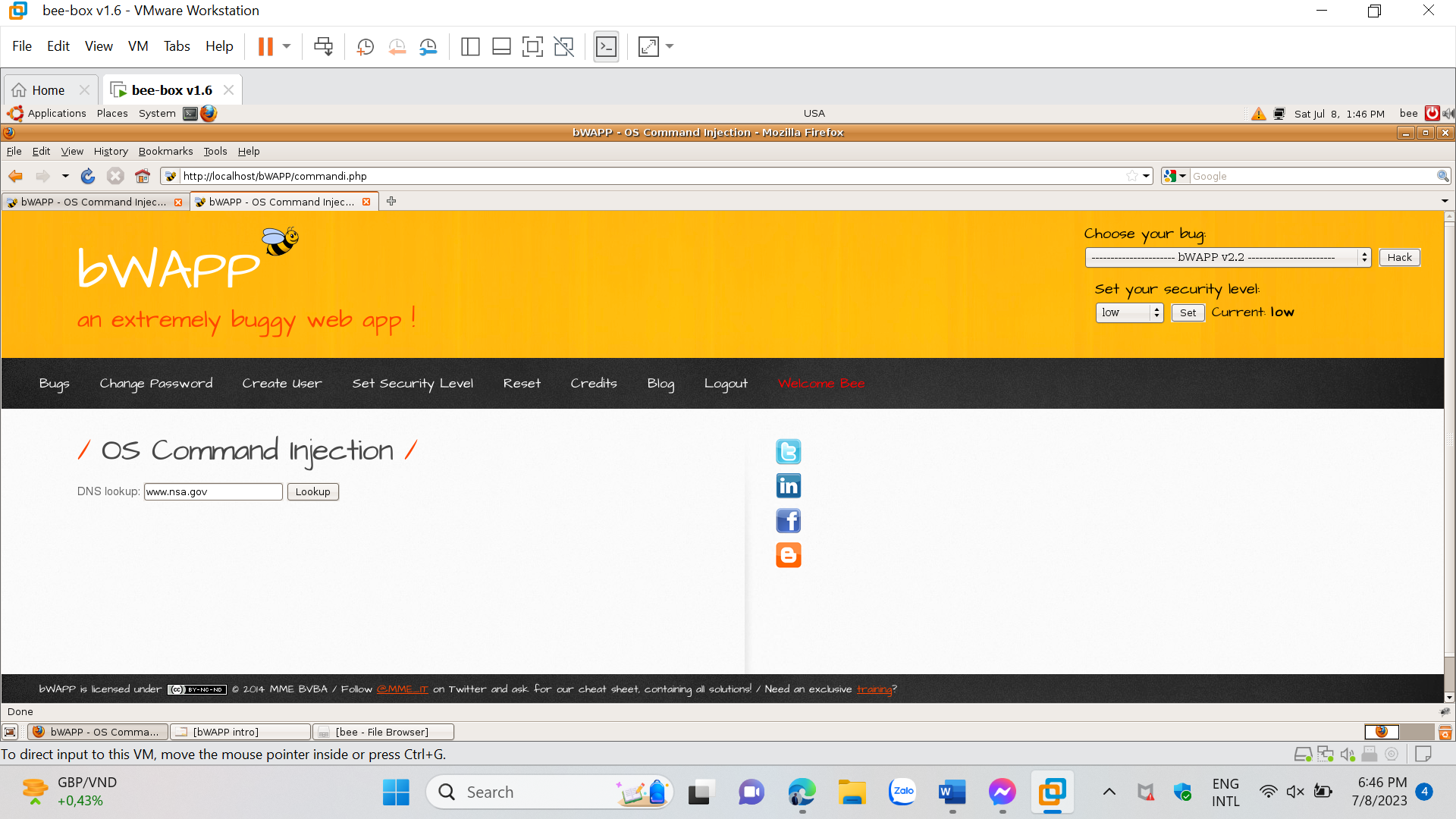
**OS Command Injection Bwapp**



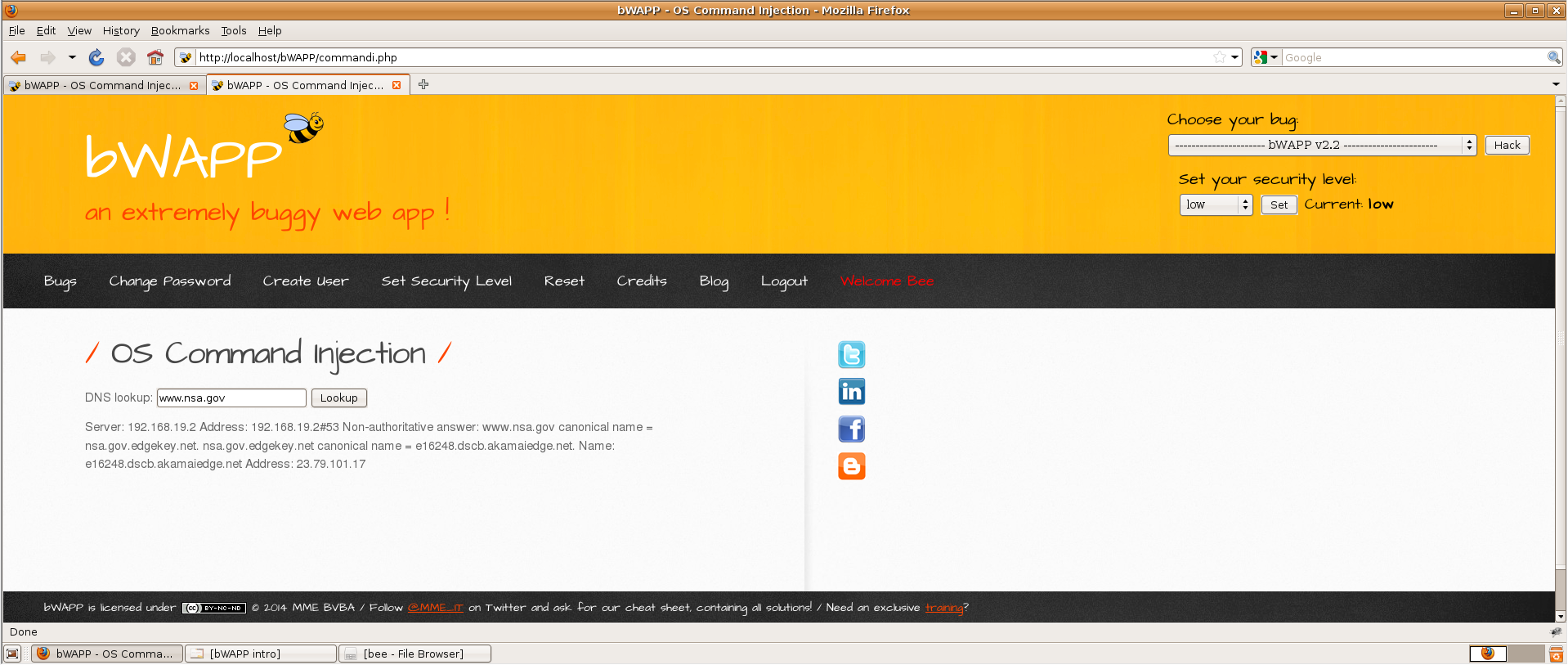
Giới thiệu về OS command injection

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. Kẻ tấn công có thể tận dụng lỗ hổng này để khai thác, lấy thông tin, chuyển cuộc tấn công sang hệ thống khác bên trong tổ chức

Để thực hiện chèn command ta sử dụng một số ký tự có chức năng phân tách lệnh, cho phép các lệnh nối với nhau như : &, &&, |, ||, ;, \n, `, $()

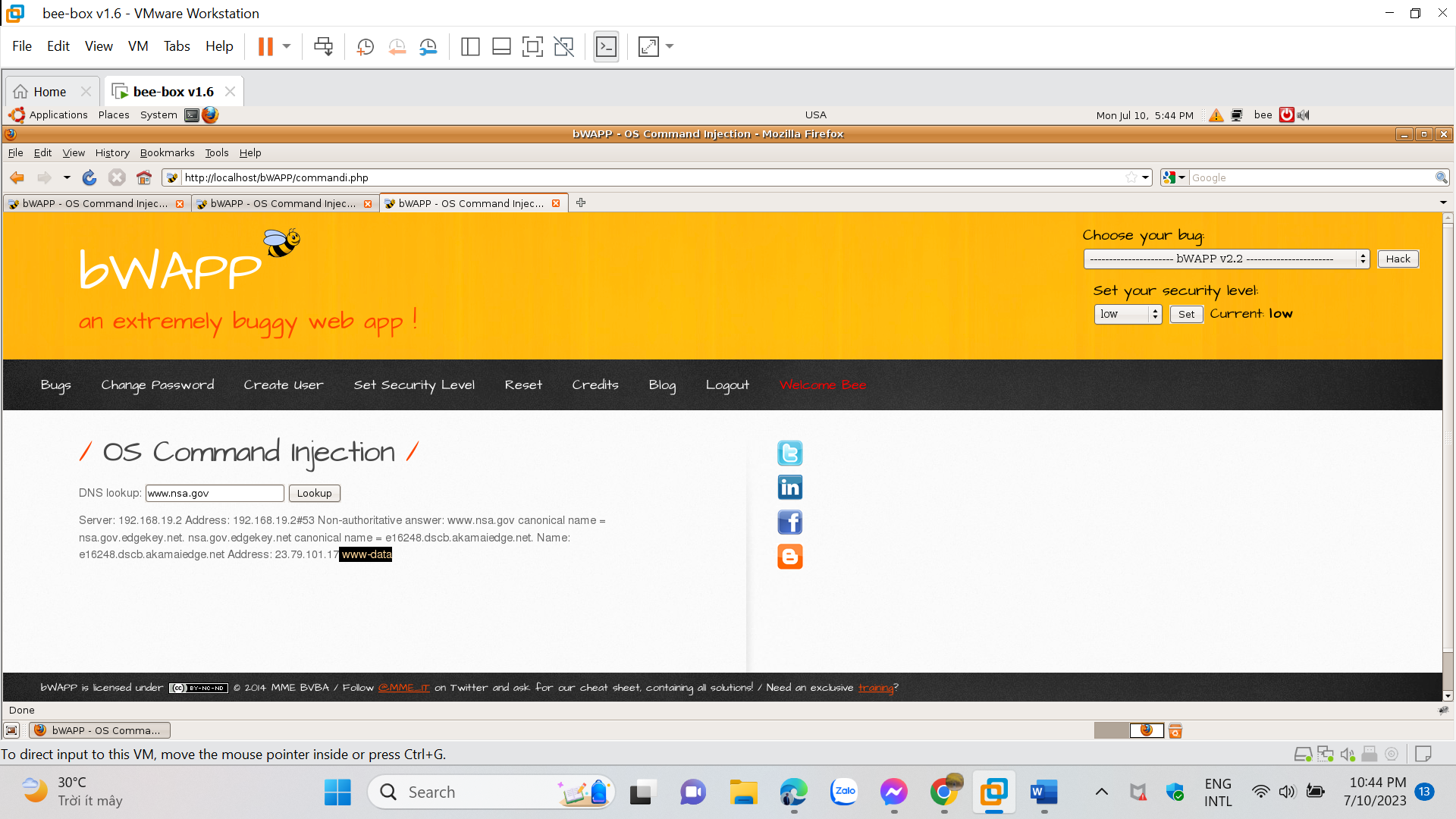
Level : Low

ở level này bwapp sử dụng shell\_exec("nslookup " . commandi($target))- 1 nslookup tool để tìm các bản ghi trả về Dns record – cung cấp thông tin về tên miền và địa chỉ ip

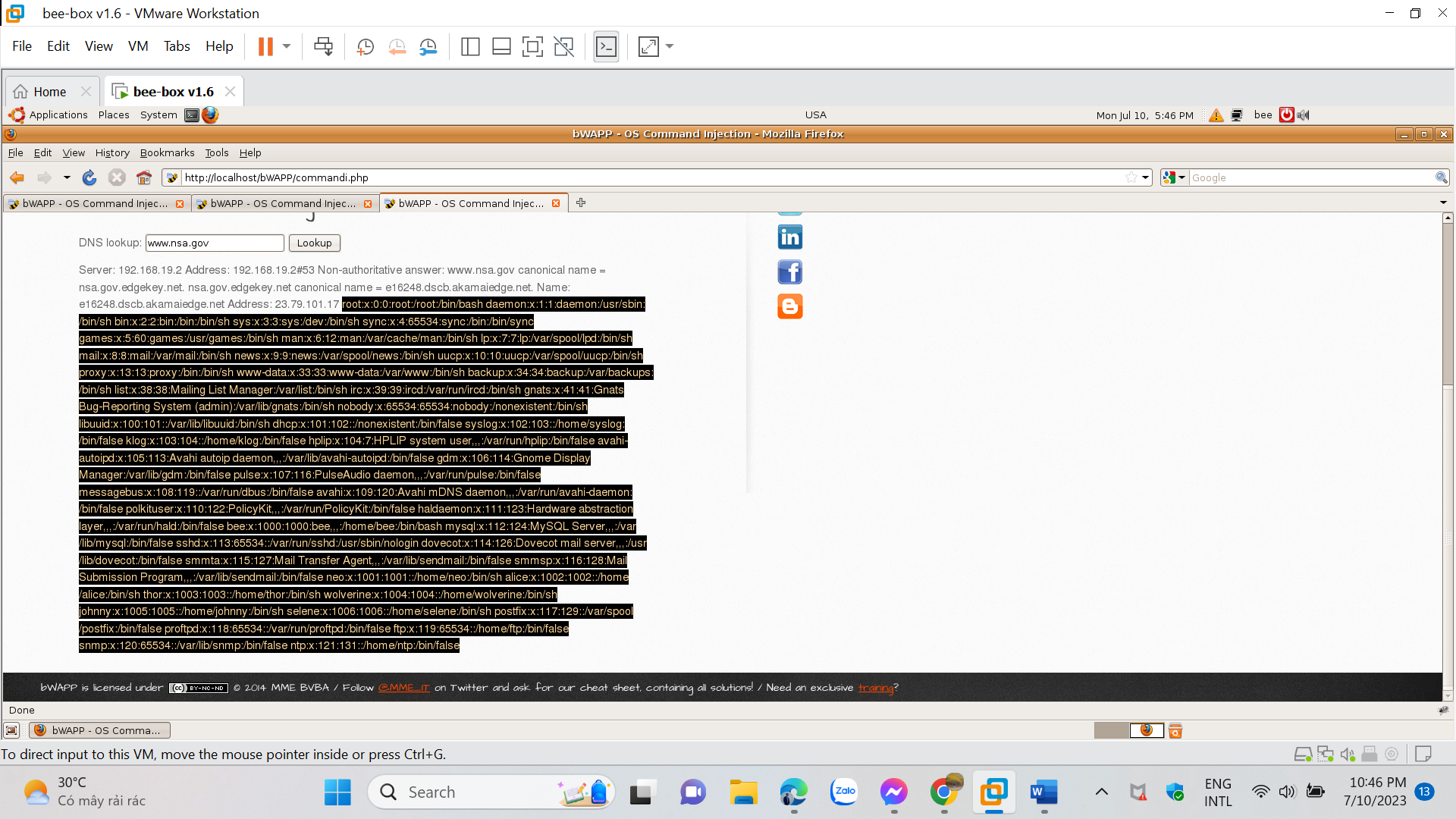


Sau khi thực thi command nslookup [www.www.nsa.gov](http://www.www.nsa.gov) . ta sẽ thử chèn command độc theo cú pháp như sau www.www.nsa.gov | {malicious command}

Ta thử command sau www.www.nsa.gov &&whoami hoặc www.www.nsa.gov ;whoami



Kết quả trả về www-data - chính là người dung hiện tại của hệ điều hành trên.

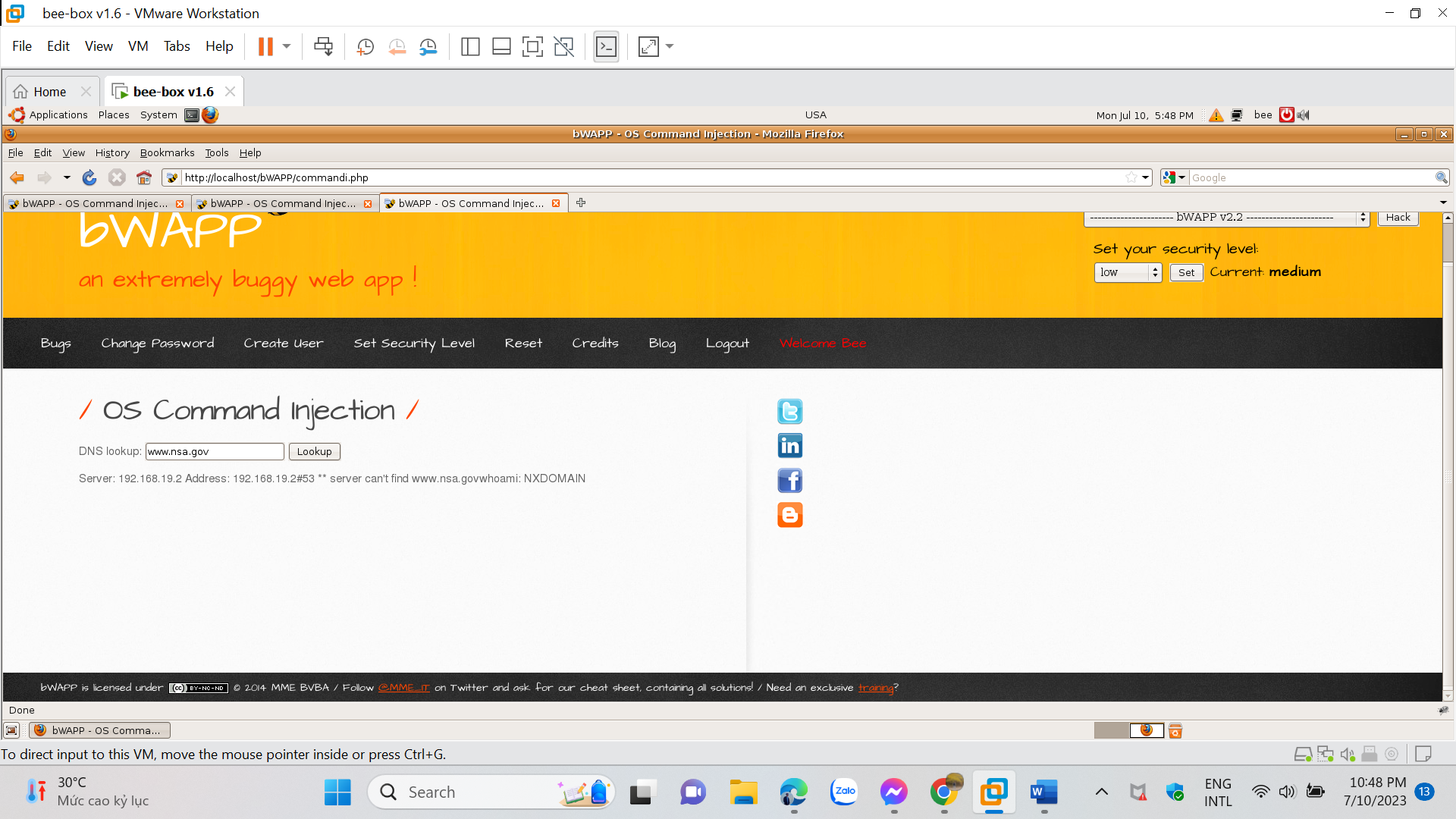
Ta thử 1 command khác là www.www.nsa.gov &&cat /etc/passwd hoặc www.www.nsa.gov &&cat /etc/passwd 

Hệ thống trả về 1 loạt các thông tin của các user ở hệ điều hành

Level : medium

ở mức độ này hệ thống đã được tăng cường tính bảo mật

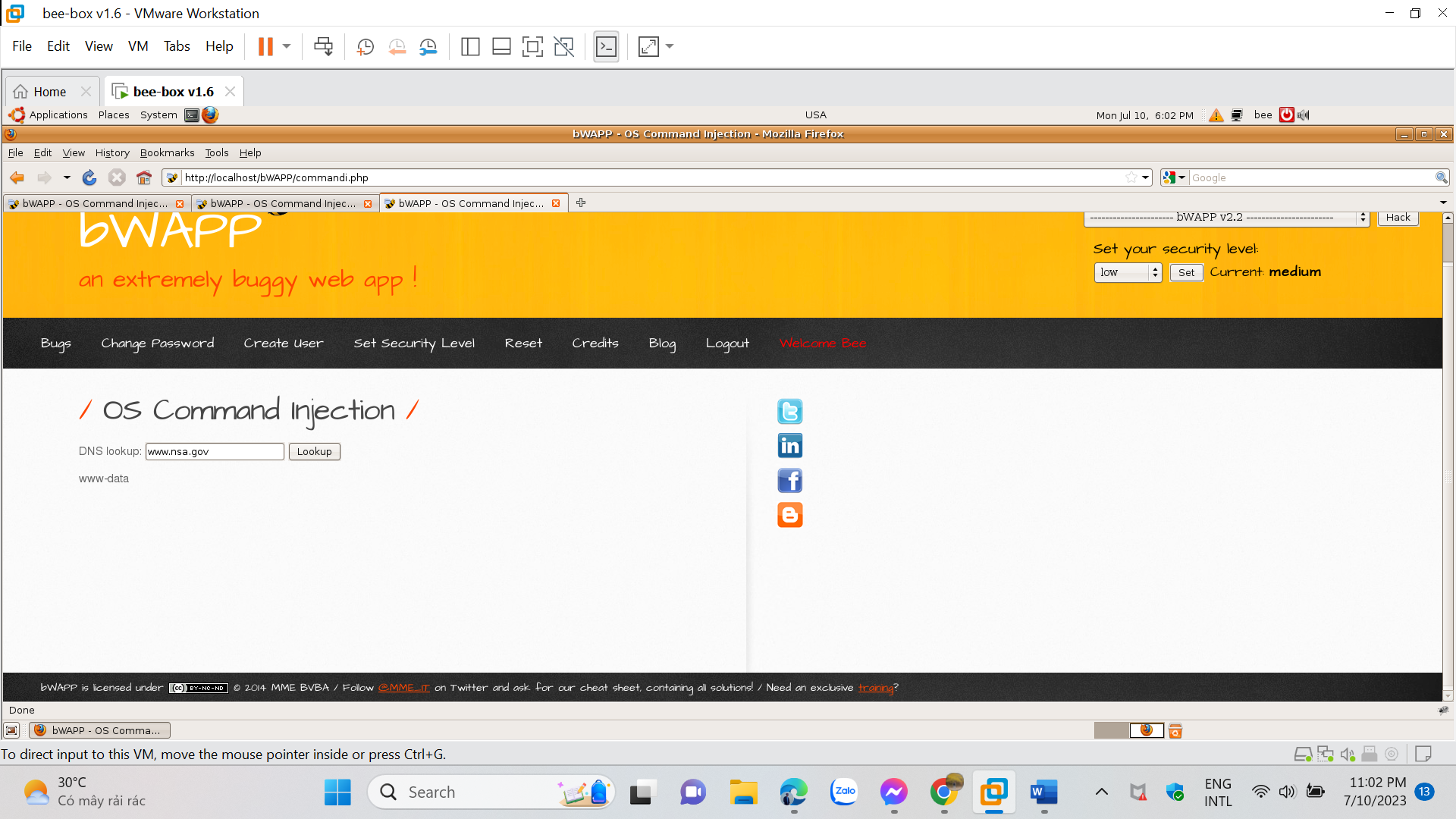
ta thử sử dụng các command ở level trước lại như www.www.nsa.gov &&whoami hoặc www.www.nsa.gov ;whoami



Ta có thể thấy hệ thống đã chặn được các command có chứa dấu &,&&,; và không trả về bất kỳ thông tin nào cả

Với level này ta sẽ sử dụng pipe command vs cú pháp sau www.www.nsa.gov | {malicious command}

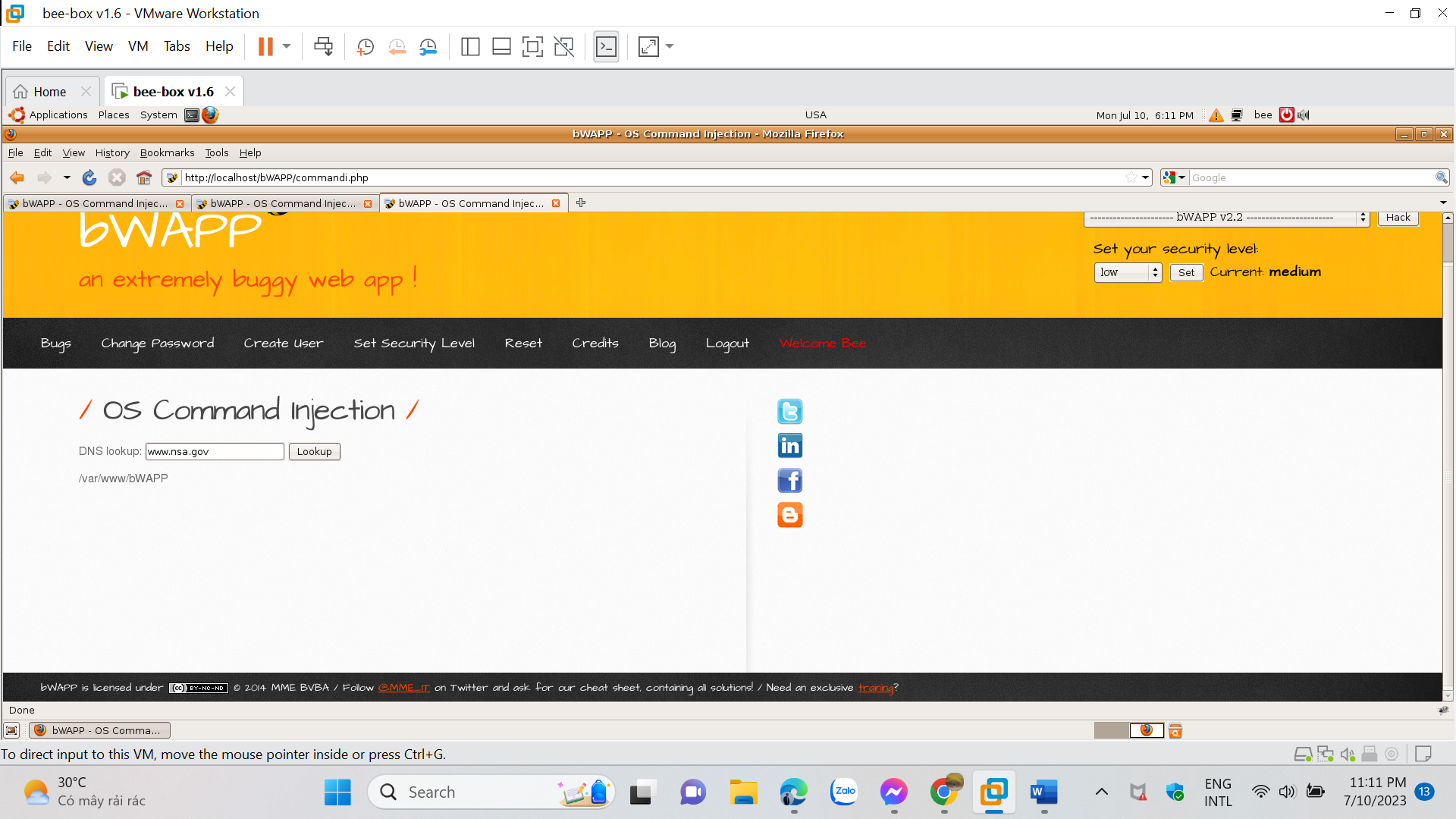
Pipe command là dạng câu lệnh ghép nối 2 lệnh vs output của lệnh trước là input của lệnh sau



Kết quả trả về giống như ở trên level : low

Ta sẽ thử sử dụng 1 số command khác dưới dạng này

www.www.nsa.gov | pwd



Kết quả trả về thư mục hiện tại của trang web

Cách phòng chống