Báo cáo Nhiệm vụ: Xử lý Dataset và Kiểm thử Bảo mật trong Đồ án

1.Giới thiệu:

Mục tiêu của đồ án là phát hiện và khắc phục các lỗ hổng bảo mật trong ứng dụng web thông qua việc xử lý dataset và thực hiện kiểm thử bảo mật. Trong phạm vi đồ án này, nhiệm vụ của em là thu thập, xử lý dataset mô phỏng các cuộc tấn công bảo mật (đặc biệt là SQL Injection) và sử dụng công cụ OWSAP ZAP để thực hiện các bài kiểm thử bảo mật nhằm phát hiện và khắc phục các điểm yếu bảo mật của hệ thống.

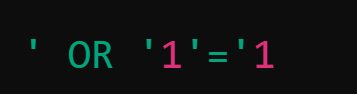
#### **2.Xử lý Dataset**

Dataset là bộ dữ liệu quan trọng giúp mô phỏng và kiểm tra các loại tấn công bảo mật. Mục tiêu của việc xử lý dataset là chuẩn bị một môi trường thực tế cho các bài kiểm thử bảo mật, đặc biệt là các cuộc tấn công SQL Injection.

**2.1.Công việc cụ thể:**

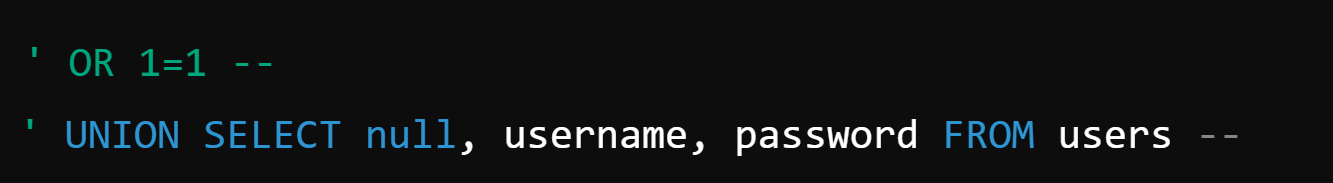
**- Thu thập Dữ liệu:** Dữ liệu sẽ được thu thập từ ứng dụng web, bao gồm các thông tin về người dùng, dữ liệu nhập vào (như các tham số tìm kiếm, đăng nhập, v.v.). Đây là dữ liệu quan trọng dùng để mô phỏng hành vi của người dùng trong hệ thống.

**- Mô phỏng Tấn công SQL Injection:** Để kiểm tra sự bảo mật, em sẽ tạo ra các chuỗi dữ liệu chứa các payload của SQL Injection, như:



Ví dụ này có thể bị hệ thống hiểu là một truy vấn hợp lệ và bỏ qua kiểm tra xác thực, dẫn đến việc lấy cắp dữ liệu.

- Dữ liệu thử nghiệm: Tạo các chuỗi payload SQL Injection để chèn vào các điểm nhập liệu (như form đăng nhập, tìm kiếm) và đánh giá phản ứng của hệ thống. Một số ví dụ payload thường gặp:



- Định dạng Dataset**:** Tập hợp các dữ liệu đầu vào đã được chuẩn bị, bao gồm cả dữ liệu hợp lệ và các payload tấn công, giúp mô phỏng các tình huống thực tế trong thử nghiệm bảo mật.

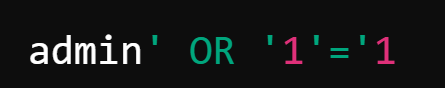
#### **3. Kiểm thử Bảo mật với OWASP ZAP**

**OWASP ZAP** (Zed Attack Proxy) là công cụ mã nguồn mở được sử dụng để quét các lỗ hổng bảo mật của ứng dụng web. Trong đồ án này, em sẽ sử dụng ZAP để thực hiện các bài kiểm thử bảo mật, đặc biệt là kiểm tra SQL Injection.

**Các phương pháp kiểm thử:**

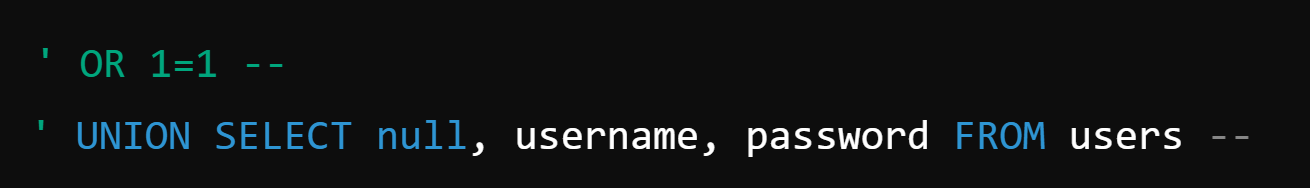
* **Kiểm thử SQL Injection:** Sử dụng tính năng "Fuzzing" của ZAP để chèn các payload SQL vào các tham số của ứng dụng (như tên người dùng, mật khẩu, hoặc các tham số URL). Quá trình này sẽ giúp phát hiện các điểm yếu trong hệ thống có thể bị tấn công bằng SQL Injection.

**Ví dụ**: Với form đăng nhập, có thể nhập vào trường "Tên đăng nhập" chuỗi:



ZAP sẽ tự động gửi chuỗi này đến máy chủ và kiểm tra phản ứng, nếu ứng dụng không bảo vệ đúng cách, nó có thể bị lỗi hoặc truy vấn dữ liệu trái phép.

* Fuzzing và Payload Injection: ZAP cho phép sử dụng các kỹ thuật fuzzing để tự động thử nhiều payload SQL khác nhau trong các trường nhập liệu. Ví dụ, thử nghiệm chèn các chuỗi sau vào các trường đầu vào:



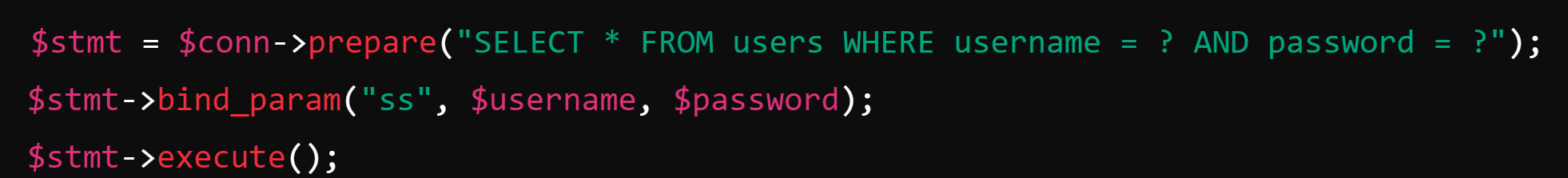
* Đánh giá phản hồi và phân tích kết quả: ZAP sẽ giúp phân tích các phản hồi từ máy chủ. Nếu phản hồi chứa các lỗi SQL hoặc các thông báo lỗi cơ sở dữ liệu (như "syntax error" hoặc "database error"), đó có thể là dấu hiệu của một lỗ hổng SQL Injection.

#### **4. Phân tích và Đưa ra Giải pháp**

Sau khi thực hiện kiểm thử bảo mật, tôi sẽ phân tích kết quả và xác định các lỗ hổng bảo mật. Các giải pháp để khắc phục SQL Injection bao gồm:

* **Sử dụng truy vấn đã tham số hóa (parameterized queries):** Thay vì chèn dữ liệu người dùng trực tiếp vào câu truy vấn SQL, sử dụng tham số hóa để đảm bảo dữ liệu không bị thực thi như một phần của mã SQL.

**Ví dụ** (trong PHP):



* Xác thực đầu vào: Kiểm tra và lọc các đầu vào từ người dùng để ngăn ngừa dữ liệu độc hại. Chỉ cho phép các ký tự hợp lệ và không chấp nhận các ký tự đặc biệt có thể gây ra lỗ hổng.
* Cập nhật phần mềm và vá lỗi bảo mật: Đảm bảo rằng ứng dụng và các thư viện sử dụng luôn được cập nhật và không chứa các lỗ hổng bảo mật đã biết.

Tài liệu tham khảo

OWASP ZAP: Hướng dẫn và tài liệu chính thức về OWASP ZAP và các tính năng bảo mật của nó có thể được tìm thấy tại [OWASP ZAP official](https://www.zaproxy.org/).

SQL Injection: Các tài liệu về SQL Injection có thể được tham khảo trong các bài viết trên OWASP và các trang như OWASP SQL Injection.

Best Practices for Web Security: OWASP Web Security Testing Guide.