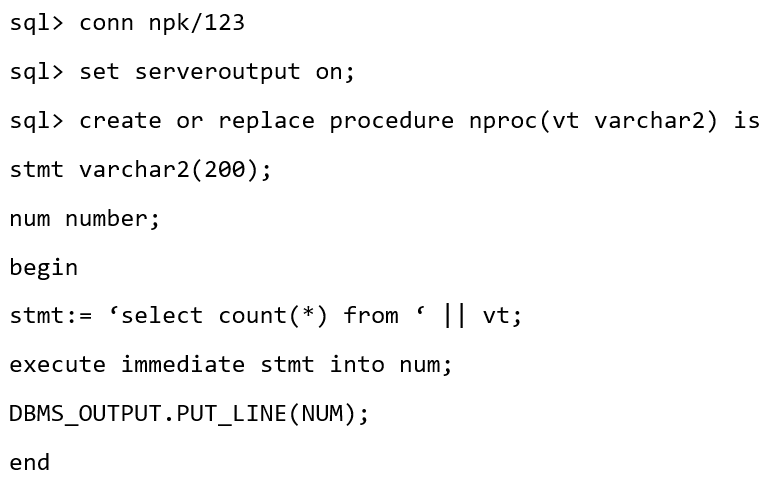


Gán quyền thực thi thủ tục đến tất cả users



Kết nối vào tài khoản user NPK

Tạo 1 thủ tục có tên NPROC với tham số truyền vào VT



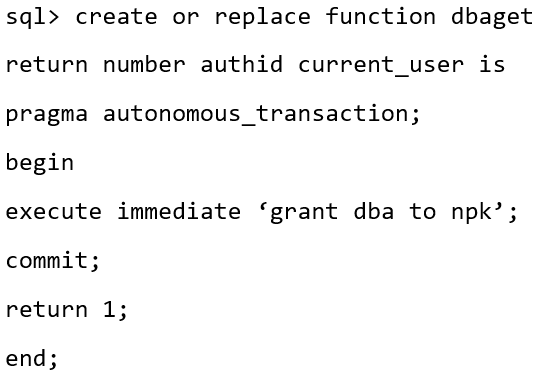
Gán quyền thực thi thủ tục đến tất cả users



Thực thi thủ tục với tham số truyền vào ‘ALL\_OBJECTS’



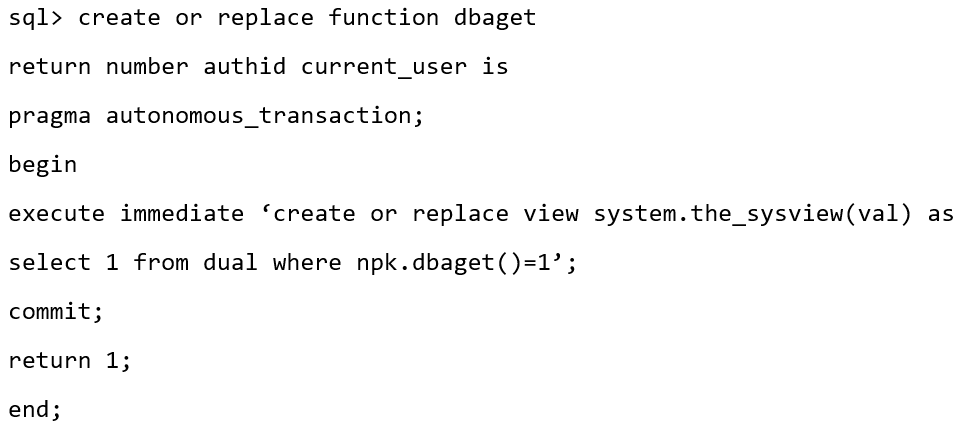
Tạo 1 hàm có tên DBAGET nhằm thực hiện gán quyền DBA cho user NPK



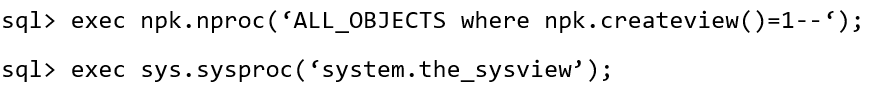
Gán quyền thực thi hàm đến tất cả users



Tạo 1 hàm có tên CREATVIEW nhằm tạo view trên hệ thống, gán quyền DBA cho user NPK



Gán quyền thực thi hàm đến tất cả users, lần lượt thực thi các hàm sau



Cài đặt role DBA thành công

# **KẾT LUẬN**

Leo thang đặc quyền trong hệ quản trị cơ sở dữ liệu Oracle là một vấn đề bảo mật đáng lo ngại, có thể gây ra hậu quả nghiêm trọng nếu không được nhận diện và xử lý kịp thời. Bài báo cáo đã cung cấp một số kiến thức về cách thức hoạt động của các cuộc tấn công leo thang đặc quyền, những lỗ hổng phổ biến trong Oracle mà kẻ tấn công có thể khai thác, và tầm quan trọng của việc áp dụng các biện pháp phòng ngừa hiệu quả.

Việc bảo vệ hệ thống cơ sở dữ liệu không chỉ đơn thuần là khắc phục các lỗ hổng khi chúng đã bị khai thác, mà còn là xây dựng một chiến lược bảo mật chủ động, bao gồm việc cập nhật thường xuyên các bản vá bảo mật, quản lý quyền truy cập chặt chẽ, và kiểm tra định kỳ cấu hình hệ thống. Đồng thời, sự hợp tác giữa các nhóm kỹ thuật và quản trị an ninh mạng là yếu tố then chốt để đảm bảo hệ thống luôn được bảo vệ toàn diện trước những mối đe dọa ngày càng phức tạp.

Dù có thể triển khai nhiều kỹ thuật khác nhau, song điều kiện tối thiểu cho bất kỳ sự leo thang đặc quyền nào cũng là cần có quyền truy cập vào tài khoản người dùng có đặc quyền thấp hơn để có được quyền truy cập. Do đó, các tài khoản người dùng thông thường đóng vai trò là tuyến phòng thủ đầu tiên.

Việc quản lý chặt chẽ và liên tục cải thiện bảo mật hệ thống là điều kiện tiên quyết để đảm bảo an toàn thông tin trong môi trường sử dụng Oracle. Các bước phòng ngừa và biện pháp khắc phục sẽ giúp giảm thiểu nguy cơ và bảo vệ dữ liệu quan trọng của tổ chức khỏi các mối đe dọa tiềm tàng.

# **TÀI LIỆU THAM KHẢO**

<https://www.oracletutorial.com/oracle-administration/oracle-database-architecture/>

<https://docs.oracle.com/cd/B19306_01/win.102/b14305/architec.htm#NTQRX292>

<https://docs.oracle.com/cd/E11882_01/server.112/e40540/physical.htm#CNCPT401>

<https://docs.oracle.com/cd/E11882_01/server.112/e40540/logical.htm#CNCPT301>

[https://docs.oracle.com/cd/B10500\_01/server.920/a96521/dba.htm](https://docs.oracle.com/cd/B10500_01/server.920/a96521/dba.htm#834)

<https://docs.oracle.com/database/121/TTSQL/privileges.htm#TTSQL338>

<https://docs.oracle.com/cd/B16351_01/doc/server.102/b14196/users_secure002.htm>

<https://docs.oracle.com/database/121/ADMIN/dba.htm#ADMIN001>

<https://docs.oracle.com/database/121/DBSEG/authentication.htm#DBSEG342>

<https://www.tranvanbinh.vn/2020/02/tutorial-dba-co-ban-chuong-5-quan-tri.html>

<https://www.netsparker.com/blog/web-security/privilege-escalation/>

<https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained>

<https://www.w4rri0r.com/sequence-of-commands/privilege-escalation-attacks.html>

<https://www.sciencedirect.com/topics/computer-science/privilege-escalation>

<https://www.acunetix.com/blog/web-security-zone/what-is-privilege-escalation/>

<https://securitydaily.net/oracle-database-attacking-tool-cong-cu-kiem-thu-bao-mat-co-so-du-lieu-oracle/>

<https://docs.oracle.com/cd/B19306_01/server.102/b14200/statements_9013.htm#i2077938>

<http://www.davidlitchfield.com/Privilege_Escalation_via_Oracle_Indexes.pdf>

The oracle hacker’s handbook: Hacking and defending oracle – David LitchField

Advanced SQL Injection in Oracle databases - Esteban Martínez Fayó

Best of Oracle Security 2014 - Alexander KornBusrt

Introduction to Database Management System – Dr. Satinder Bal Gupta & Aditya Mittal