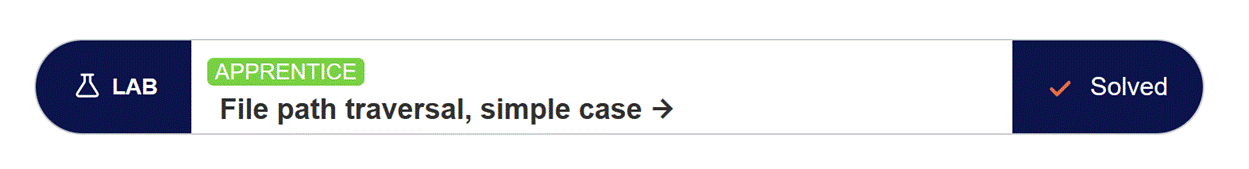
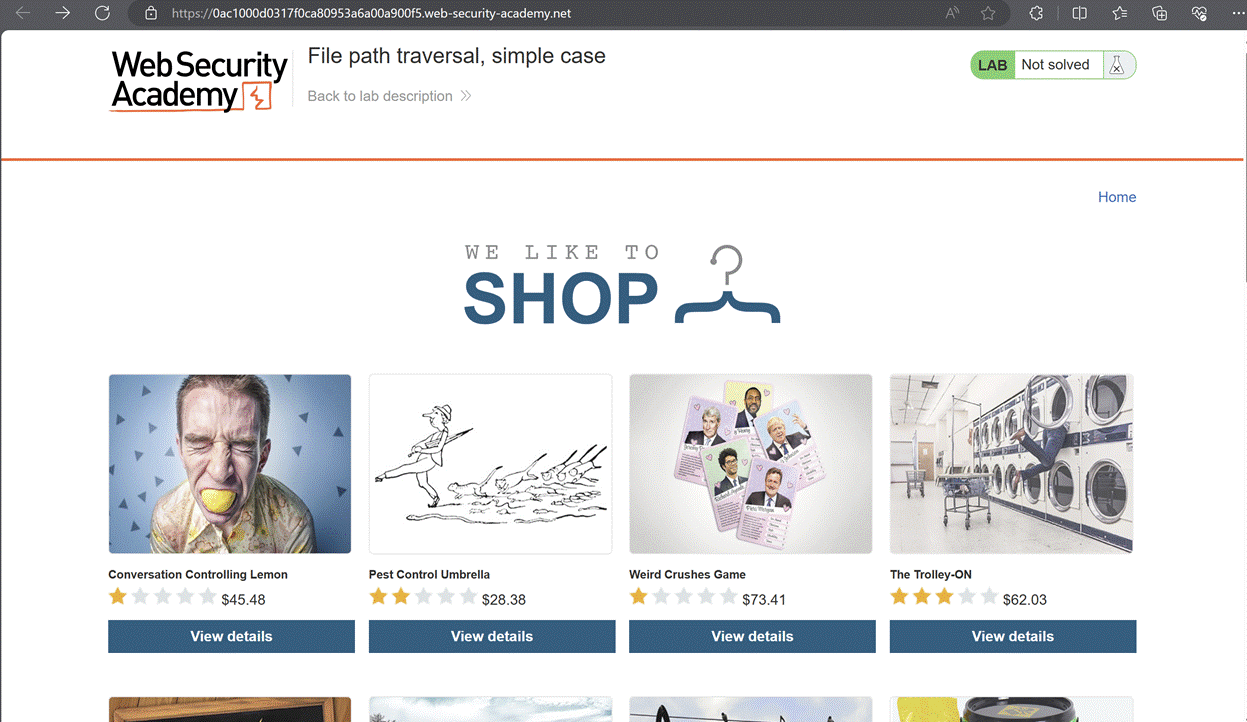
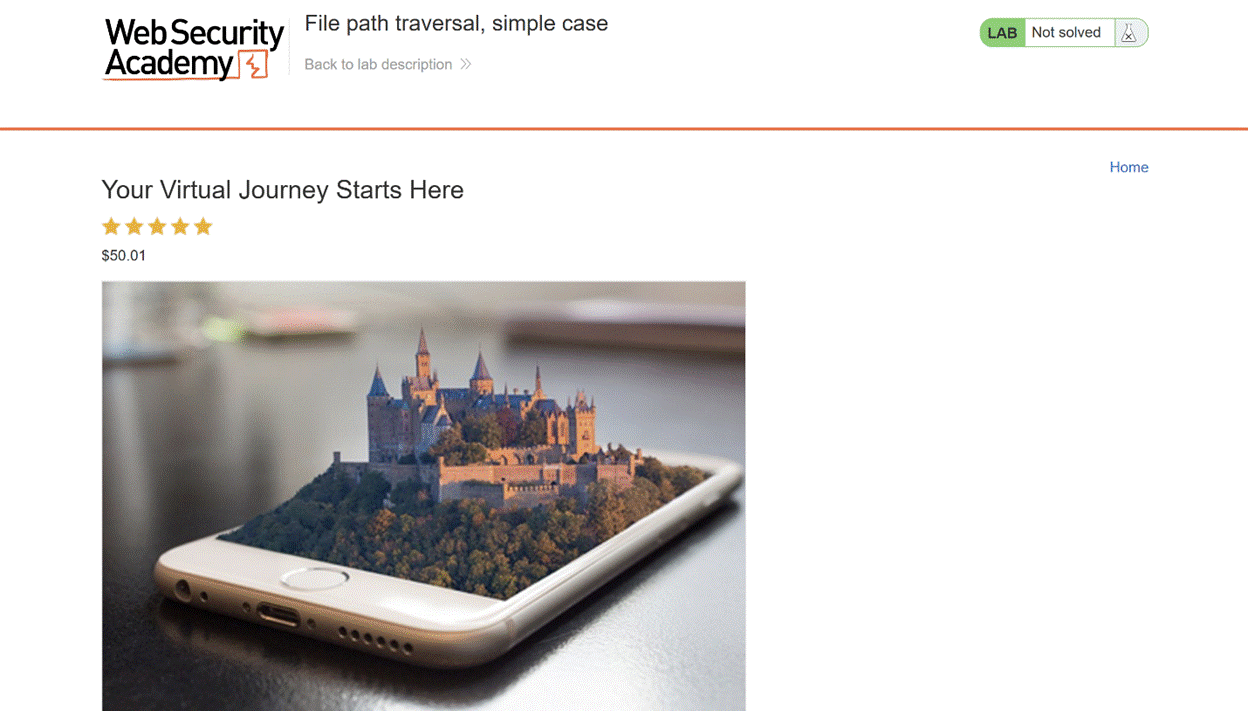
**PATH TRAVERSAL**



Giao diện bài lab như sau

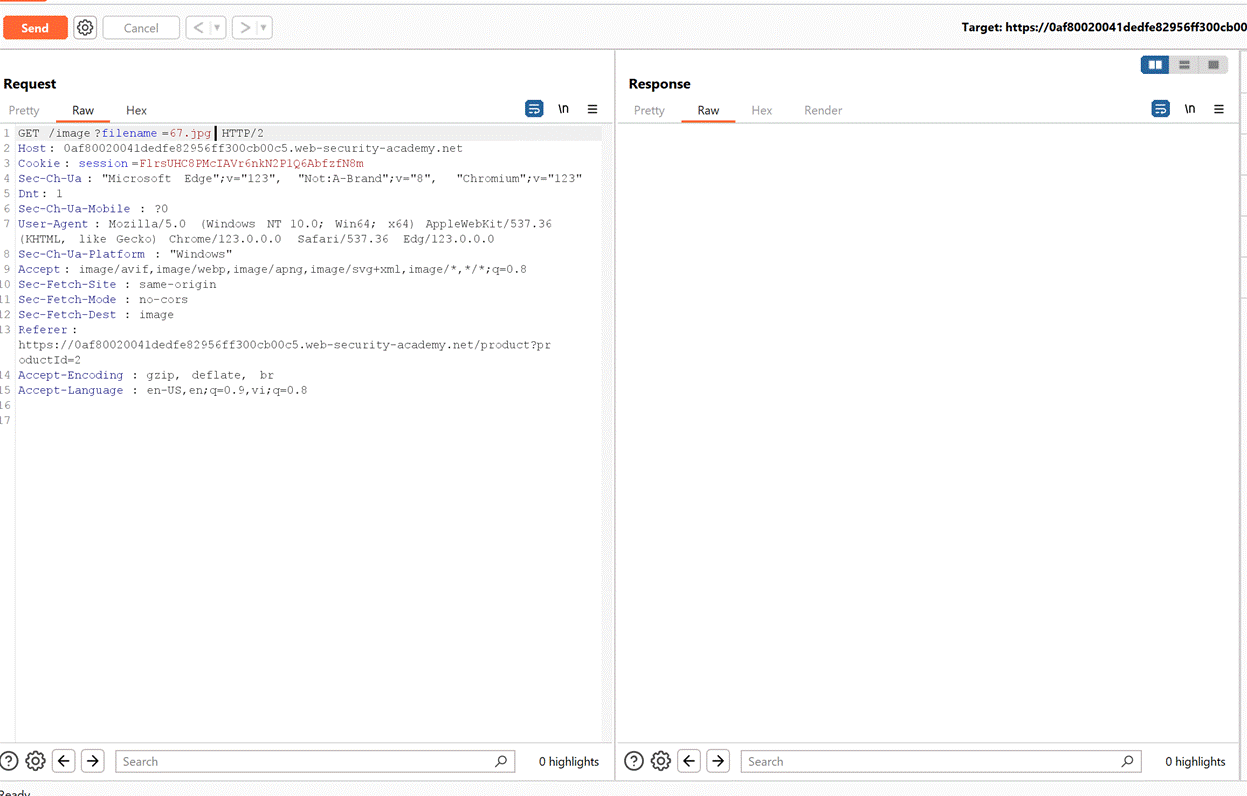


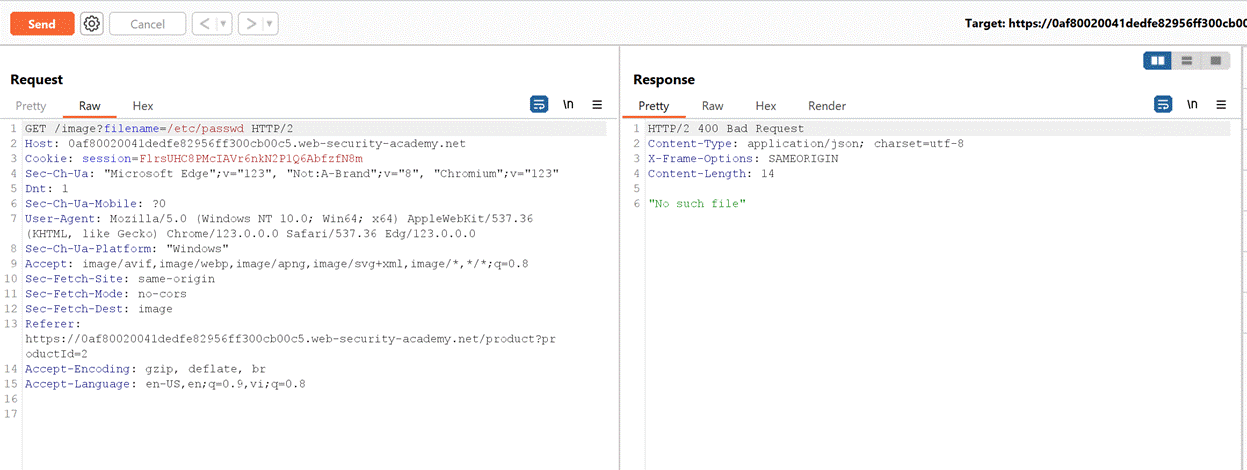
Ta thử vào xem 1 sản phẩm và sử dụng Burpsuite để bắt gói tin

Ta nhận thấy có thể tồn tại 1 lỗ hổng path traversal ở gói tin GET /image?filename=67.jpg

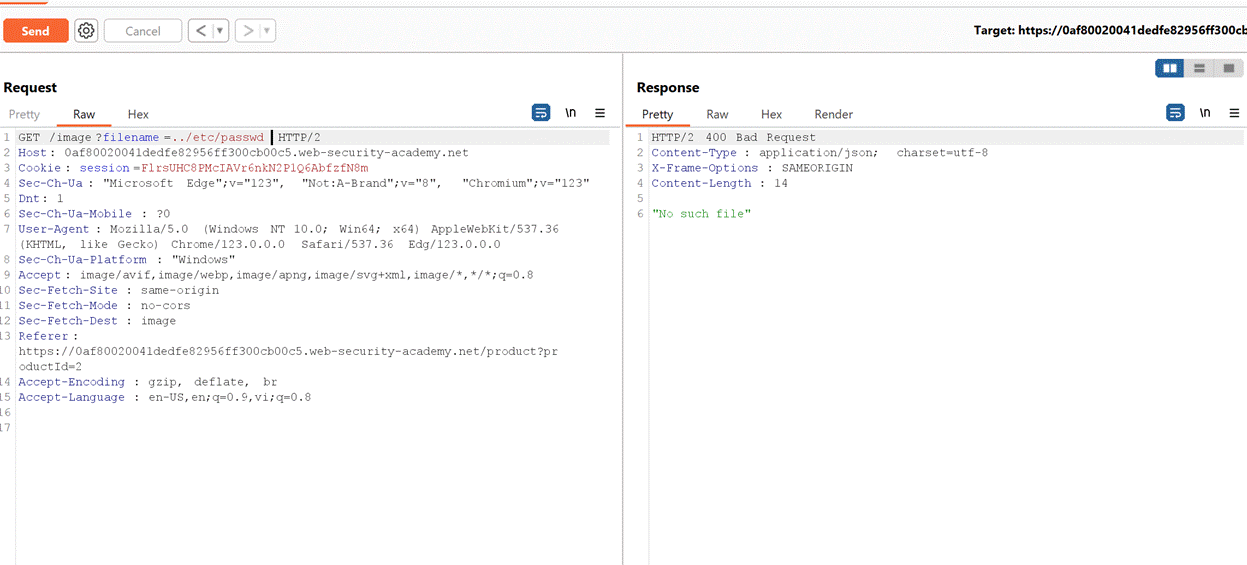


Ta chuyển gói tin sang repeater để tiến hành khai thác

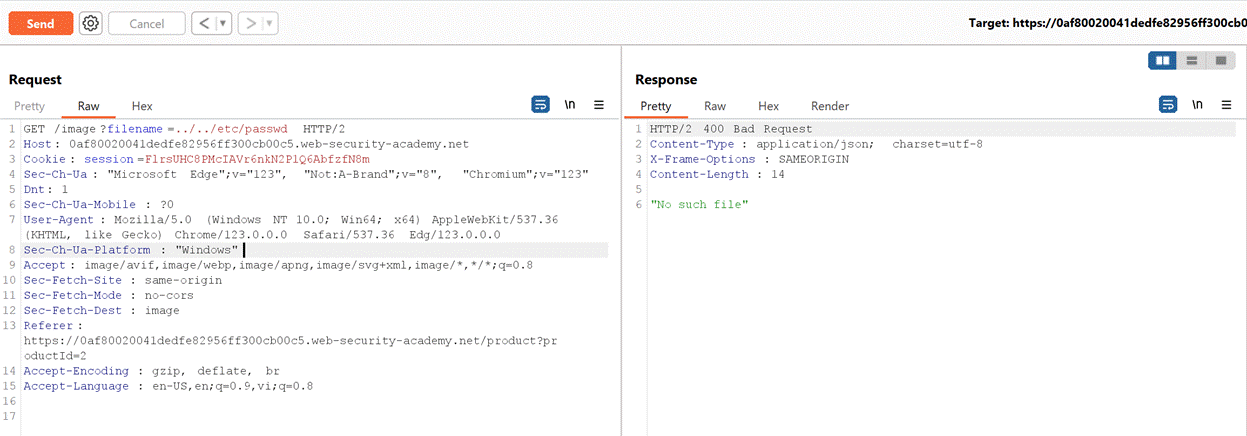


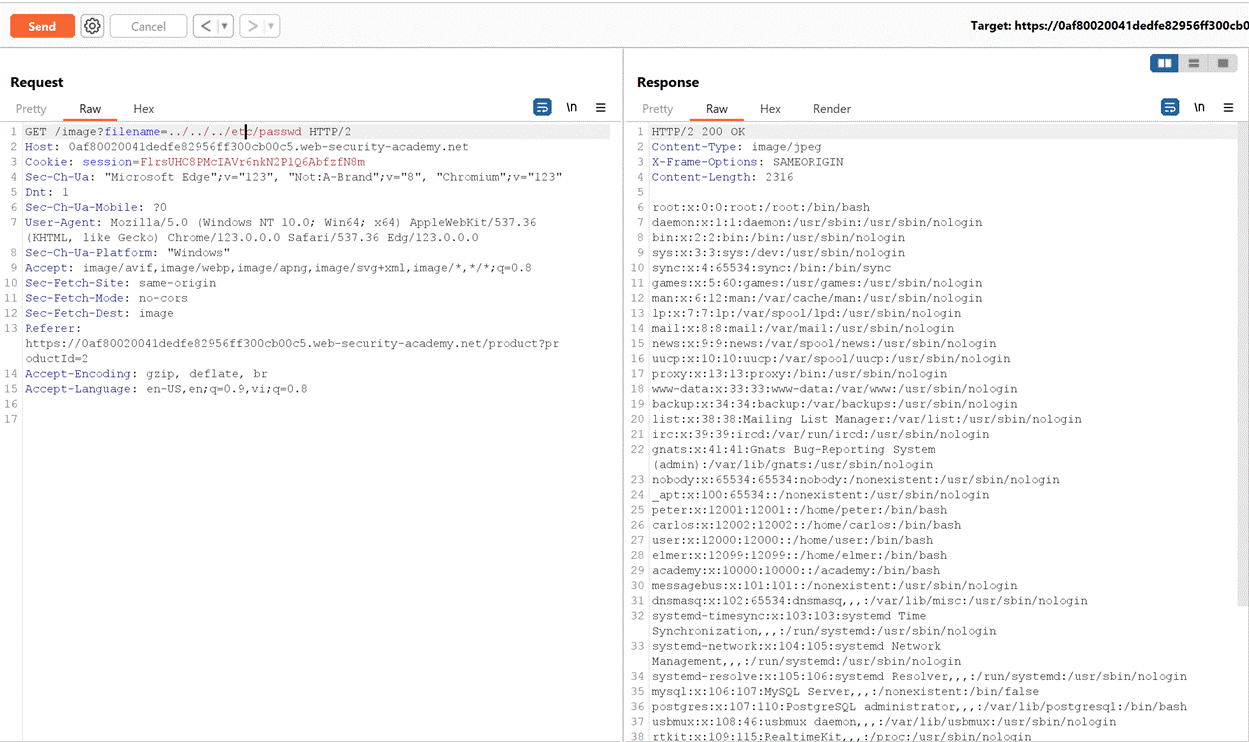
Đề bài yêu cầu ta cần phải tìm thấy nội dung của file /etc/passwd, vậy nên ta thử thay đổi nội dung của filename thành /etc/passwd để xem kết quả

Ta không tìm thấy file ở thư mục hiện tại, thay vào đó ta có thể lùi lại 1 thư mục bằng cách sử dụng path traversal sequences  “../”

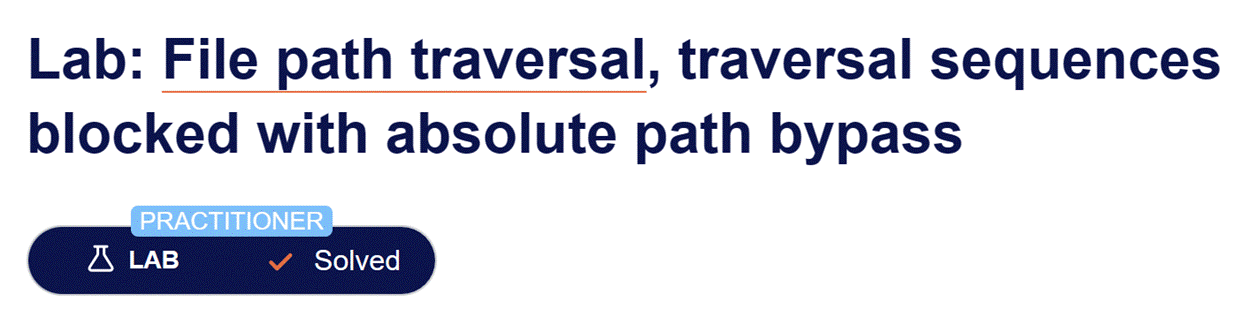


Tiếp tục thêm kí tự “../” đến khi đọc được file cần thiết

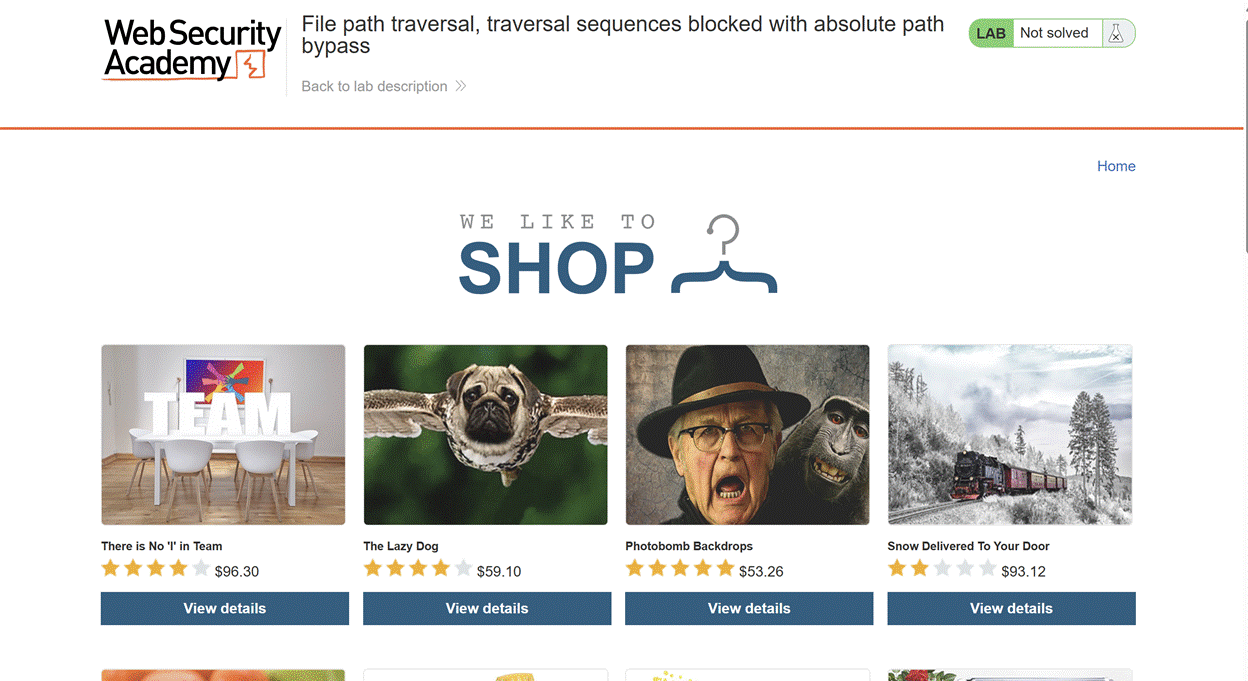




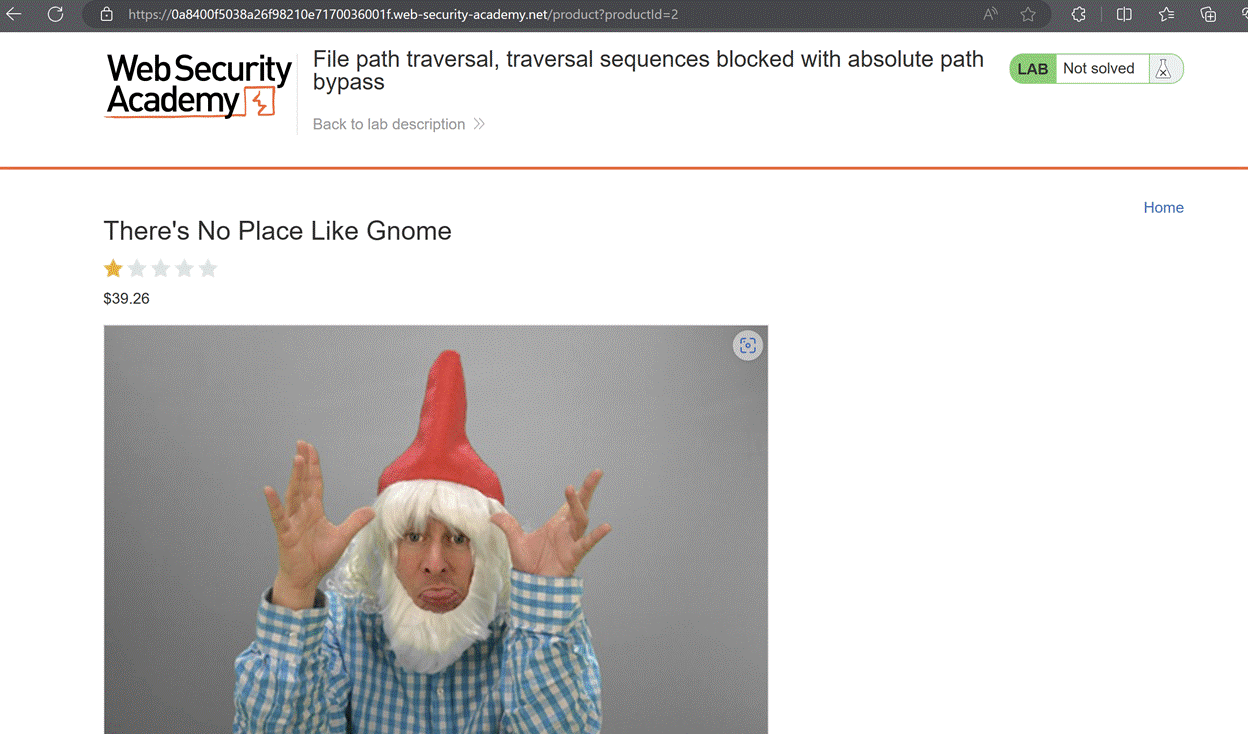
Ta đã đọc được file /etc/passwd và hoàn thành lab này.



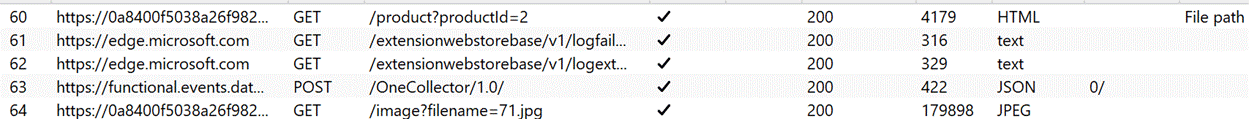
Tiến  hành access đến trang lab

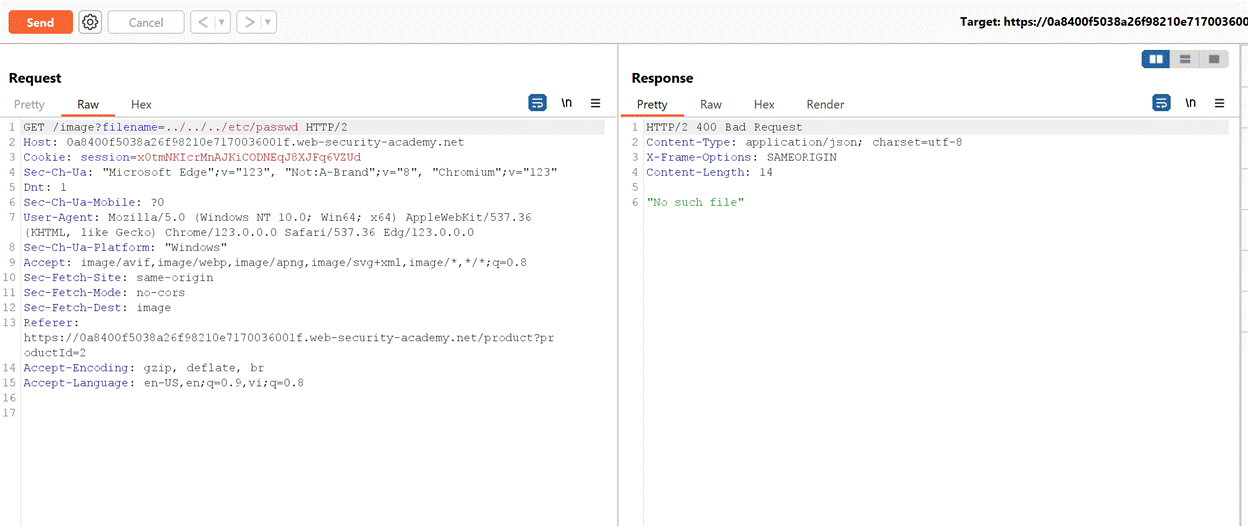


Vẫn như lab trên, ta nhấn vào xem 1 sản phẩm bất kỳ và sử dụng burpsuite để bắt các gói tin.

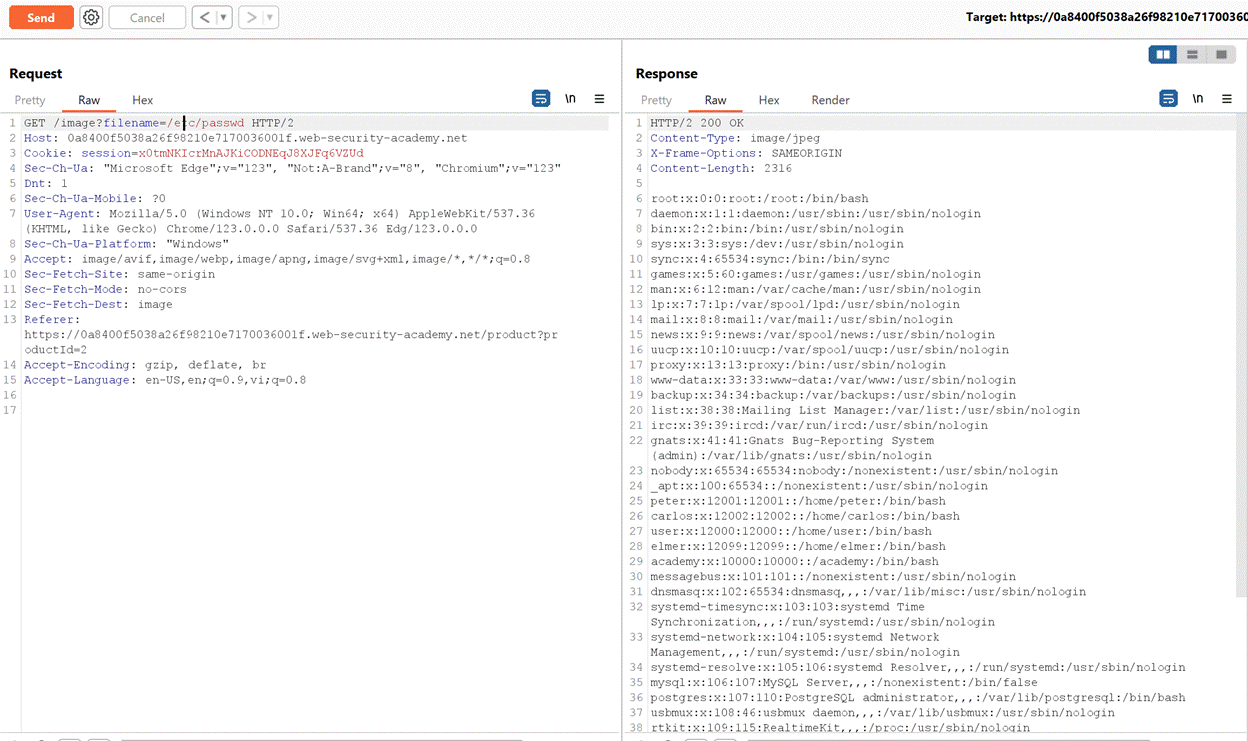


Và vẫn như challenge trên, lỗ hổng lại xuất hiện tại trường filename

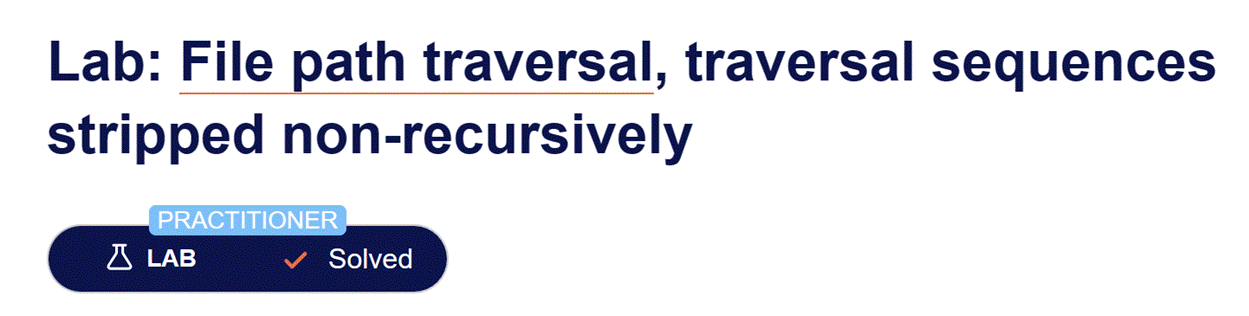


Gửi gói tin sang repeater để thực hiện khai thác, ta cũng thử ghi đường dẫn giống lab trước là ../../../etc/passwd. Tuy nhiên lần này ta không thể khai thác thành công như trước.  


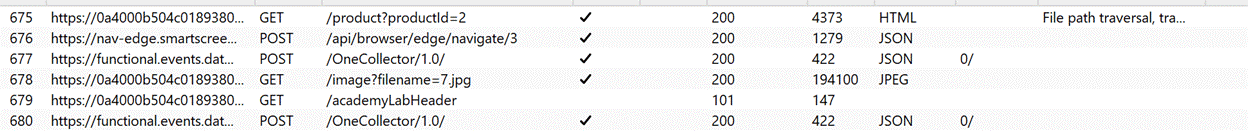
Trong mô tả của bài lab, người ta nói rằng các traversal sequences đã bị block và giá trị của trường filename có liên quan đến đường dẫn mặc định. Vậy ta thử bỏ hết các kí tự ../ và sử dụng trực tiếp đường dẫn tuyệt đối /etc/passwd.

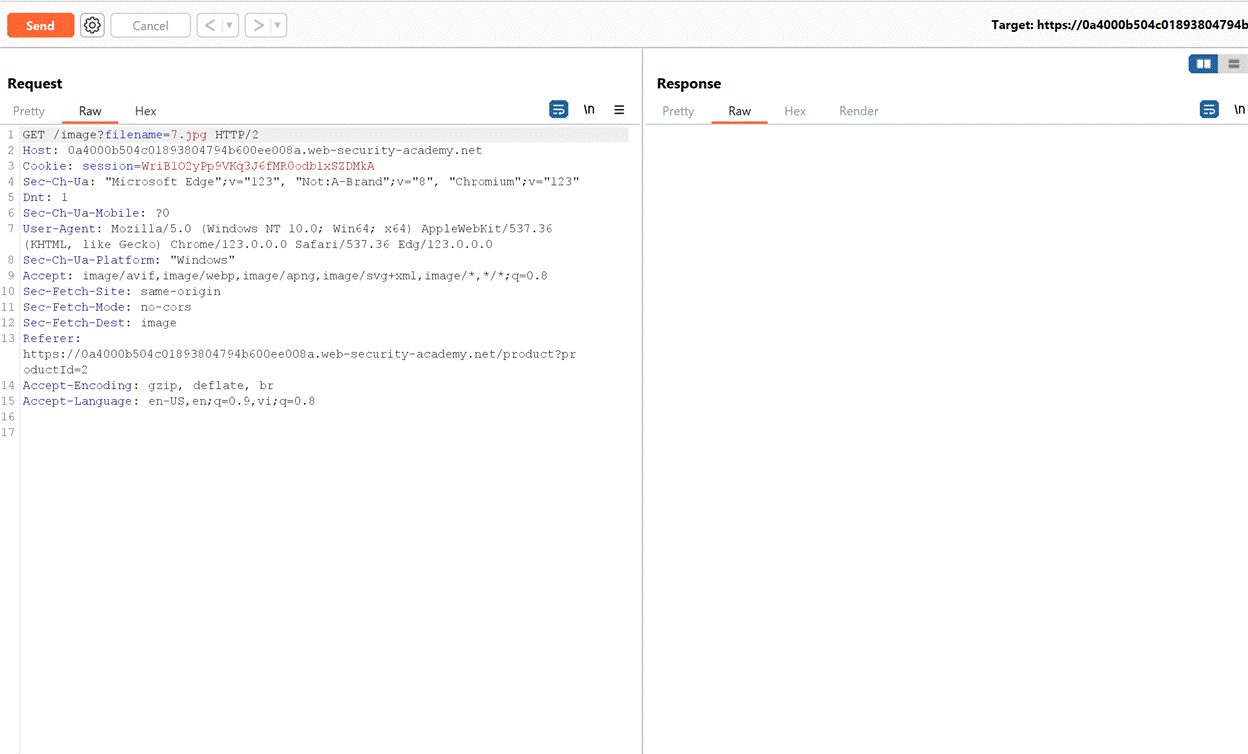


Và ta đã đọc thành công /etc/passwd

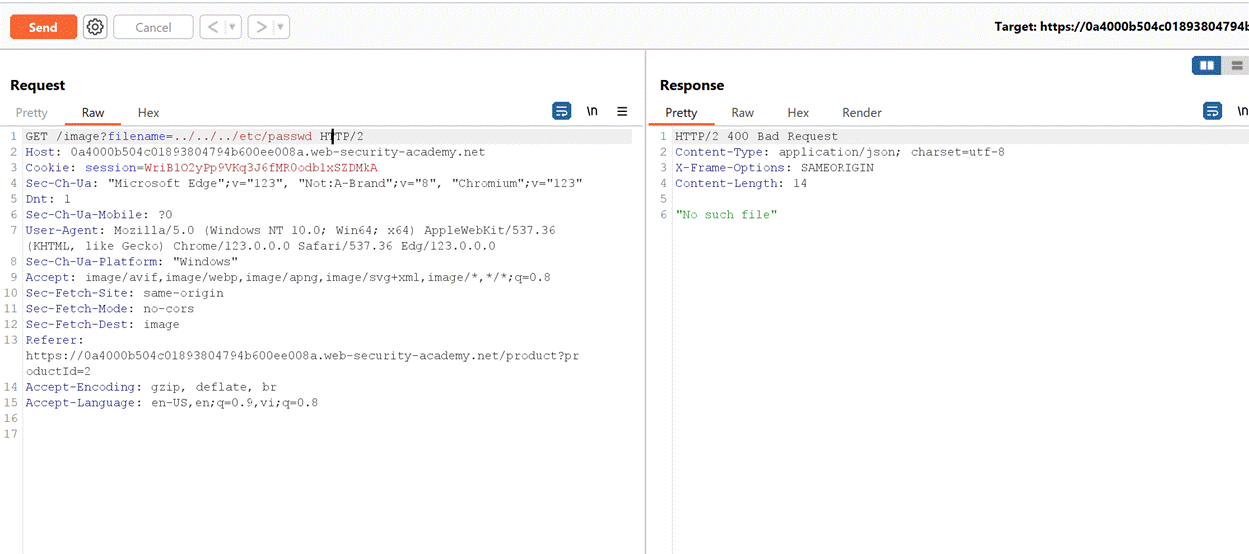


Ở lab này, ta vẫn bắt gói tin bằng Burpsuite và thực hiện chuyển gói tin đến repeater để khai thác





Ta thử với ../../../etc/passwd và xem kết quả

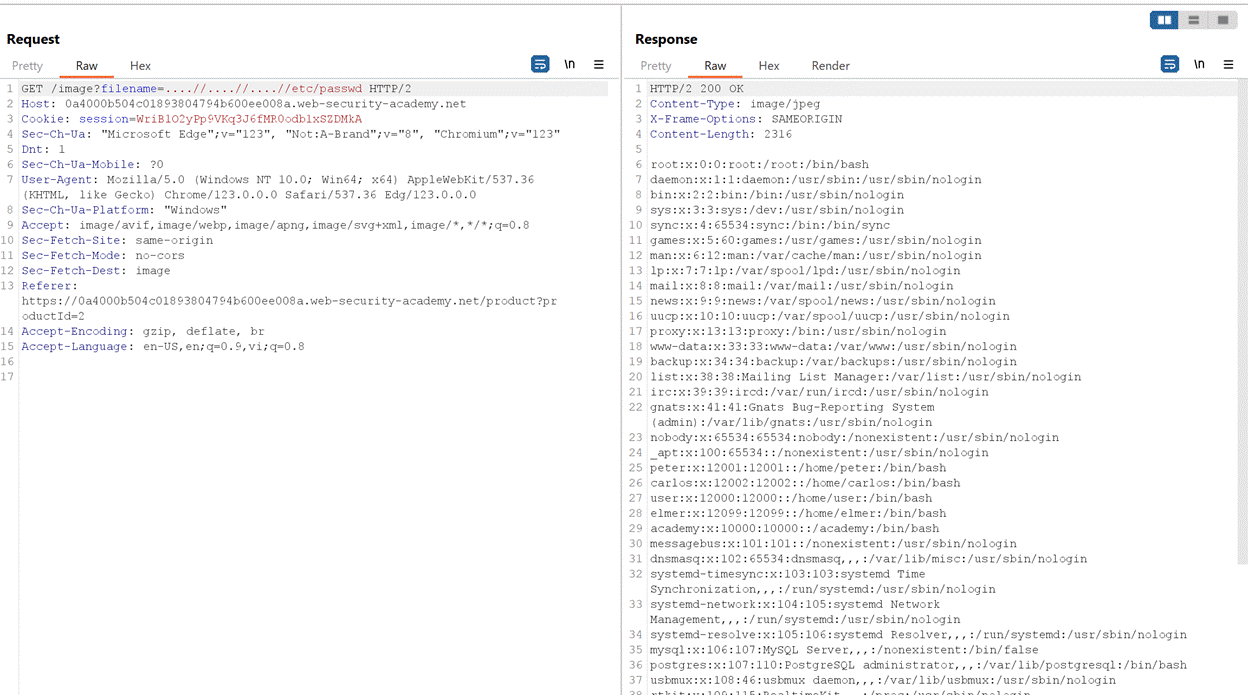
  
Ta đọc file không thành công, quay trở lại với mô tả của bài lab. Ở lab này, khi gửi 1 request đến server, path traversal sequences sẽ bị loại bỏ. Ví dụ:

../../../etc/passwd à /etc/passwd

Vậy ta có  thể bypass được việc này bằng cách tạo chuỗi như sau:

….//….//….//etc/passwd à ../../../etc/passwd

Ta tiến hành chèn chuỗi trên vào filename và xem kết quả:



Vậy ta đã hoàn thành lab này.

 Kết quả

A screenshot of a computer

Description automatically generated