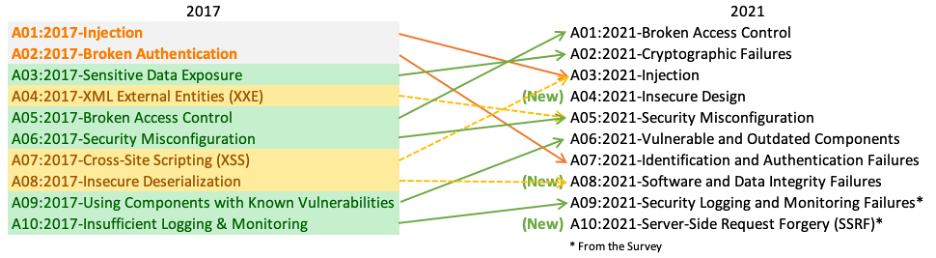
Project 3 - Phát triển công cụ rà soát lỗ hổng SQL injection

Tuần 3+4: Tổng quan đề tài, giới thiệu sơ lược công cụ

Lê Ngọc Hoa 20200234

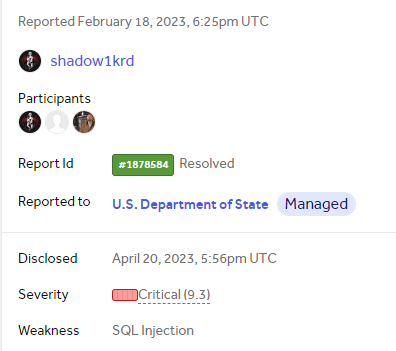
1. Lý do chọn đề tài

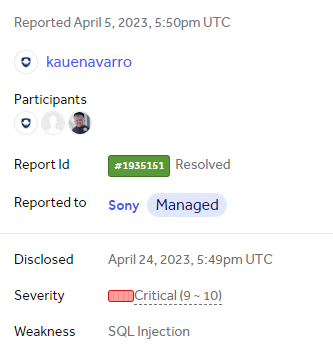
Dù là một lỗ hổng đã xuất hiện từ rất lâu, SQL injection vẫn nằm trong nhóm lỗ hổng Top 3 theo bảng xếp hạng OWASP top 10 năm 2021



<https://owasp.org/Top10/>

Trong năm 2023, các diễn đàn bug bounty lớn vẫn nhận số lượng lớn các báo cáo về lỗ hổng SQLi trong các hệ thống khách hàng của họ:



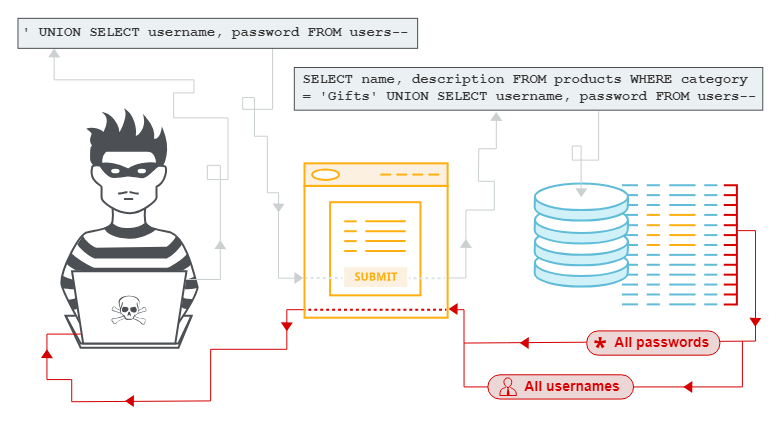


Mặc dù các dịch vụ WAF đã giúp ngăn chặn phần lớn các cuộc tấn công, nhưng với số lượng sản phẩm web lớn và gia tăng nhanh chóng không thể áp dụng WAF toàn phần do vấn đề chi phí và tài nguyên, attacker vẫn có thể lợi dụng lỗ hổng SQLi tấn công vào database của các công ty.

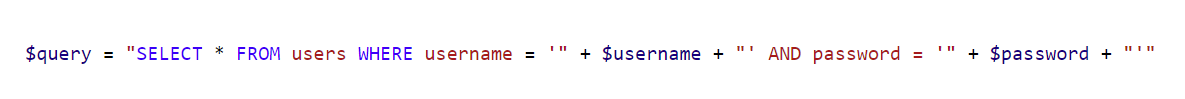
Công cụ rà soát lỗ hổng SQLi với mục đích giúp giảm thiểu lỗ hổng SQLi xuống mức tối thiểu, rà soát sản phẩm trước khi đưa ra thị trường, tính tự động còn giúp tiết kiệm chi phí cho công việc pentest ứng dụng.

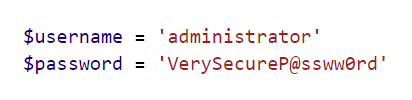
1. Tổng quan lỗ hổng SQL injection
2. Khái niệm

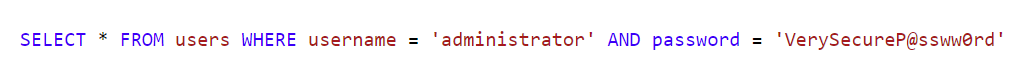
SQL injection (SQLi) là một lỗ hổng bảo mật web cho phép kẻ tấn công can thiệp vào các truy vấn mà ứng dụng thực hiện đối với cơ sở dữ liệu của nó.

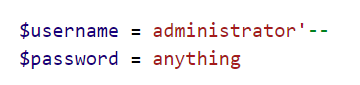


1. Ví dụ nhỏ









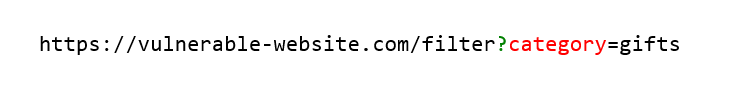


1. Dự kiến cơ chế phát hiện lỗ hổng của công cụ
2. Inject point

Inject point chỉ các trường input (thông thường được nhập bởi user) có thể tương tác trong câu query SQL. Chia theo hai loại method của request được gửi tới server: GET và POST

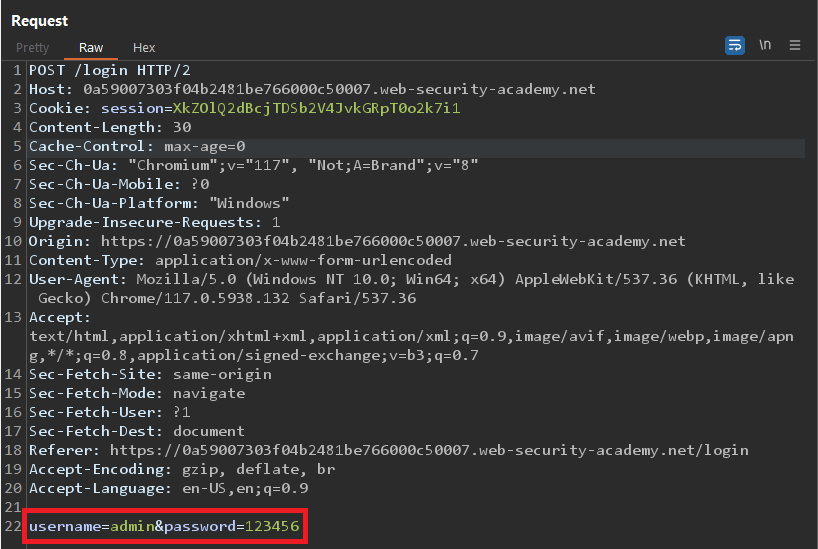
* GET request

Tham số được truyền qua URL



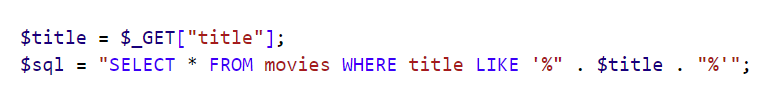
* POST request

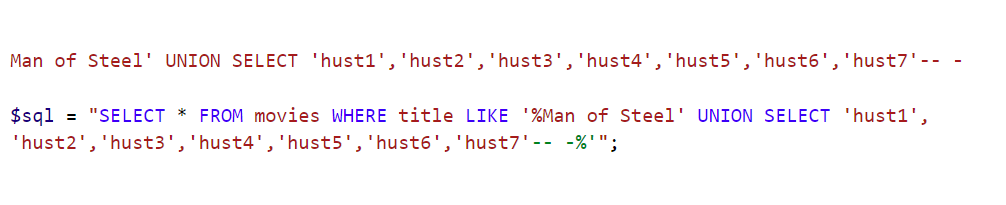
Thường là tham số lấy từ các form (ví dụ login form), xác định qua gói tin request (lấy từ một số công cụ proxy như BurpSuite)

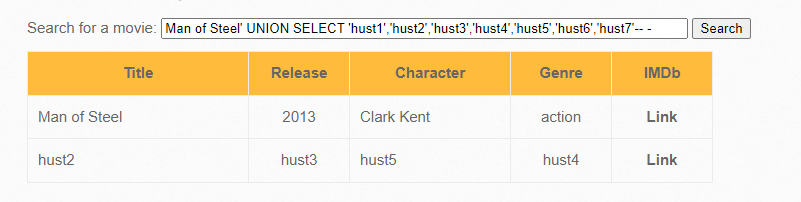


1. Phát hiện (Ví dụ với MySQL)

* Trường hợp 1: website hiển thị dữ liệu output lấy từ database → UNION attack







* Trường hợp 2: Website không hiển thị output từ câu query → Time based attack

