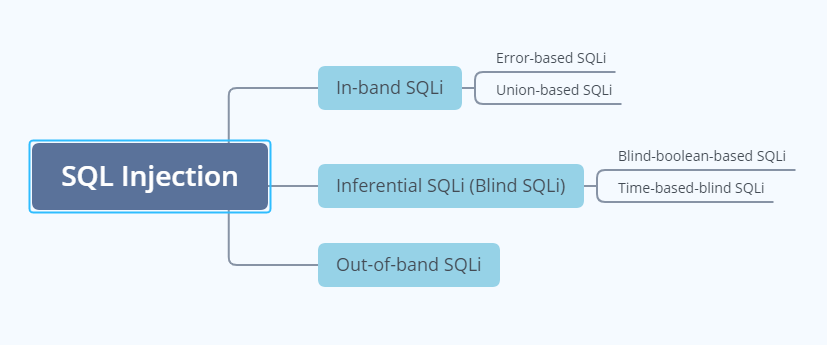
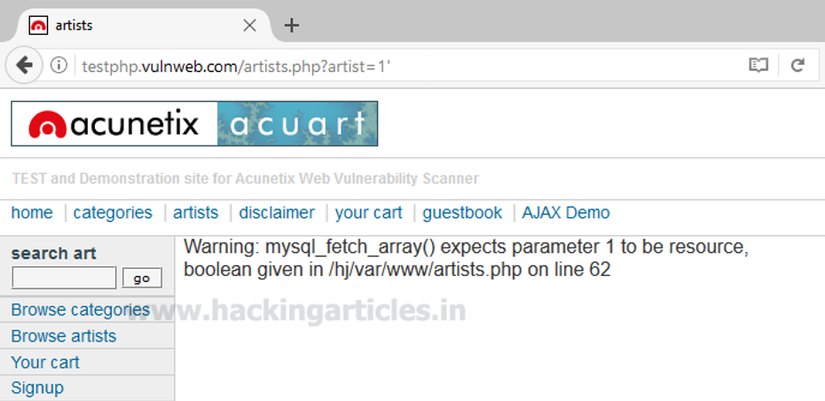
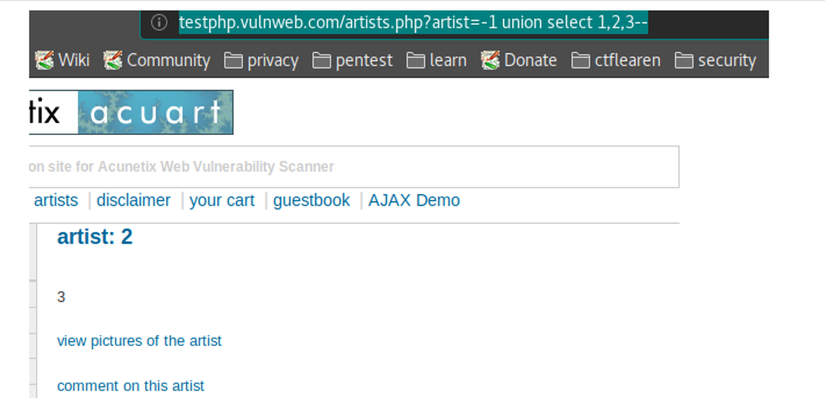
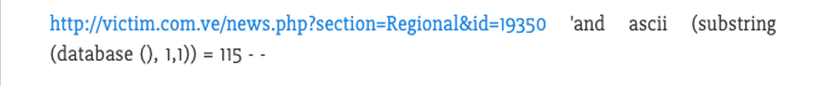
**SQL INJECTION**

1. **Kiến thức cơ bản**
   1. **Giới thiệu SQLi**

* SQL injection là một lỗ hổng bảo mật web cho phép kẻ tấn công can thiệp vào các truy vấn mà ứng dụng thực hiện đối với cơ sở dữ liệu của nó. Nó thường cho phép kẻ tấn công xem dữ liệu mà chúng thường không thể lấy được. Điều này có thể bao gồm dữ liệu thuộc về người dùng khác hoặc bất kỳ dữ liệu nào khác mà bản thân ứng dụng có thể truy cập. Trong nhiều trường hợp, kẻ tấn công có thể sửa đổi hoặc xóa dữ liệu này, gây ra những thay đổi liên tục đối với nội dung hoặc hành vi của ứng dụng.
* Trong một số tình huống, kẻ tấn công có thể leo thang một cuộc tấn công SQL injection để xâm nhập máy chủ bên dưới hoặc cơ sở hạ tầng back-end khác hoặc thực hiện một cuộc tấn công từ chối dịch vụ.
* Một cuộc tấn công SQL injection thành công có thể dẫn đến việc truy cập trái phép vào dữ liệu nhạy cảm, chẳng hạn như mật khẩu, chi tiết thẻ tín dụng hoặc thông tin người dùng cá nhân. Nhiều vụ vi phạm dữ liệu cấu hình cao trong những năm gần đây là kết quả của các cuộc tấn công SQL injection, dẫn đến thiệt hại về danh tiếng và tiền phạt theo quy định. Trong một số trường hợp, kẻ tấn công có thể có được một cửa hậu liên tục vào hệ thống của tổ chức, dẫn đến một thỏa hiệp lâu dài có thể không được chú ý trong một thời gian dài.
  1. **Các loại SQLi, cách nhận biết và phòng tránh.**
* Các loại SQL thường gặp:
  + Retrieving hidden data: truy xuất dữ liệu ẩn – kẻ tấn công có thể sửa đổi câu truy vấn SQL để trả về thông tin bổ sung, ngoài mục đích thông tin ban đầu được cung cấp.
  + Subverting application logic: kẻ tấn công có thể thay đổi một truy vấn để can thiệp vào logic của ứng dụng.
  + UNION attacks: kẻ tấn công có thể lấy dữ liệu từ các bảng CSDL khác nhau.
  + Examining the database: kẻ tấn công có thể trích xuất thông tin về phiên bản và cấu trúc của CSDL.
  + Blind SQL injection: kết quả truy vấn của kẻ tấn công không được trả về trong phản hồi của ứng dụng.
  + …
* Có thể phân lại SQL như sau:  
  
* In-band SQLi: Đây là dạng tấn công phổ biến nhất và cũng dễ để khai thác lỗ hổng SQL Injection nhất. Xảy ra khi hacker có thể tổ chức tấn công và thu thập kết quả trực tiếp trên cùng một kênh liên lạc
  + Error-based SQLi:
    - Là một kỹ thuật tấn công SQL Injection dựa vào thông báo lỗi được trả về từ Database Server có chứa thông tin về cấu trúc của cơ sở dữ liệu.  
      
  + Union-based SQLi:
    - Là một kỹ thuật tấn công SQL Injection dựa vào sức mạnh của toán tử UNION trong ngôn ngữ SQL cho phép tổng hợp kết quả của 2 hay nhiều câu truy vấn SELECTION trong cùng 1 kết quả và được trả về như một phần của HTTP response.  
      
* Inferential SQLi (Blind SQLi):
  + Không giống như In-band SQLi, Inferential SQL Injection tốn nhiều thời gian hơn cho việc tấn công do không có bất kì dữ liệu nào được thực sự trả về thông qua web application và hacker thì không thể theo dõi kết quả trực tiếp như kiểu tấn công In-band.
  + Thay vào đó, kẻ tấn công sẽ cố gắng xây dựng lại cấu trúc cơ sở dữ liệu bằng việc gửi đi các payloads, dựa vào kết quả phản hồi của web application và kết quả hành vi của database server.
  + Blind-boolean-based:
    - Là kĩ thuật tấn công SQL Injection dựa vào việc gửi các truy vấn tới cơ sở dữ liệu bắt buộc ứng dụng trả về các kết quả khác nhau phụ thuộc vào câu truy vấn là True hay False.
    - Tuỳ thuộc kết quả trả về của câu truy vấn mà HTTP reponse có thể thay đổi, hoặc giữ nguyên
    - Kiểu tấn công này thường chậm (đặc biệt với cơ sở dữ liệu có kích thước lớn) do người tấn công cần phải liệt kê từng dữ liệu, hoặc mò từng kí tự  
      
  + Time-based Blind SQLi:
    - Time-base Blind SQLi là kĩ thuật tấn công dựa vào việc gửi những câu truy vấn tới cơ sở dữ liệu và buộc cơ sở dữ liệu phải chờ một khoảng thời gian (thường tính bằng giây) trước khi phản hồi.
    - Thời gian phản hồi (ngay lập tức hay trễ theo khoảng thời gian được set) cho phép kẻ tấn công suy đoán kết quả truy vấn là TRUE hay FALSE
    - Kiểu tấn công này cũng tốn nhiều thời gian tương tự như Boolean-based SQLi
* Out-of-band SQLi
  + Out-of-band SQLi không phải dạng tấn công phổ biến, chủ yếu bởi vì nó phụ thuộc vào các tính năng được bật trên Database Server được sở dụng bởi Web Application.
  + Kiểu tấn công này xảy ra khi hacker không thể trực tiếp tấn công và thu thập kết quả trực tiếp trên cùng một kênh (In-band SQLi), và đặc biệt là việc phản hồi từ server là không ổn định
  + Kiểu tấn công này phụ thuộc vào khả năng server thực hiện các request DNS hoặc HTTP để chuyển dữ liệu cho kẻ tấn công.
  + Ví dụ như câu lệnh xp\_dirtree trên Microsoft SQL Server có thể sử dụng để thực hiện DNS request tới một server khác do kẻ tấn công kiểm soát, hoặc Oracle Database’s UTL HTTP Package có thể sử dụng để gửi HTTP request từ SQL và PL/SQL tới server do kẻ tấn công làm chủ

1. **Nâng cao**
   1. **Bypass filter**

* Một số WAF filter các kí tự đặc biệt, các xâu như UNION, ORDER, … ta có thể bypass bằng cách thêm chữ hoa chữ thường, encode url, … hoặc dùng các hàm encode unhex, convert, …
* Một số web check kí tự đầu vào bằng hàm addslash(), có thể them kí tự %bf hoặc %af trước dấu nháy đơn để khi đi qua bộ lọc còn lại dấu nháy đơn (/’).
* …
  1. **Tối ưu tấn công Boolean-based SQLi**
* Thay vì tìm kiếm tuần tự, có thể tìm kiếm nhị phân để tăng tốc độ.
* Có thể chạy đa luồng vì kết quả kí tự sau không cần liên quan đến kí tự trước.