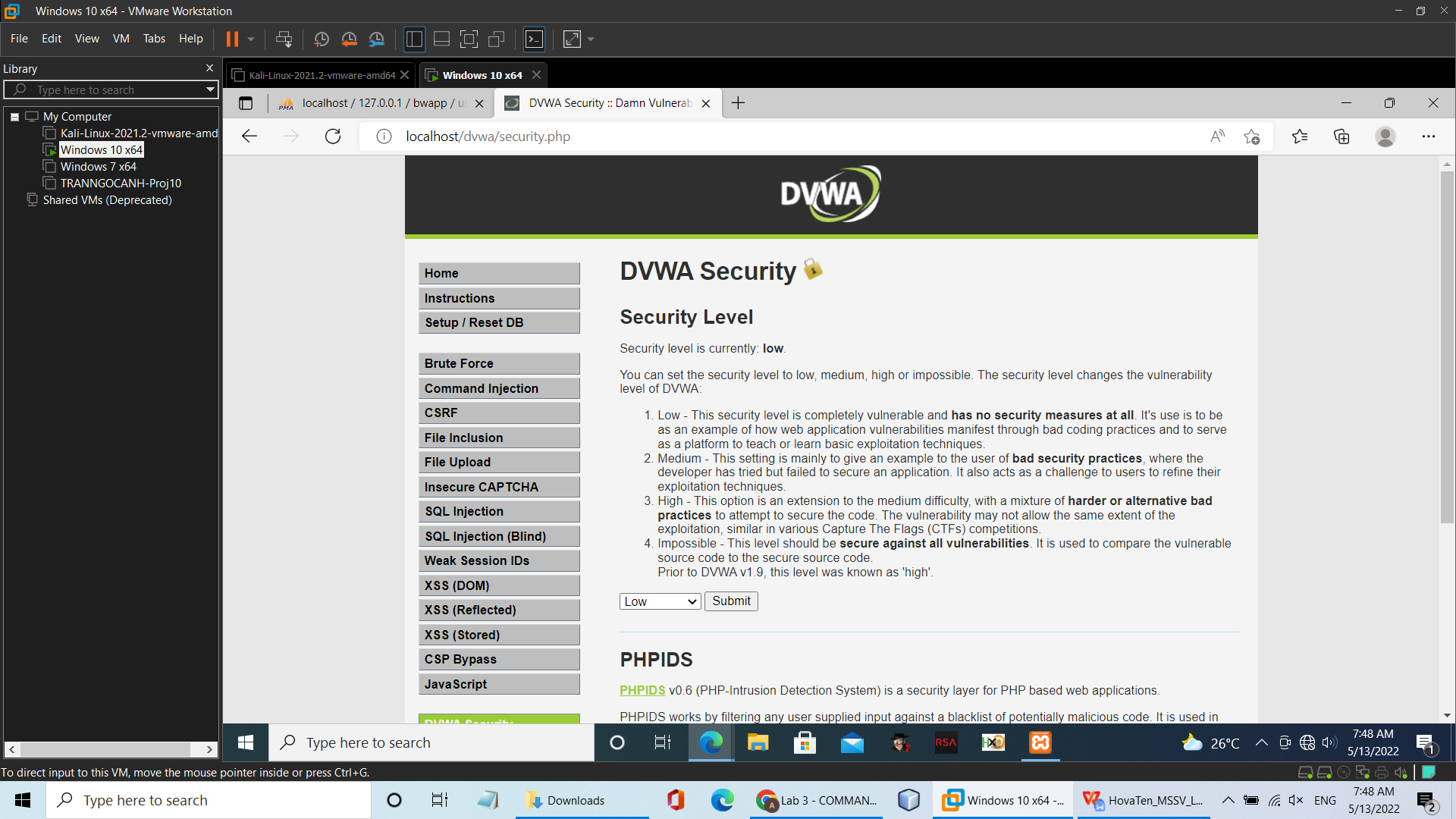
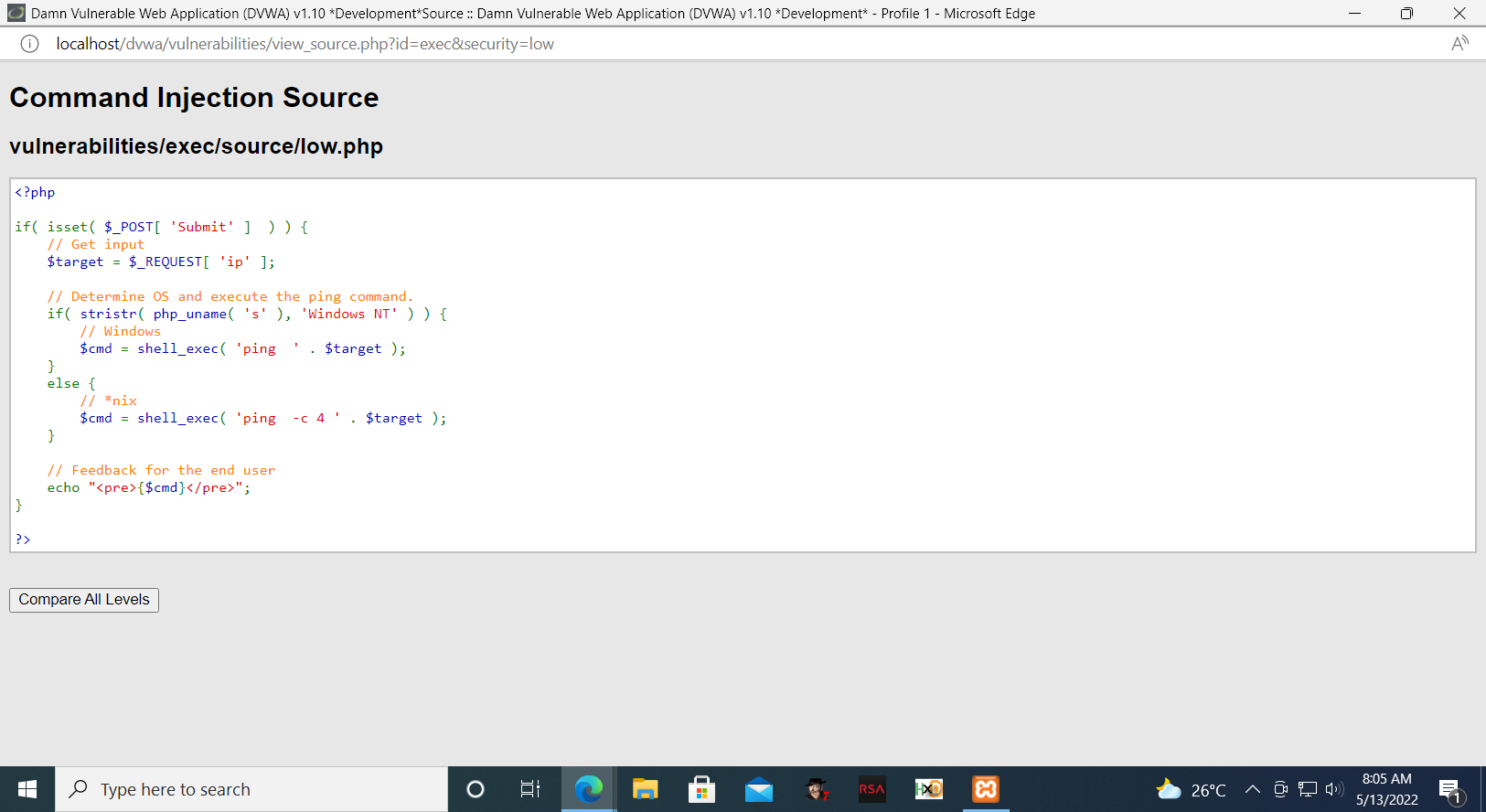
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 13/5/2022 |

**LAB3 : COMMAND EXECUTION BASIC TESTING**

OS Command Injection (hay còn được gọi là shell injection) là một lỗ hổng bảo mật web cho phép kẻ tấn công thực thi các lệnh hệ điều hành (OS) tùy ý trên máy chủ đang chạy service nào đó.

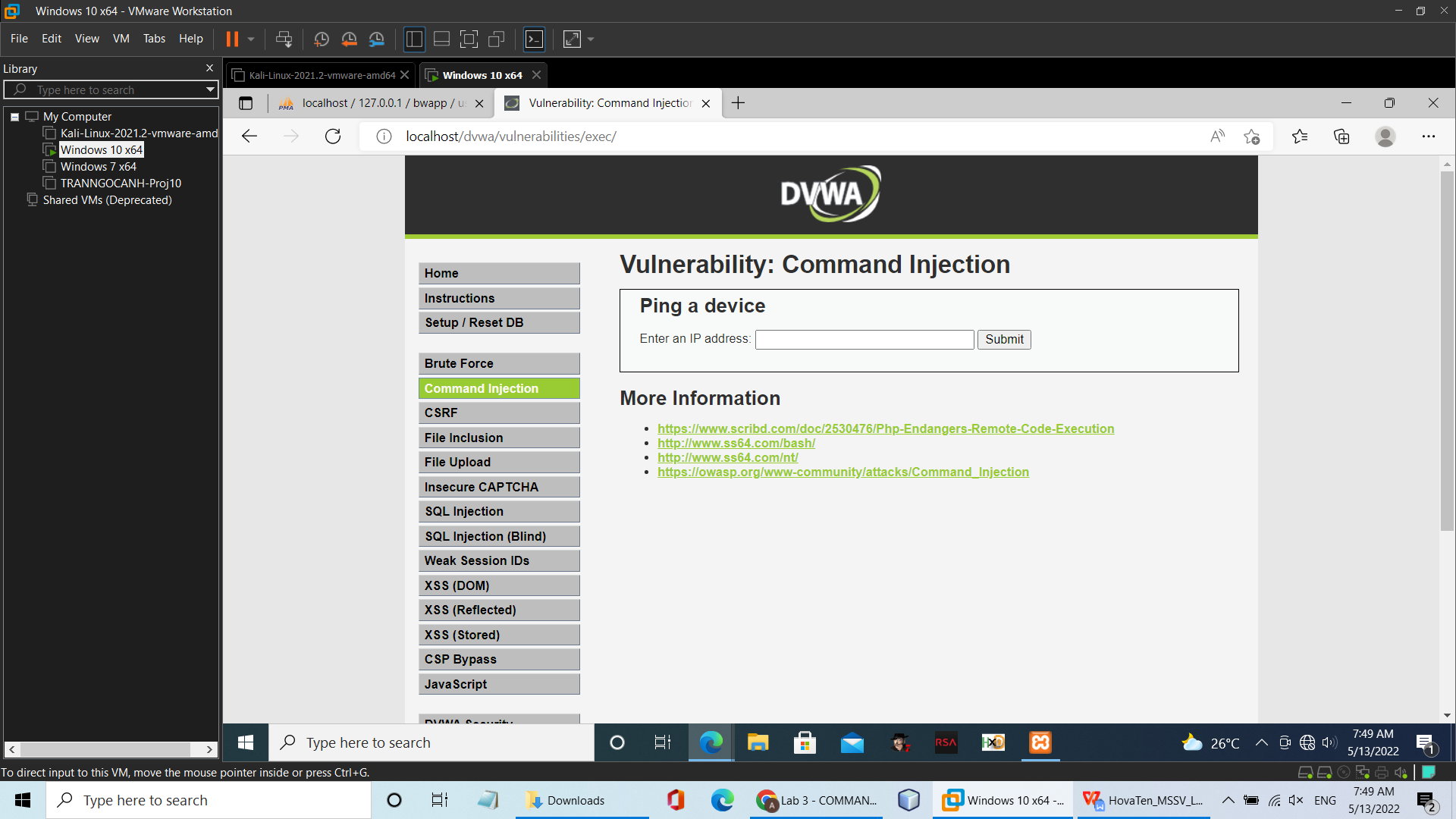
1. **Low**



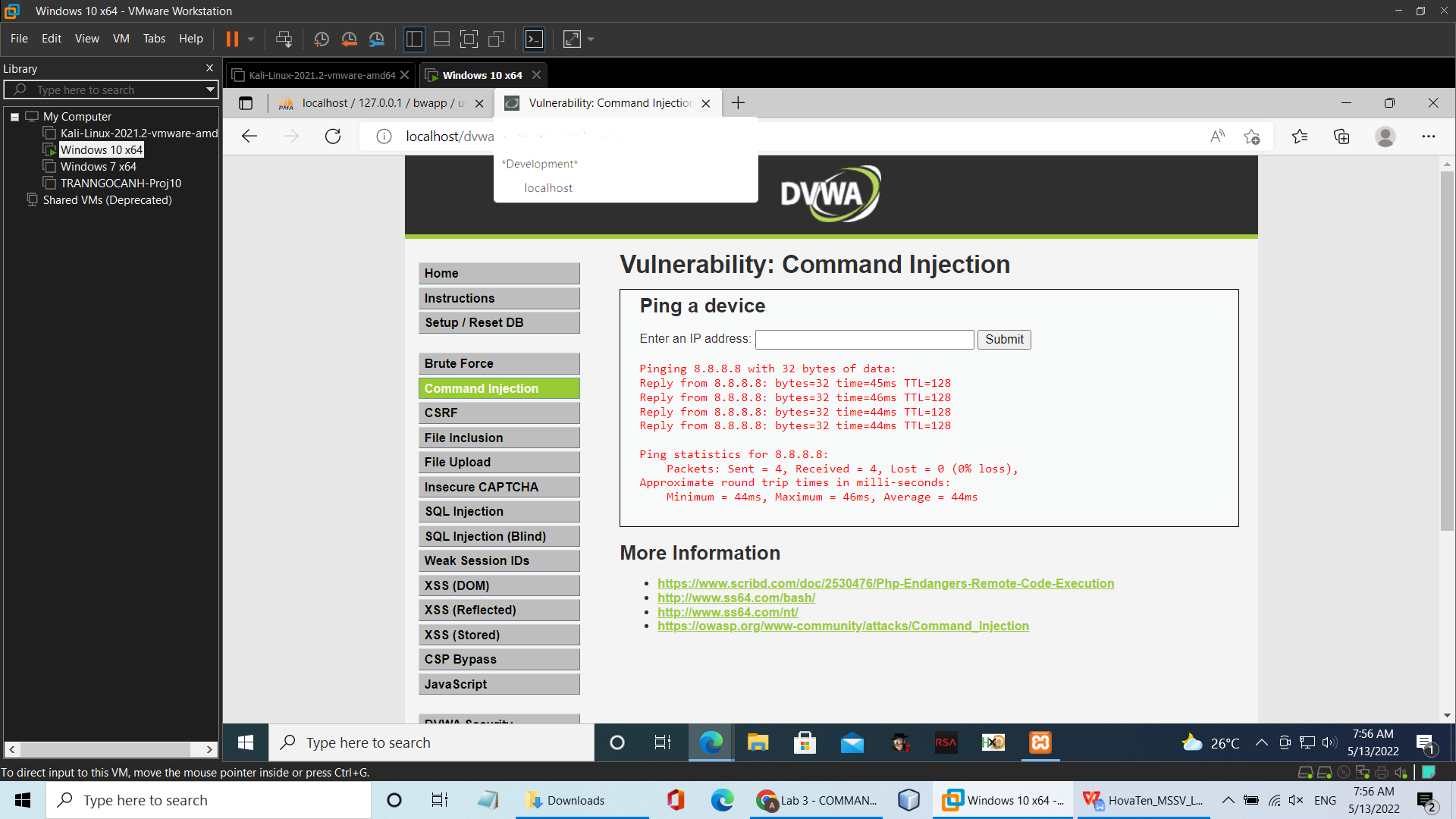


- Nhìn qua source code chúng ta xác định được nguyên nhân do :

**+ Hàm shell\_exec()** trong [PHP](http://php.net/manual/en/function.shell-exec.php) : giúp thực thi câu lệnh được truyền vào thông qua chương trình shell dưới hệ thống và trả về output dưới dạng string . Ở đây đầu vào được nhập tùy ý từ người dùng và không được kiểm tra trước khi đưa vào hàm trên để thực thi.

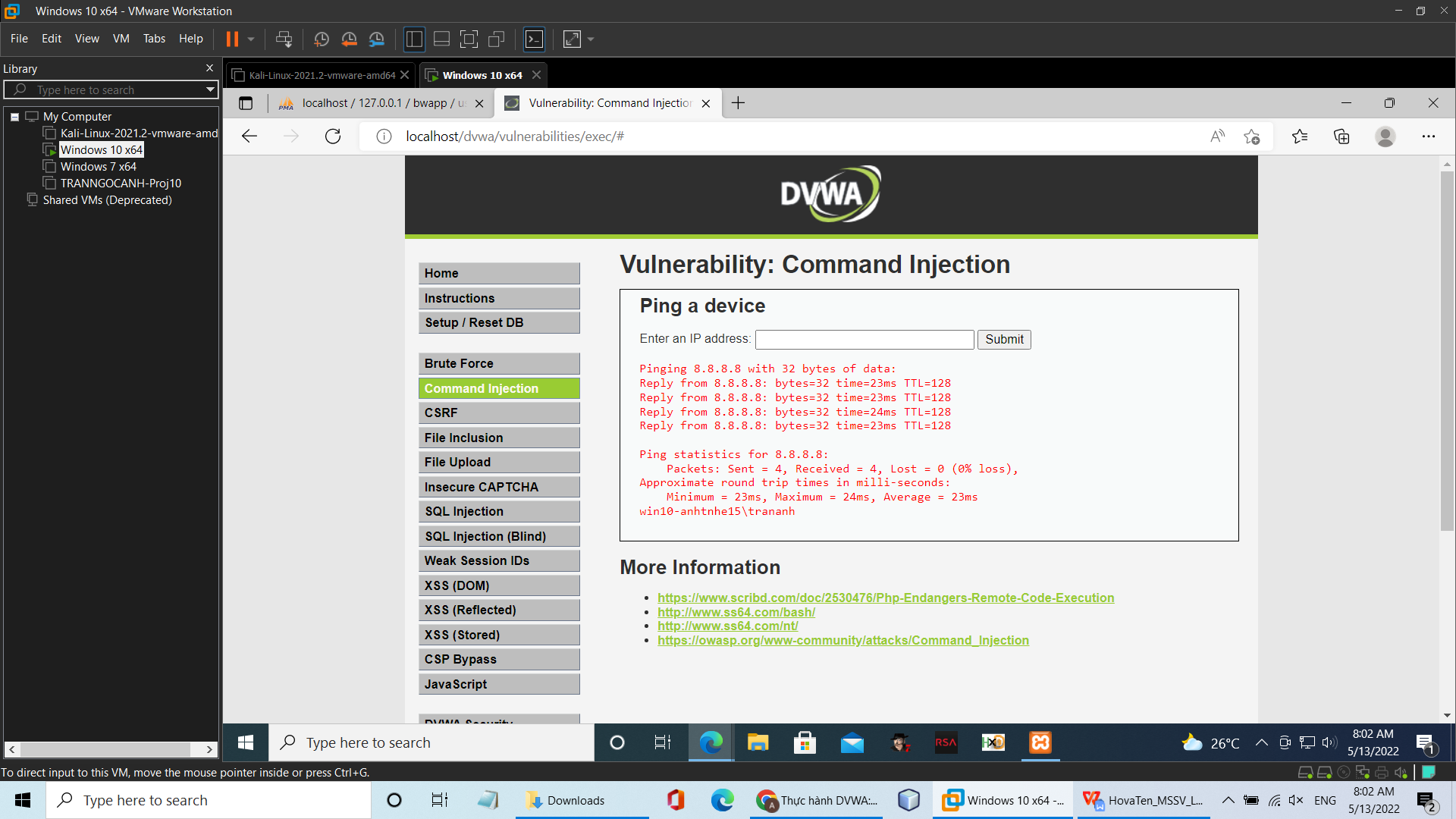


- Chúng ta thử một lệnh ping 8.8.8.8

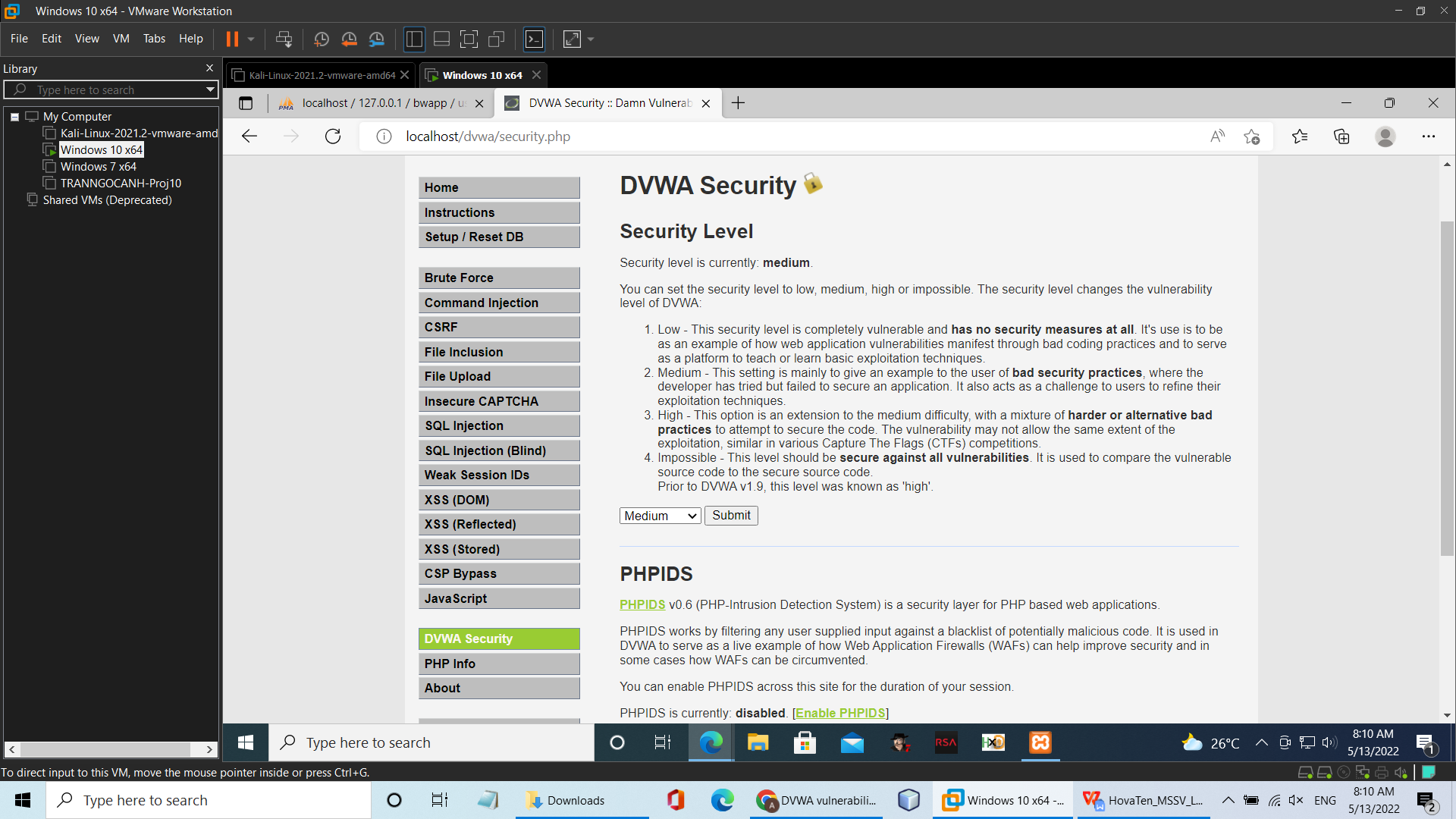


- Kết hợp lệnh ping với chạy một lệnh hệ thống để xem người dùng hiện tại bằng cách nối 2 câu lệnh bằng dấu ‘&&’ .

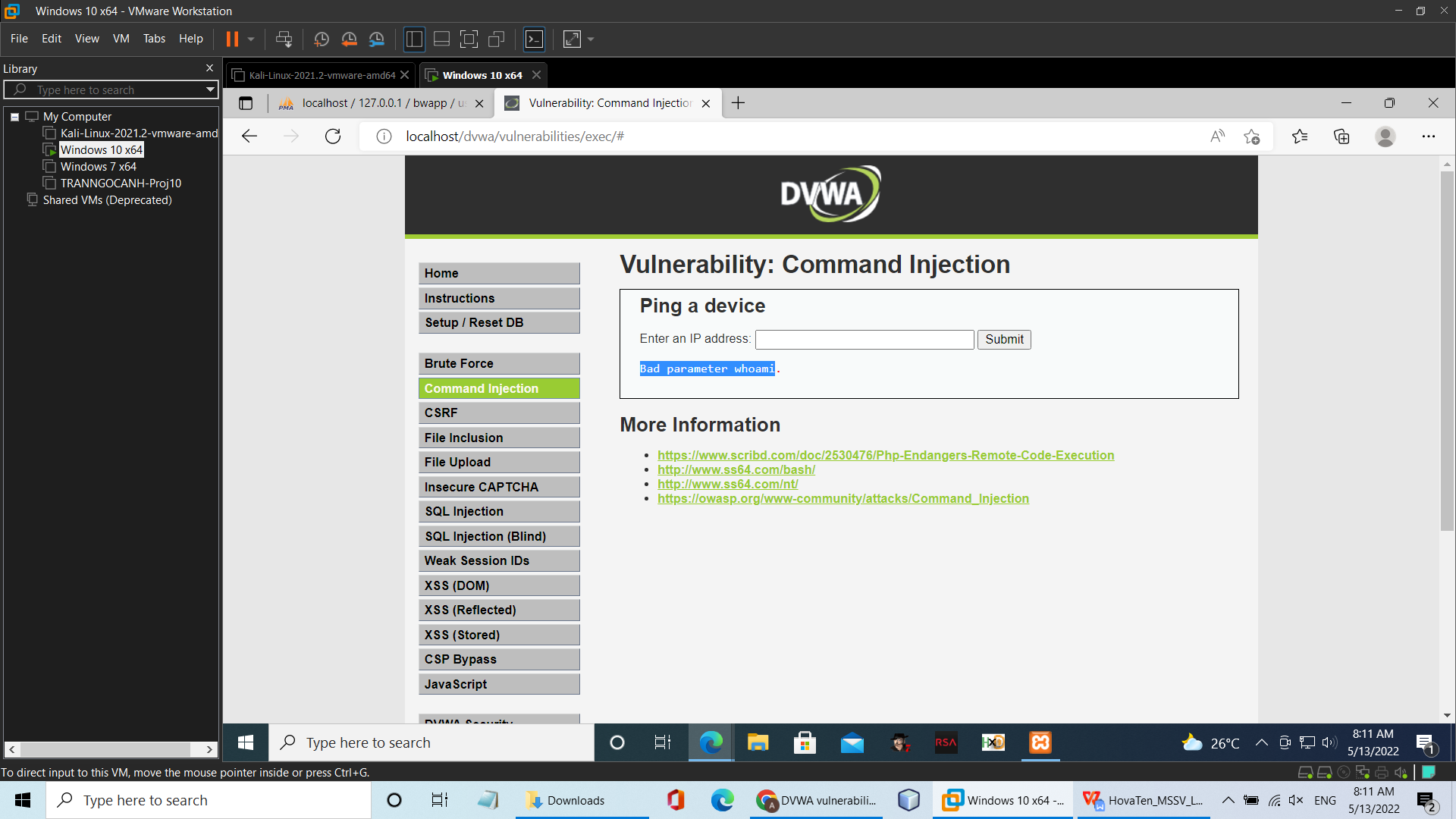
(8.8.8.8 && whoami)



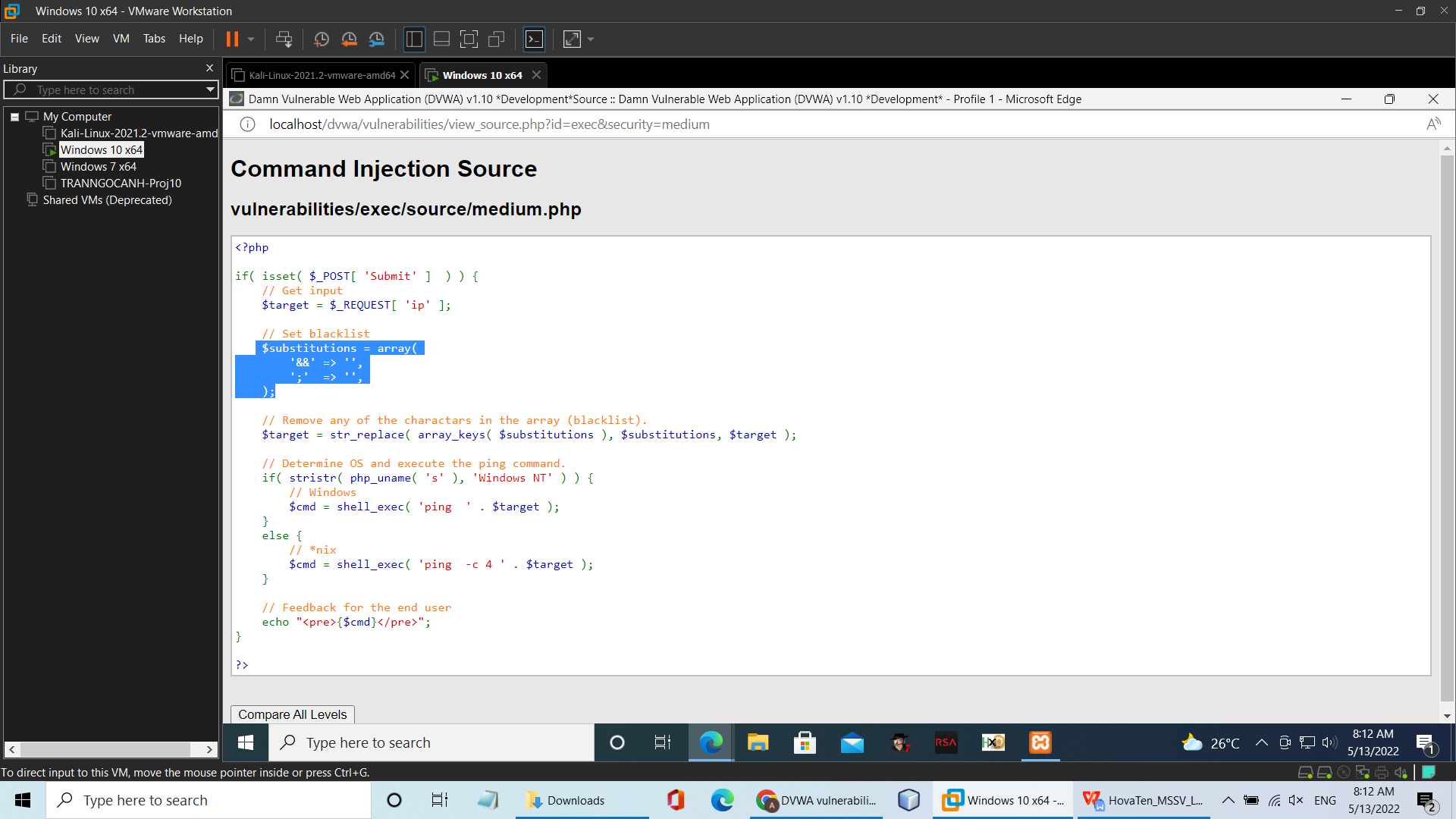
1. **Medium**



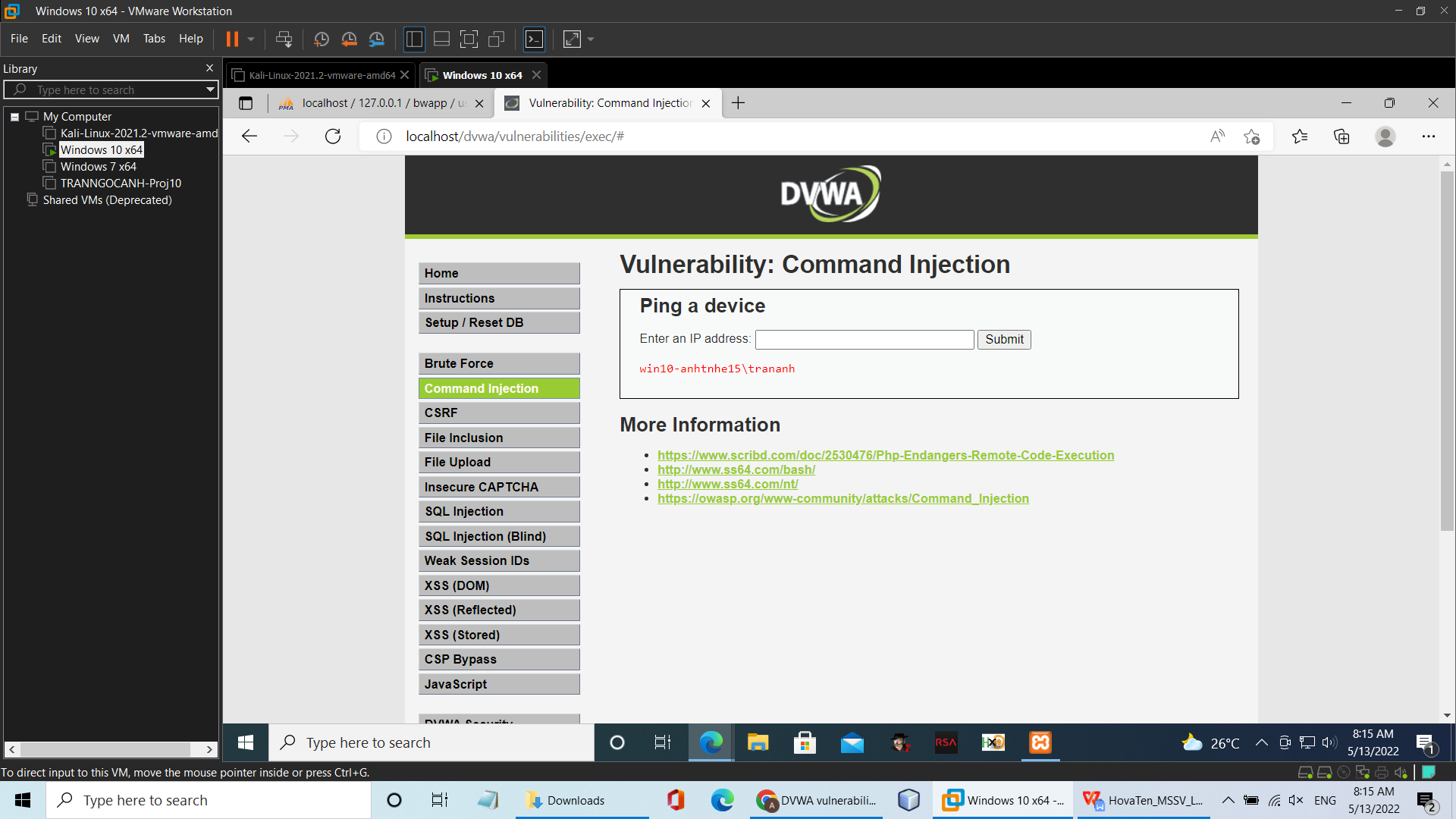
- Ở mức medium chúng ta vẫn thử như mức low nhưng không thực thi được lệnh mình mong muốn.



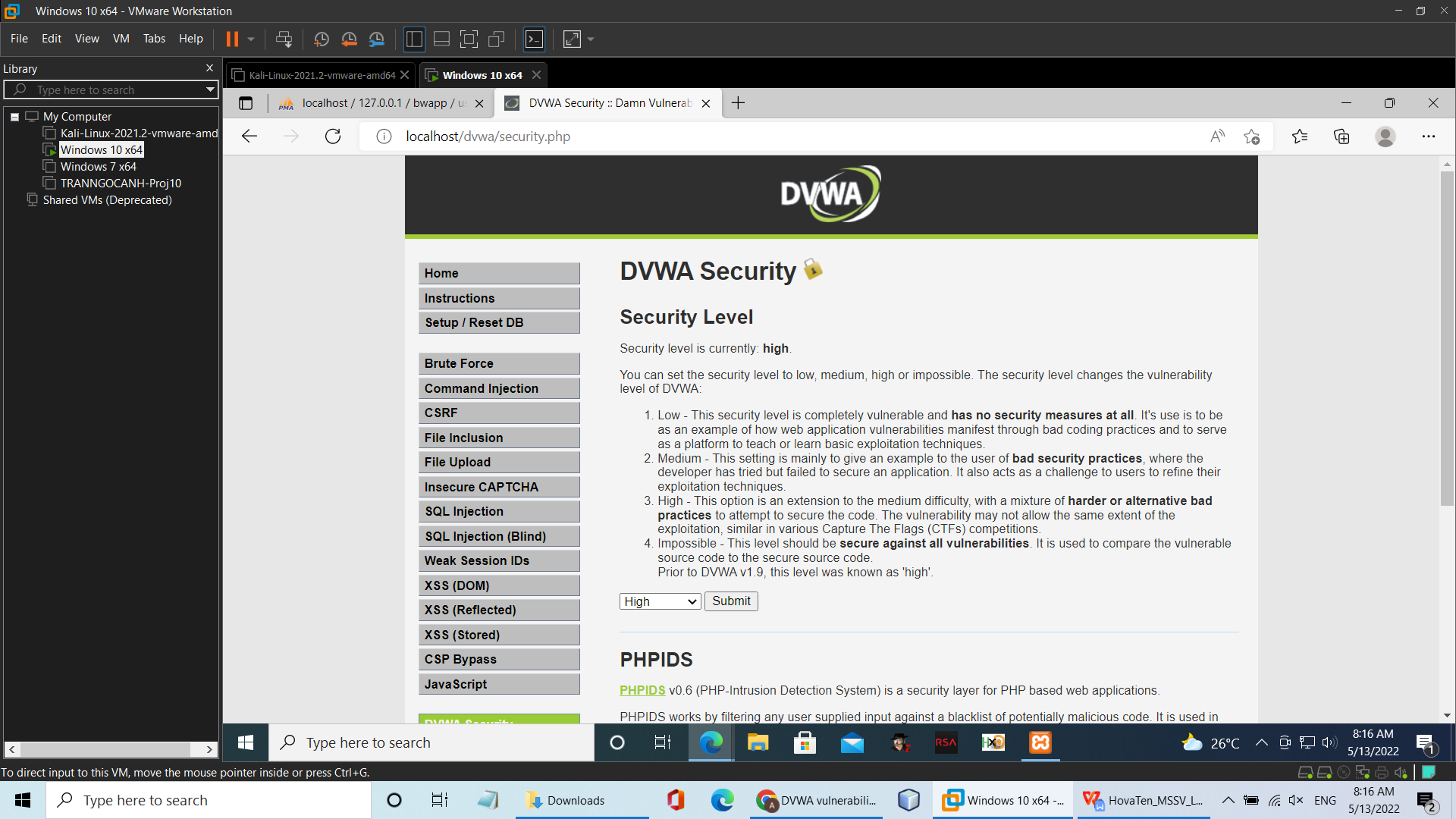
- Lúc này nhìn vào source code chúng ta thấy đầu vào đã được lọc bởi 1 backlist thay thế hai dấu && và ; để tránh nối 2 câu lệnh.



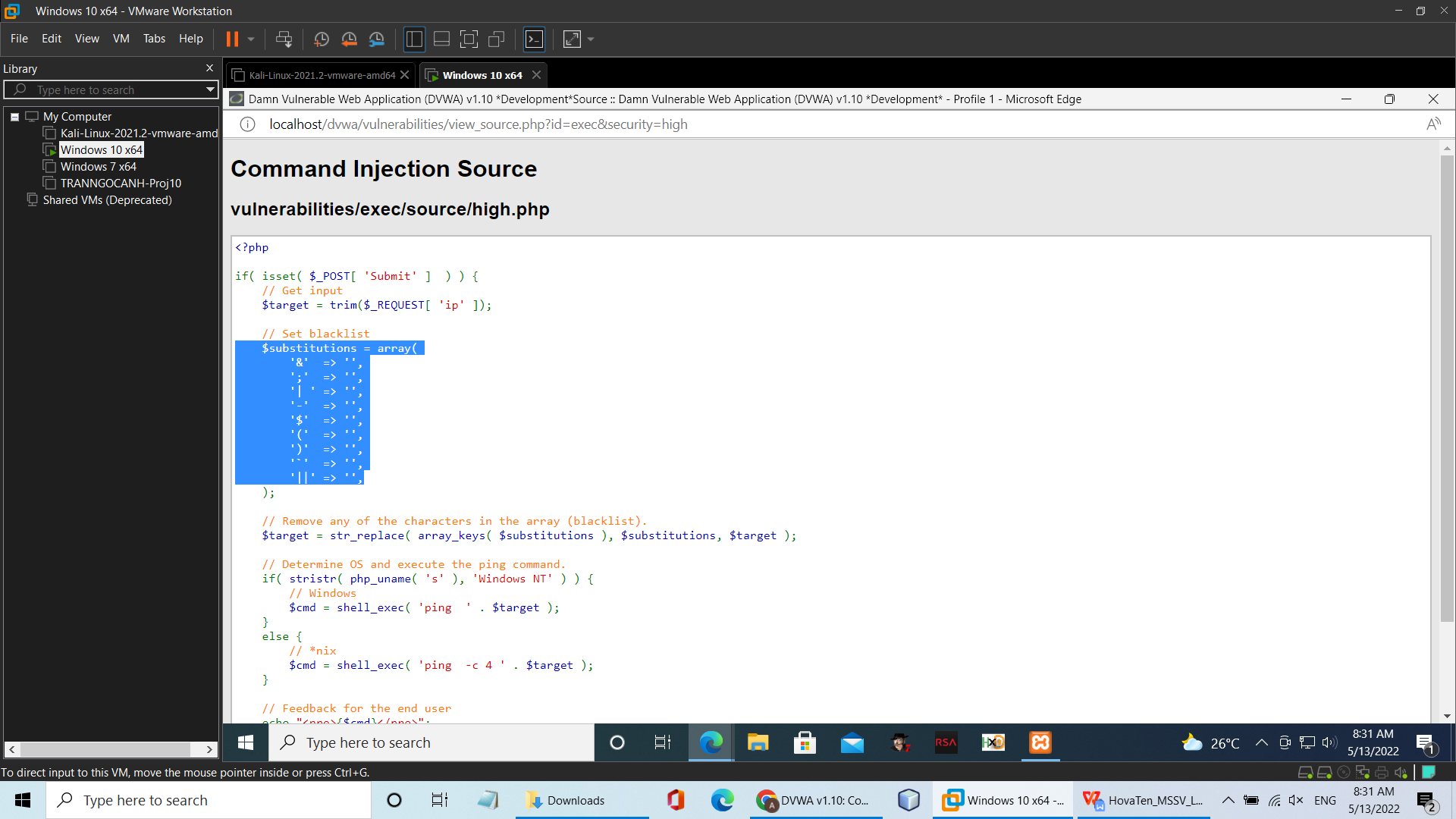
- Chúng ta thử dùng dấu | để nối 2 câu lệnh thay vì dấu ‘&&’ và ‘;’ sẽ giải quyết được mức medium (8.8.8.8 | whoami)



1. **High**



- Ở mức high sẽ khó khai thác hơn do danh sách backlist trở nên nhiều hơn ( xem source code ).



- Ở đây chúng ta sẽ thử câu lệnh 8.8.8.8|whoami thì sẽ vượt qua được mức high do chưa đầu vào chưa validate ‘|’.

