

# MỘT

## DANH SÁCH KIỂM TRA HACK API



Phươ ng pháp kiểm thử (xem Chươ ng

0) Xác định phươ ng pháp tiếp cận: hộp đen, hộp xám hay hộp trắng? (trang 4-6)

Trình sát bị động (xem Chươ ng 6) Tiến

hành khám phá bề mặt tấn công (trang 124-132) Kiểm tra

các bí mật bị lộ (trang 133-136)

Active Reconnaissance (xem Chươ ng 6)

Quét các cổng và dịch vụ đang mở (trang 138) Sử

dụng ứng dụng như dự định (trang 137) Kiểm tra

ứng dụng web bằng DevTools (trang 139-142) Tìm kiếm các thư

mục liên quan đến API (trang 143) -146) Khám phá các

điểm cuối API (trang 146-148)

Phân tích điểm cuối (xem Chương 7)

Tìm và xem xét tài liệu API (trang 156-159)      Thiết kế ngữ ợc API  
(trang 161-164)      Sử dụng API như dự kiến (trang 167-  
168)      Phân tích các phản hồi đối với việc tiết lộ  
thông tin quá mức triển lãm dữ liệu  
chắc chắn và lỗi logic nghiệp vụ (trang 169-174)

Kiểm tra xác thực (xem Chương 8)      Tiến

hành kiểm tra xác thực cơ bản (trang 180-186)      Tấn công và thao  
túng mã thông báo API (trang 187-197)

Tiến hành Fuzzing (xem Chương 9)

Fuzzing tất cả mọi thứ (trang 202-218)

Kiểm tra ủy quyền (xem Chương 10)      Khám

phá các phư ơ ng pháp xác định tài nguyên (trang 224-225)      Kiểm tra  
BOLA (trang 225-227)      Kiểm tra BFLA  
(trang 227-230)

Thử nghiệm gán khối lư ợng (xem Chương 11)

Khám phá các tham số tiêu chuẩn đư ợc sử dụng trong các yêu cầu (trang 238-  
240)      Thử nghiệm gán khối lư ợng (trang 240-243)

Kiểm tra tiêm nhiễm (xem Chương 12)

Khám phá các yêu cầu chấp nhận đầu vào của ngư ời dùng (trang  
250)      Kiểm tra XSS/XAS (trang 251-253)

Thực hiện các cuộc tấn công dành riêng cho cơ sở dữ liệu  
(trang 253-259)      Thực hiện tiêm nhiễm hệ điều hành (trang 259) -260)

Kiểm tra giới hạn tốc độ (xem Chương 13)

Kiểm tra sự tồn tại của giới hạn tốc độ (trang 276)

Kiểm tra các phư ơ ng pháp tránh giới hạn tốc độ (trang 276-278)

Kiểm tra các phư ơ ng pháp vư ợt qua giới hạn tốc độ (trang 278-284)

Kỹ thuật né tránh (xem Chương 13)      Thêm

chuỗi kết thúc vào các cuộc tấn công (trang 270-271)      Thêm

trư ờng hợp chuyển sang tấn công (trang 271-272)      Mã hóa

tải trọng (trang 272)      Kết hợp các

kỹ thuật trốn tránh khác nhau (trang 273-275)      Rửa sạch và lặp lại

hoặc áp dụng các kỹ thuật né tránh cho tất cả các cuộc tấn công trư ớc đó  
(trang 322)