**TẤN CÔNG SQL INJECTION BẰNG UNION**

- Khi 1 ứng dụng dễ bị tấn công và kết quả truy vấn được trả về trong phản hồi, có thể sử dụng từ khóa UNION để truy xuất dữ liệu từ các bảng khác trong CSDL.

- Từ khóa UNION cho phép thực hiện 1 hoặc nhiều truy vấn SELECT bổ sung và thêm kết quả vào truy vấn ban đầu. Ví dụ:

SELECT a, b FROM table1 UNION SELECT c, d FROM table2

- Truy vấn này trả về 1 tập kết quả duy nhất với 2 cột, chứa các giá trị từ các cột a và b trong table1 và cột c và d trong table2.

- Để UNION có hiệu quả, 2 yêu cầu chính phải được đáp ứng:

* Các truy vấn riêng lẻ phải được trả về cùng số cột.
* Các kiểu dữ liệu trong mỗi cột phải tương thích với các truy vấn riêng lẻ.

- Để thực hiện tấn công UNION, đảm bảo cuộc tấn công đáp ứng được 2 yêu cầu sau:

* Có bao nhiêu cột được trả về từ truy vấn ban đầu
* Những cột nào được trả về từ truy vấn gốc có kiểu dữ liệu phù hợp để lưu trữ kết quả từ truy vấn được đưa vào

**Xác định số lượng cột cần thiết (\*)**

- Khi tấn công UNION, có 2 phương pháp hiệu quả để xác định có bao nhiêu cột được trả về từ truy vấn gốc.

- 1 phương pháp bao gồm việc chèn 1 loạt các mệnh đề ORDER BY và tăng chỉ số cột được chỉ định cho đến khi xảy ra lỗi. Ví dụ, nếu điểm chèn là 1 chuỗi được trích dẫn trong mệnh đề WHERE của truy vấn gốc, sẽ gửi:

' ORDER BY 1--

' ORDER BY 2--

' ORDER BY 3--

etc.

- Chuỗi tải trọng này sửa đổi truy vấn gốc để sắp xếp kết quả theo các cột khác nhau trong tập kết quả. Cột trong mệnh ORDER BYđề có thể được chỉ định theo chỉ mục của nó, do đó bạn không cần biết tên của bất kỳ cột nào. Khi chỉ mục cột được chỉ định vượt quá số lượng cột thực tế trong tập kết quả, cơ sở dữ liệu trả về lỗi, chẳng hạn như:

The ORDER BY position number 3 is out of range of the number of items in the select list.

- Ứng dụng có thể thực sự trả về lỗi cơ sở dữ liệu trong phản hồi HTTP của nó, nhưng nó cũng có thể đưa ra phản hồi lỗi chung. Trong những trường hợp khác, nó có thể chỉ trả về không có kết quả nào cả. Dù bằng cách nào, miễn là bạn có thể phát hiện ra một số khác biệt trong phản hồi, bạn có thể suy ra có bao nhiêu cột đang được trả về từ truy vấn.

- Phương pháp thứ hai bao gồm việc gửi một loạt UNION SELECT các dữ liệu chỉ định số lượng giá trị null khác nhau:

' UNION SELECT NULL--

' UNION SELECT NULL,NULL--

' UNION SELECT NULL,NULL,NULL--

etc.

- Nếu số lượng giá trị null không khớp với số lượng cột, cơ sở dữ liệu sẽ trả về lỗi, chẳng hạn như:

All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists.

- Chúng tôi sử dụng NULL.asp các giá trị trả về từ truy vấn được đưa vào SELECTvì kiểu dữ liệu trong mỗi cột phải tương thích giữa truy vấn gốc và truy vấn được đưa vào. NULLcó thể chuyển đổi sang mọi kiểu dữ liệu phổ biến, do đó, nó tối đa hóa cơ hội tải trọng sẽ thành công khi số cột là chính xác.

- Tương tự như ORDER BYkỹ thuật này, ứng dụng có thể thực sự trả về lỗi cơ sở dữ liệu trong phản hồi HTTP của nó, nhưng có thể trả về lỗi chung hoặc đơn giản là không trả về kết quả nào. Khi số lượng giá trị null khớp với số lượng cột, cơ sở dữ liệu trả về một hàng bổ sung trong tập kết quả, chứa các giá trị null trong mỗi cột. Hiệu ứng đối với phản hồi HTTP phụ thuộc vào mã của ứng dụng. Nếu may mắn, bạn sẽ thấy một số nội dung bổ sung trong phản hồi, chẳng hạn như một hàng bổ sung trên bảng HTML. Nếu không, các giá trị null có thể kích hoạt một lỗi khác, chẳng hạn như NullPointerException. *Trong trường hợp xấu nhất, phản hồi có thể trông giống như phản hồi do số lượng giá trị null không chính xác. Điều này sẽ khiến phương pháp này không hiệu quả.*

**Cú pháp dành riêng cho CSDL (\*)**

- Trên Oracle, mọi SELECT truy vấn phải sử dụng FROM từ khóa và chỉ định một bảng hợp lệ. Có một bảng tích hợp trên Oracle được gọi là dualcó thể được sử dụng cho mục đích này. Vì vậy, các truy vấn được tiêm vào trên Oracle sẽ cần trông giống như sau:

' UNION SELECT NULL FROM DUAL—

- Các tải trọng được mô tả sử dụng chuỗi chú thích gạch ngang kép --để chú thích phần còn lại của truy vấn gốc sau điểm tiêm. Trên MySQL, chuỗi gạch ngang kép phải được theo sau bởi một khoảng trắng. Ngoài ra, có thể sử dụng ký tự băm #để xác định chú thích.

**Tìm các cột có kiểu dữ liệu hữu ích (\*)**

- Tấn công SQL injection UNION cho phép bạn lấy kết quả từ truy vấn inject. Dữ liệu thú vị mà bạn muốn lấy thường ở dạng chuỗi. Điều này có nghĩa là bạn cần tìm một hoặc nhiều cột trong kết quả truy vấn gốc có kiểu dữ liệu là hoặc tương thích với dữ liệu chuỗi.

- Sau khi xác định số lượng cột cần thiết, bạn có thể thăm dò từng cột để kiểm tra xem nó có thể chứa dữ liệu chuỗi hay không. Bạn có thể gửi một loạt UNION SELECTcác tải trọng đặt giá trị chuỗi vào từng cột theo lượt. Ví dụ, nếu truy vấn trả về bốn cột, bạn sẽ gửi:

' UNION SELECT 'a',NULL,NULL,NULL--

' UNION SELECT NULL,'a',NULL,NULL--

' UNION SELECT NULL,NULL,'a',NULL--

' UNION SELECT NULL,NULL,NULL,'a'—

- Nếu kiểu dữ liệu cột không tương thích với dữ liệu chuỗi, truy vấn được đưa vào sẽ gây ra lỗi cơ sở dữ liệu, chẳng hạn như:

Conversion failed when converting the varchar value 'a' to data type int.

Nếu không xảy ra lỗi và phản hồi của ứng dụng chứa một số nội dung bổ sung bao gồm giá trị chuỗi được đưa vào thì cột có liên quan sẽ phù hợp để truy xuất dữ liệu chuỗi.

**Sử dụng tấn công UNION để lấy dữ liệu (\*)**

- Khi bạn đã xác định được số cột trả về bởi truy vấn ban đầu và tìm ra cột nào có thể chứa dữ liệu chuỗi, bạn đã có thể truy xuất dữ liệu thú vị.

Giả sử:

* Truy vấn ban đầu trả về hai cột, cả hai đều có thể chứa dữ liệu chuỗi.
* Điểm chèn là một chuỗi được trích dẫn trong mệnh WHEREđề.
* Cơ sở dữ liệu chứa một bảng có tên userslà các cột usernamevà password.

Trong ví dụ này, bạn có thể lấy nội dung của usersbảng bằng cách gửi dữ liệu đầu vào:

' UNION SELECT username, password FROM users—

- Để thực hiện cuộc tấn công này, bạn cần biết rằng có một bảng được gọi là userscó hai cột được gọi usernamelà và password. Nếu không có thông tin này, bạn sẽ phải đoán tên của các bảng và cột. Tất cả các cơ sở dữ liệu hiện đại đều cung cấp các cách để kiểm tra cấu trúc cơ sở dữ liệu và xác định chúng chứa những bảng và cột nào.

**Lấy nhiều giá trị trong 1 cột duy nhất (\*)**

- Trong một số trường hợp, truy vấn trong ví dụ trước chỉ có thể trả về một cột duy nhất.

Bạn có thể lấy nhiều giá trị cùng nhau trong một cột duy nhất này bằng cách nối các giá trị lại với nhau. Bạn có thể bao gồm một dấu phân cách để phân biệt các giá trị kết hợp. Ví dụ, trên Oracle, bạn có thể gửi đầu vào:

' UNION SELECT username || '~' || password FROM users—

- Điều này sử dụng chuỗi double-pipe ||là toán tử nối chuỗi trên Oracle. Truy vấn được tiêm sẽ nối các giá trị của các trường usernamevà password, được phân tách bằng ~ký tự.

Kết quả từ truy vấn chứa tất cả tên người dùng và mật khẩu, ví dụ:

...

administrator~s3cure

wiener~peter

carlos~montoya

...

Các cơ sở dữ liệu khác nhau sử dụng cú pháp khác nhau để thực hiện nối chuỗi. Để biết thêm chi tiết, hãy xem bảng hướng dẫn về SQL injection .