**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

**KIỂM THỬ LỖ HỔNG SQL INJECTION**

***Họ và tên: ĐỖ VĂN KHẢI***

***https://youtu.be/-8honApgKk8***

***Yêu cầu kết quả thực hành:***

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

**Câu 1HTTP Request *(3.5 điểm)***

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

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

<https://blogradio.vn/blog-cua-toi/2909?&p=428>

tham số ở đây là p=428

* Phân tích và phán đoán kiểu truy vấn **(0.25 điểm)**

SELECT \* FROM Posts WHERE BlogId = 2909 AND PostId = 428

* Phân tích và phán đoán vị trí của các giá trị tham số đầu vào được sử dụng trong câu truy vấn **(0.5 điểm)**

2909 là ID của blog hoặc người dùng

p là ID của một bài viết hoặc ID trang

* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**

Có thể thay đổi, xoá dữ liệu, hoặc điều khiển toàn bộ hệ thống.

*Lưu ý:*

* *Nói rõ mục đích sử dụng các giá trị kiểm thử*
* *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

**Câu 2 Tham số đầu vào trong Cookie *(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web https://www.google.com/search?q=network.proxy.allow\_hijacking\_localhost&oq=network.proxy.allow\_hijacking\_localhost&gs\_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzU0NmowajGoAgCwAgE&sourceid=chrome&ie=UTF-8&sei=tAX\_Z5SnIZqzwPAPgM-16QI

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

AEC, NID, SG\_SS

* Phân tích và phán đoán kiểu truy vấn, phân tích và phán đoán vị trí của các tham số đầu vào được sử dụng trong câu truy vấn **(0.25 điểm)**
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(3 điểm)**

*Lưu ý:*

* *Nói rõ mục đích sử dụng các giá trị kiểm thử*
* *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

**Câu 3 *(3 điểm)***

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

* Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**
* Phân tích và phán đoán kiểu truy vấn, vị trí của các tham số đầu vào được sử dụng trong câu truy vấn **(0.25 điểm)**
* Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**

*Lưu ý:*

* *Nói rõ mục đích sử dụng các giá trị kiểm thử*
* *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*