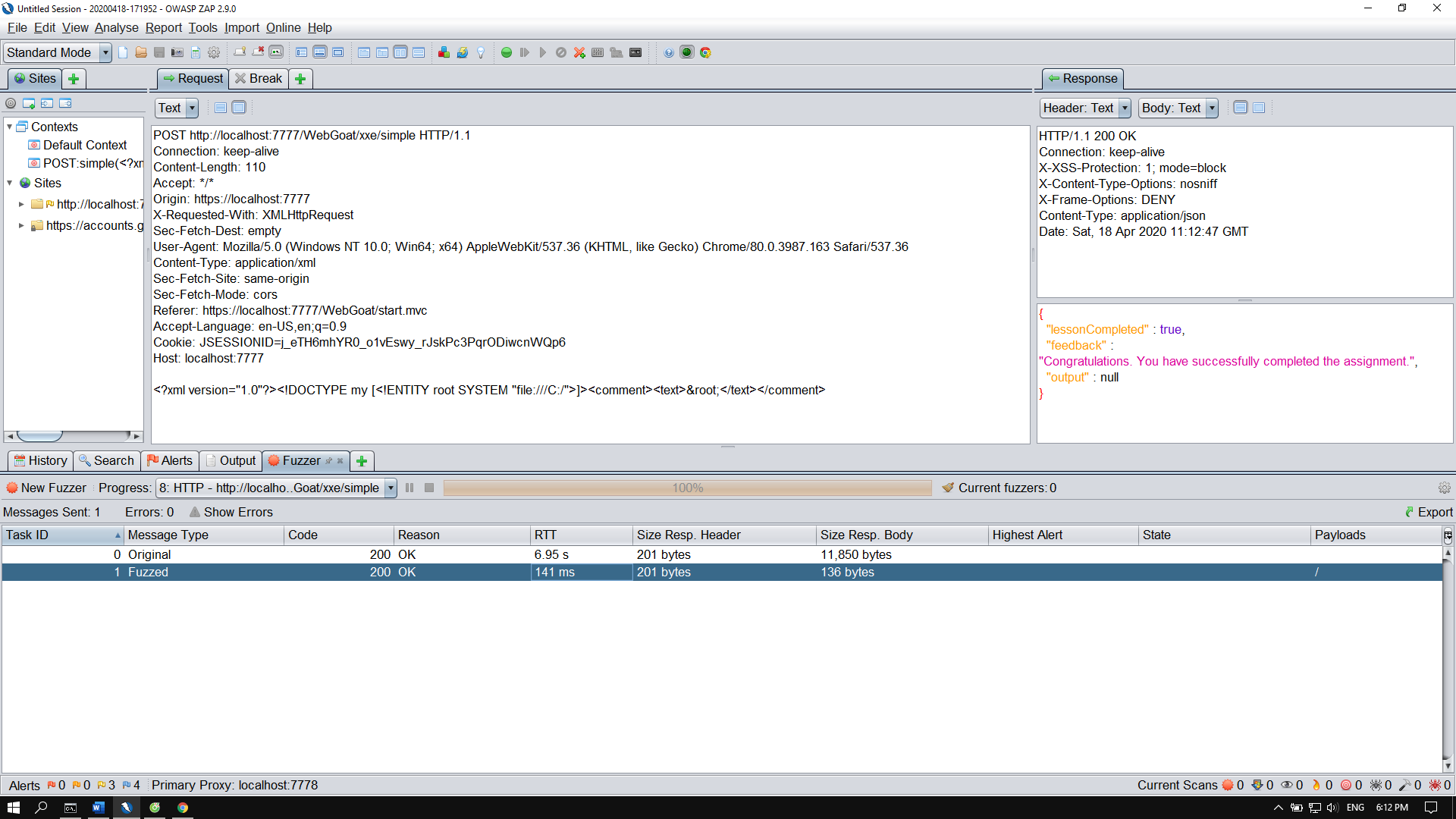
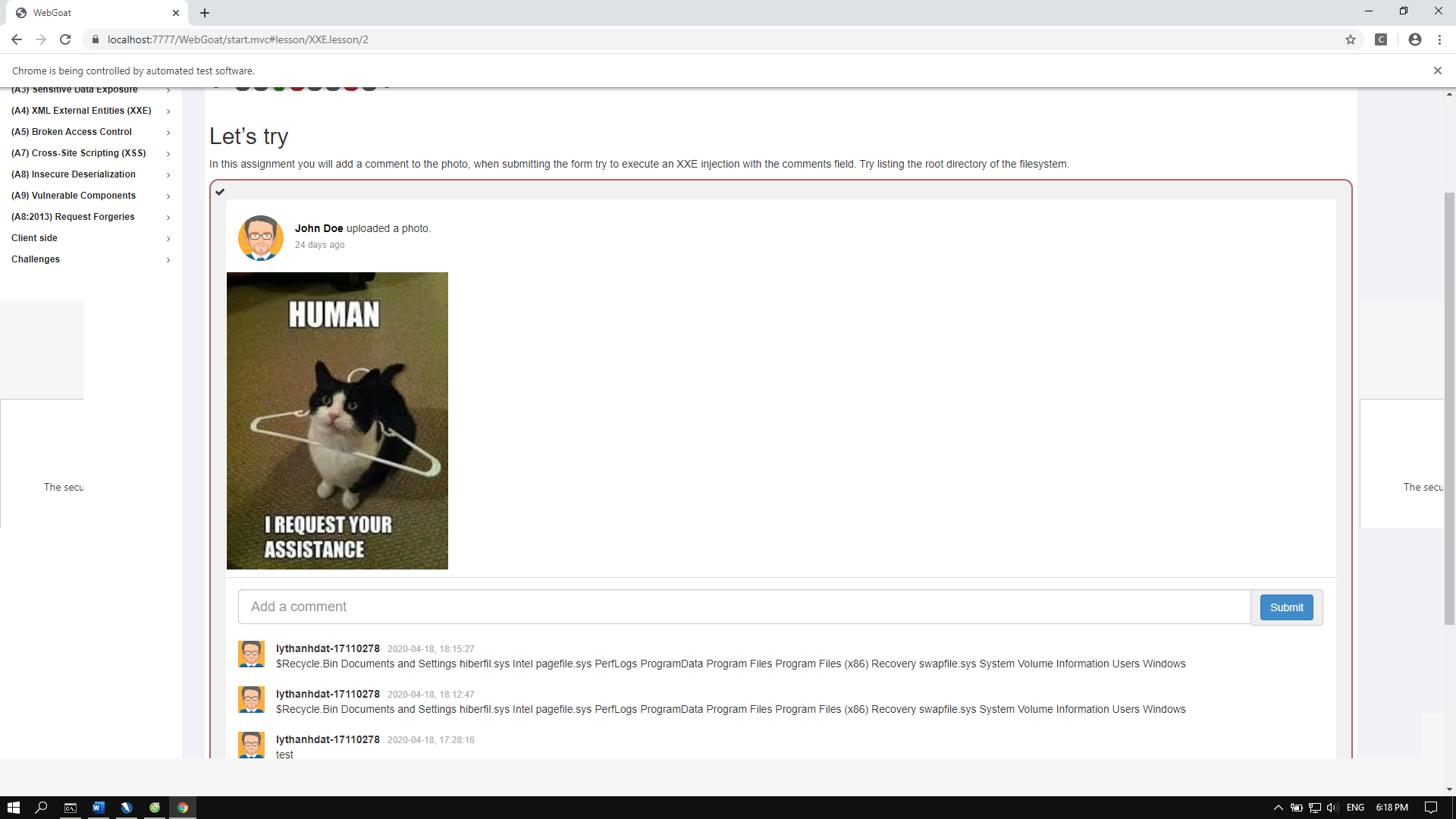
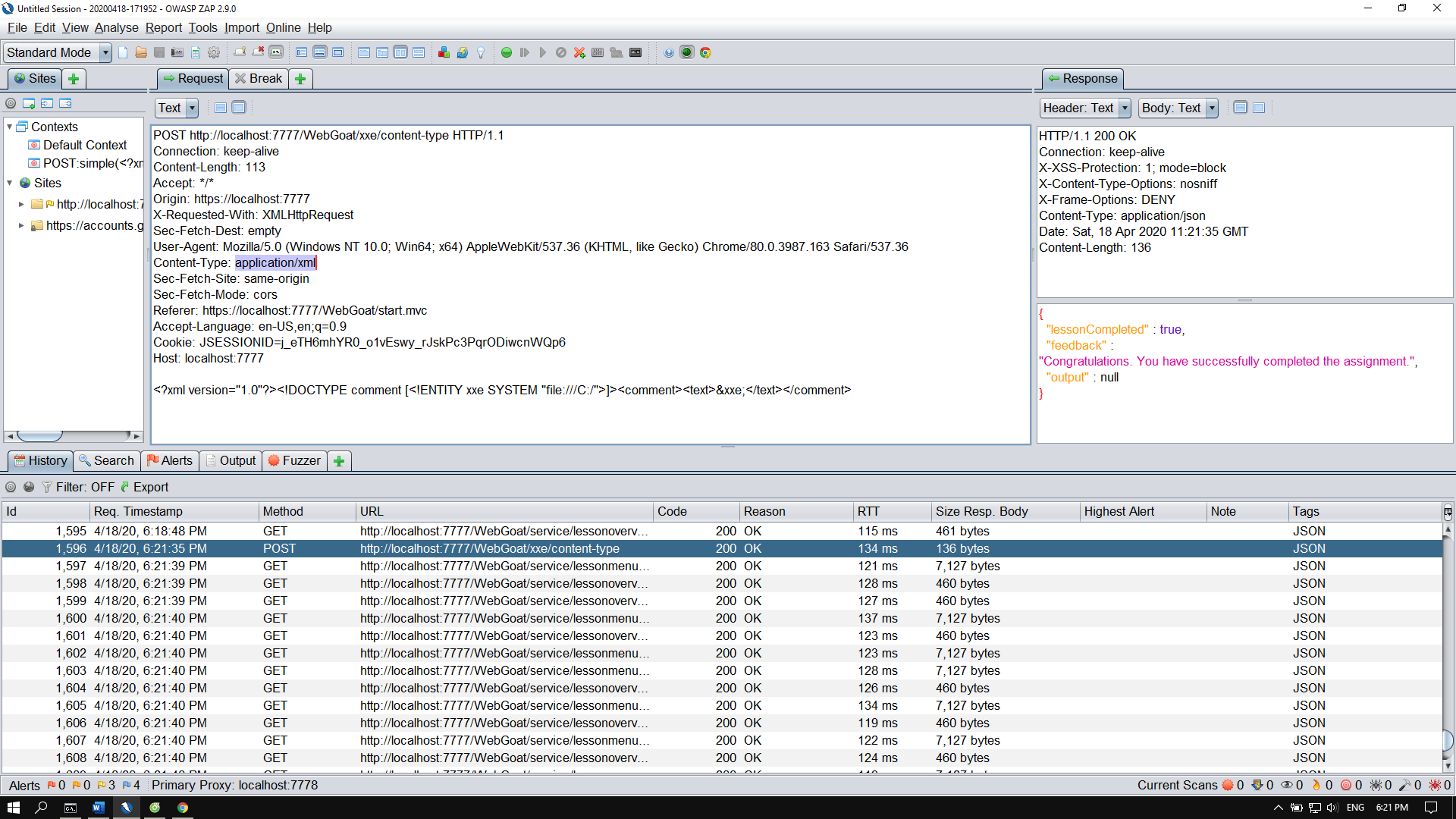
Họ và tên: Lý Thành Đạt

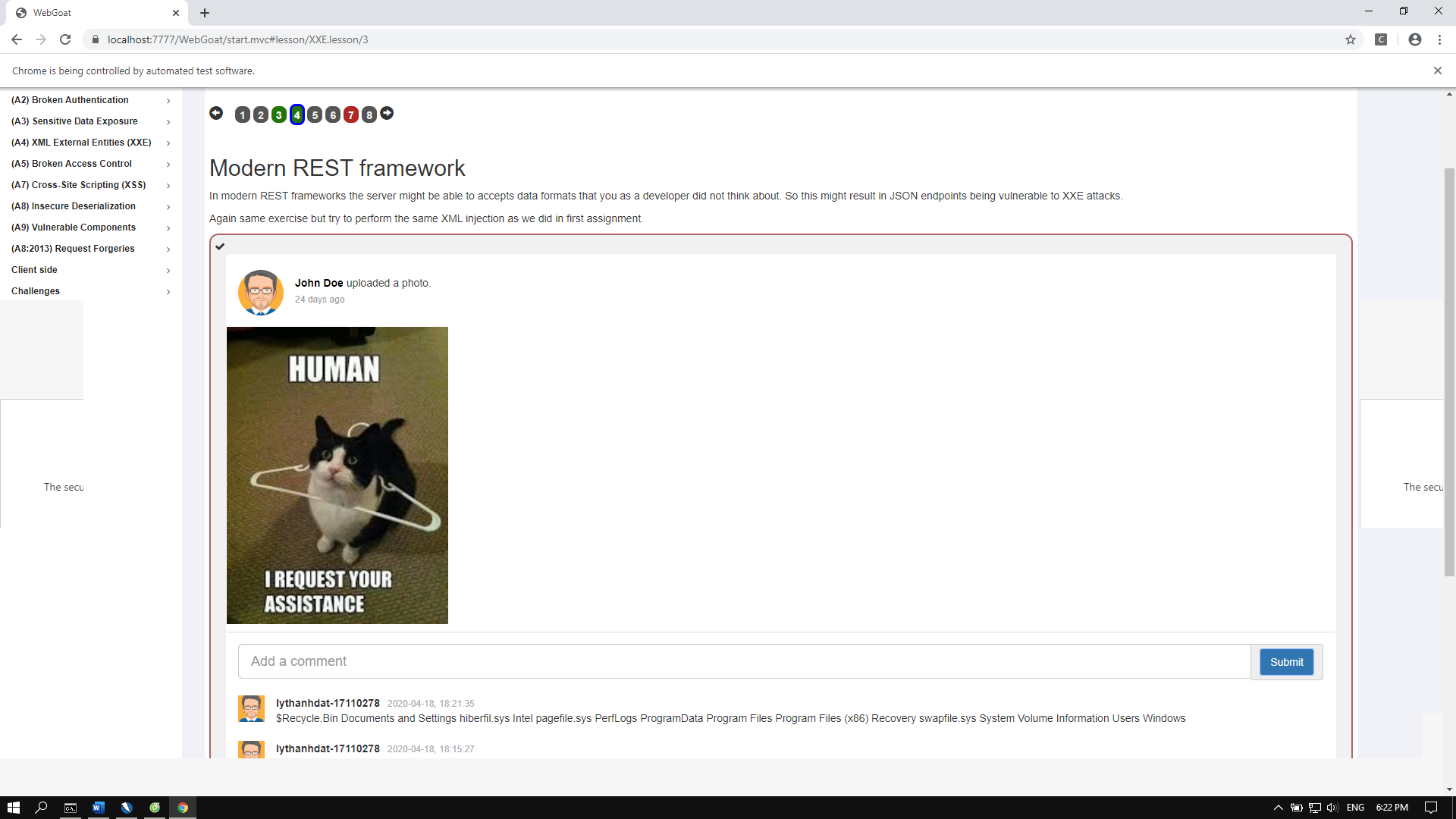
MSSV: 17110278

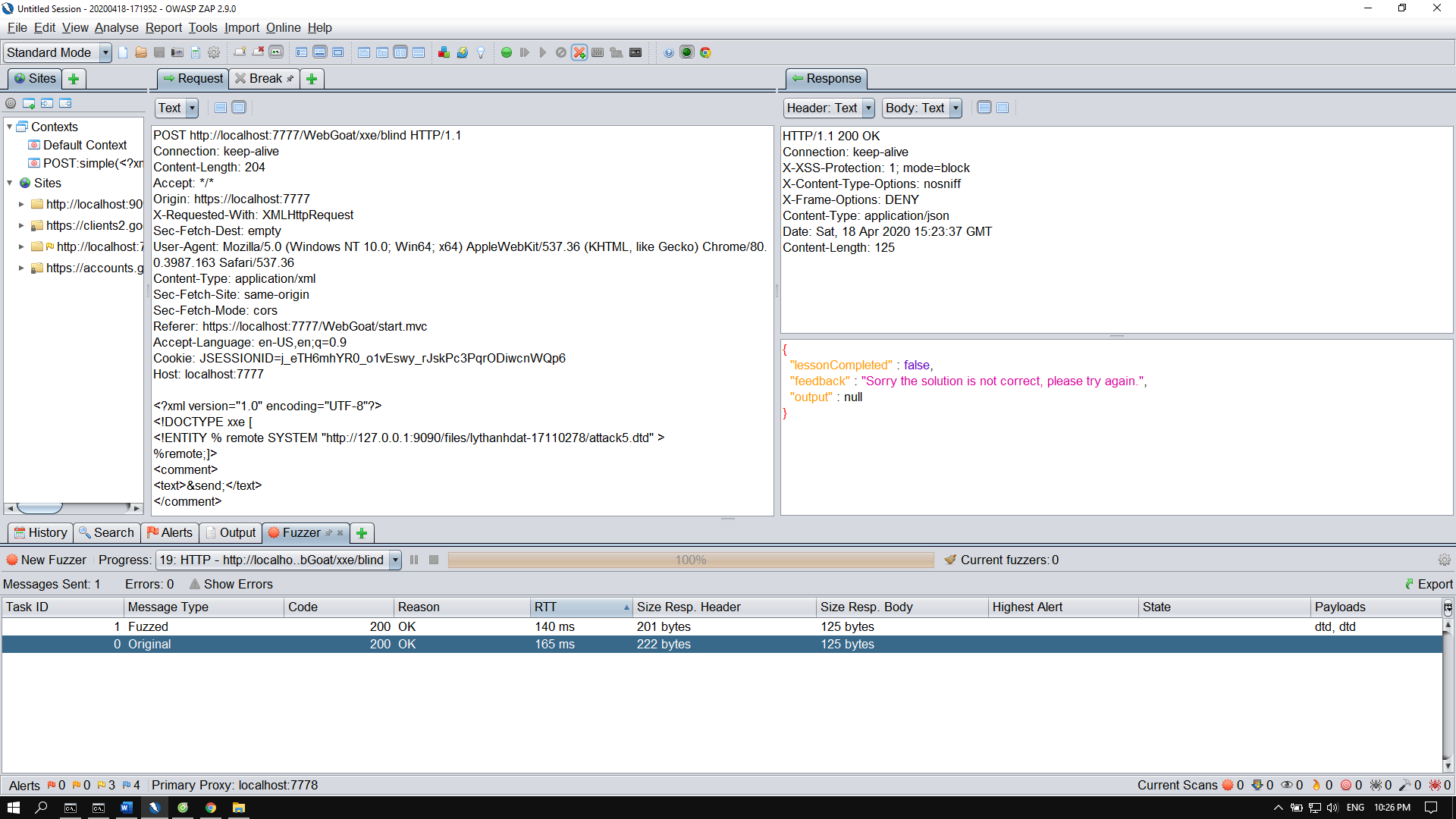
Nội dung: Thực hành XXE - Broken Access Control

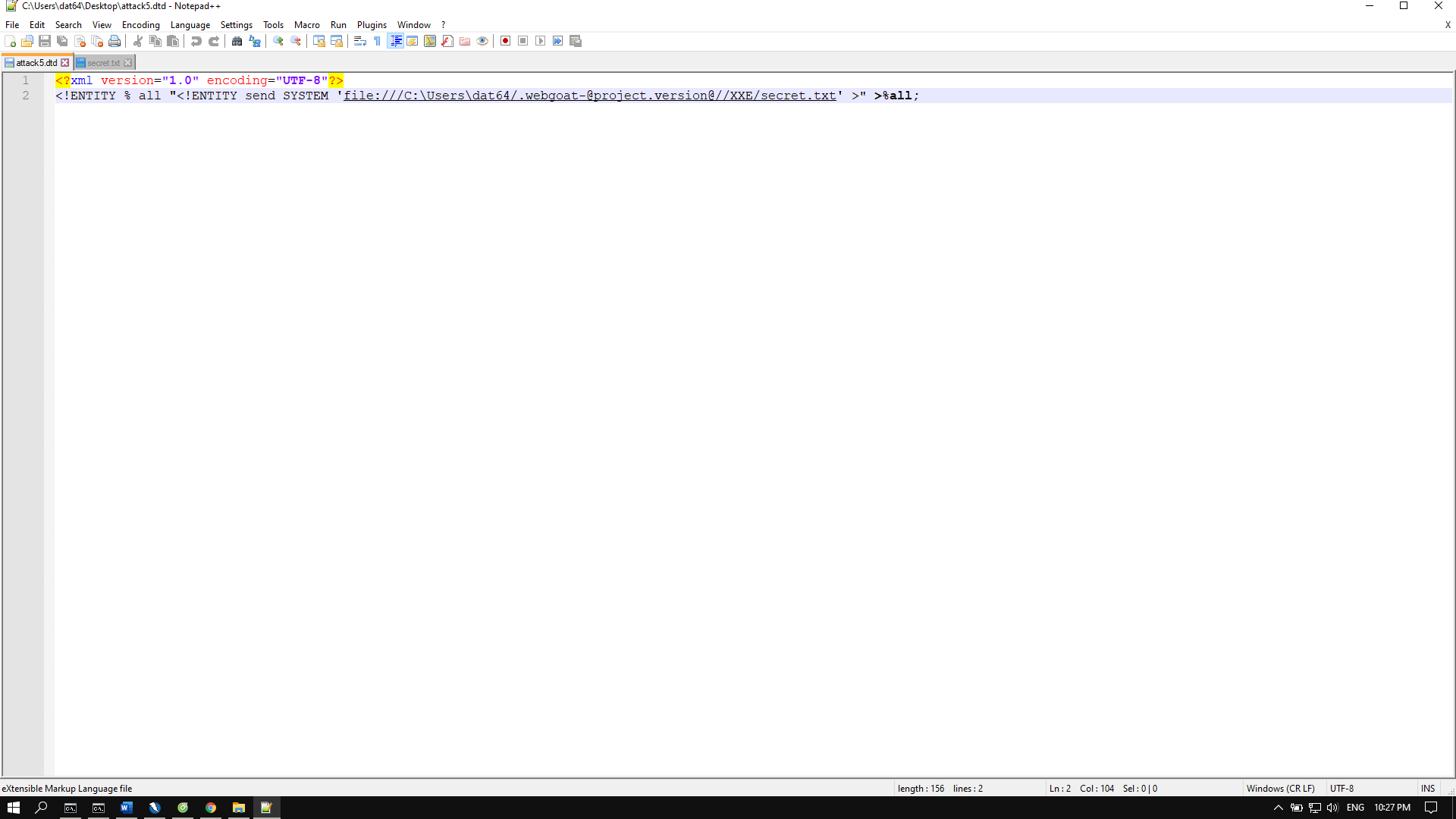


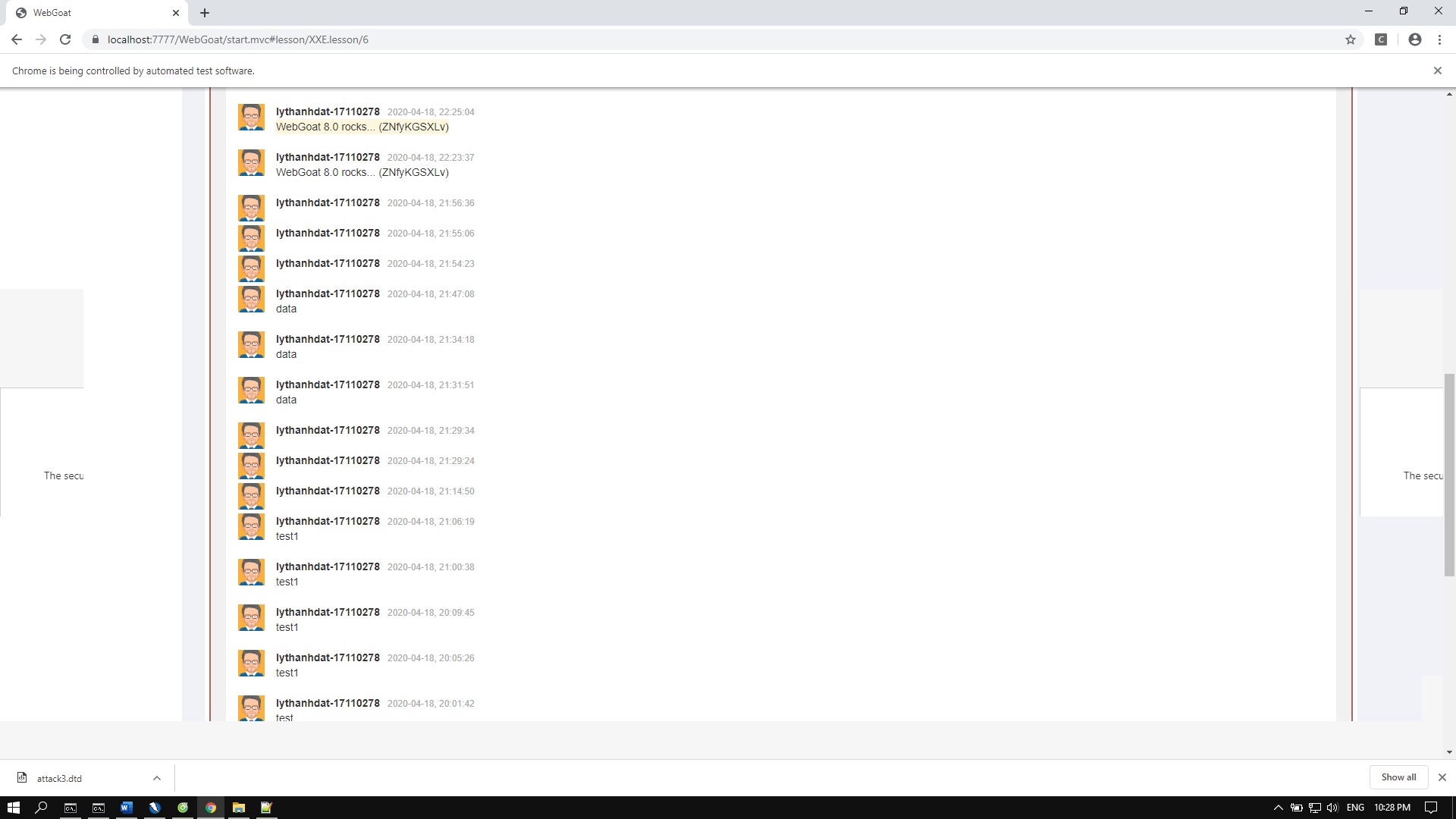


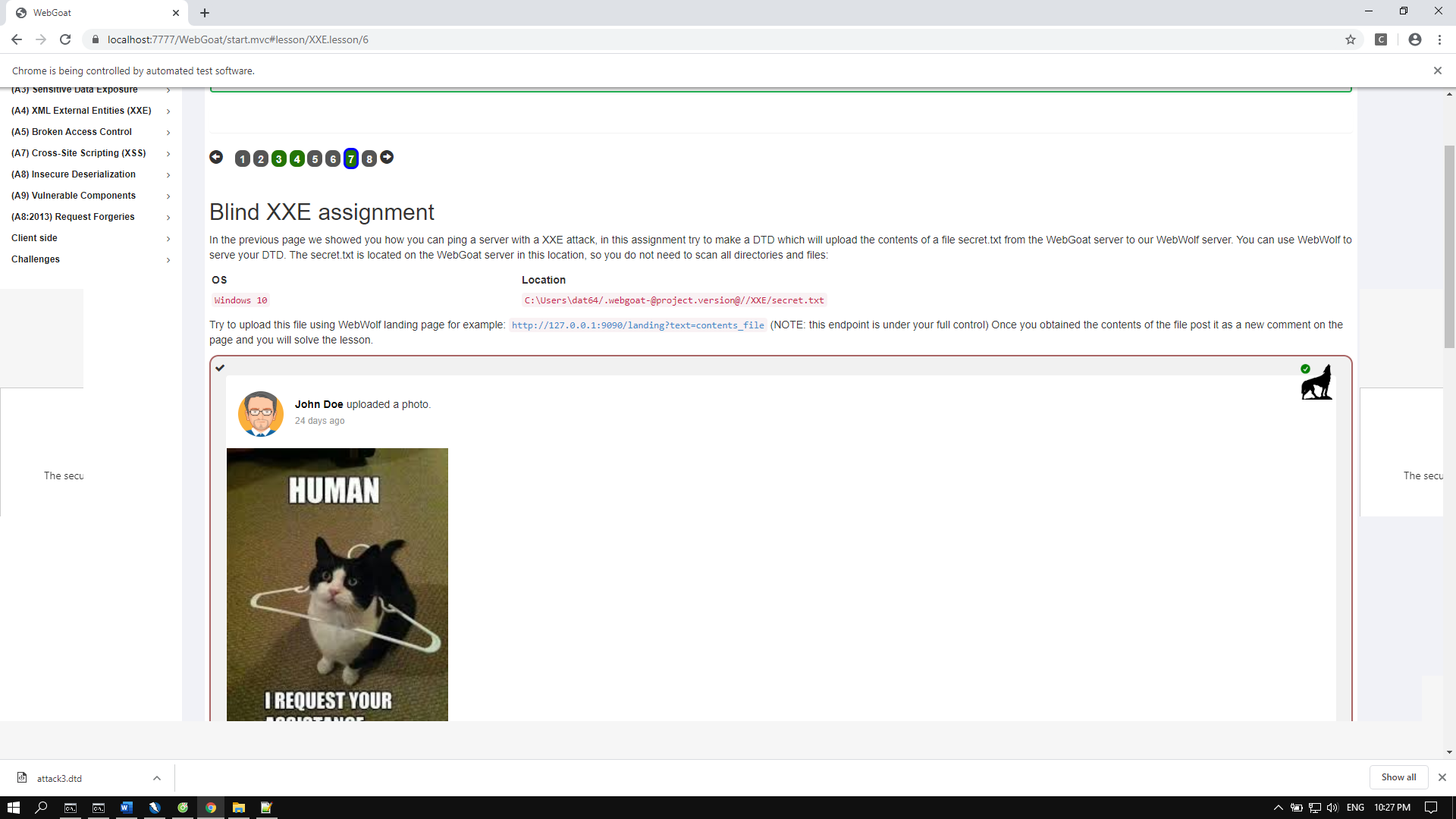


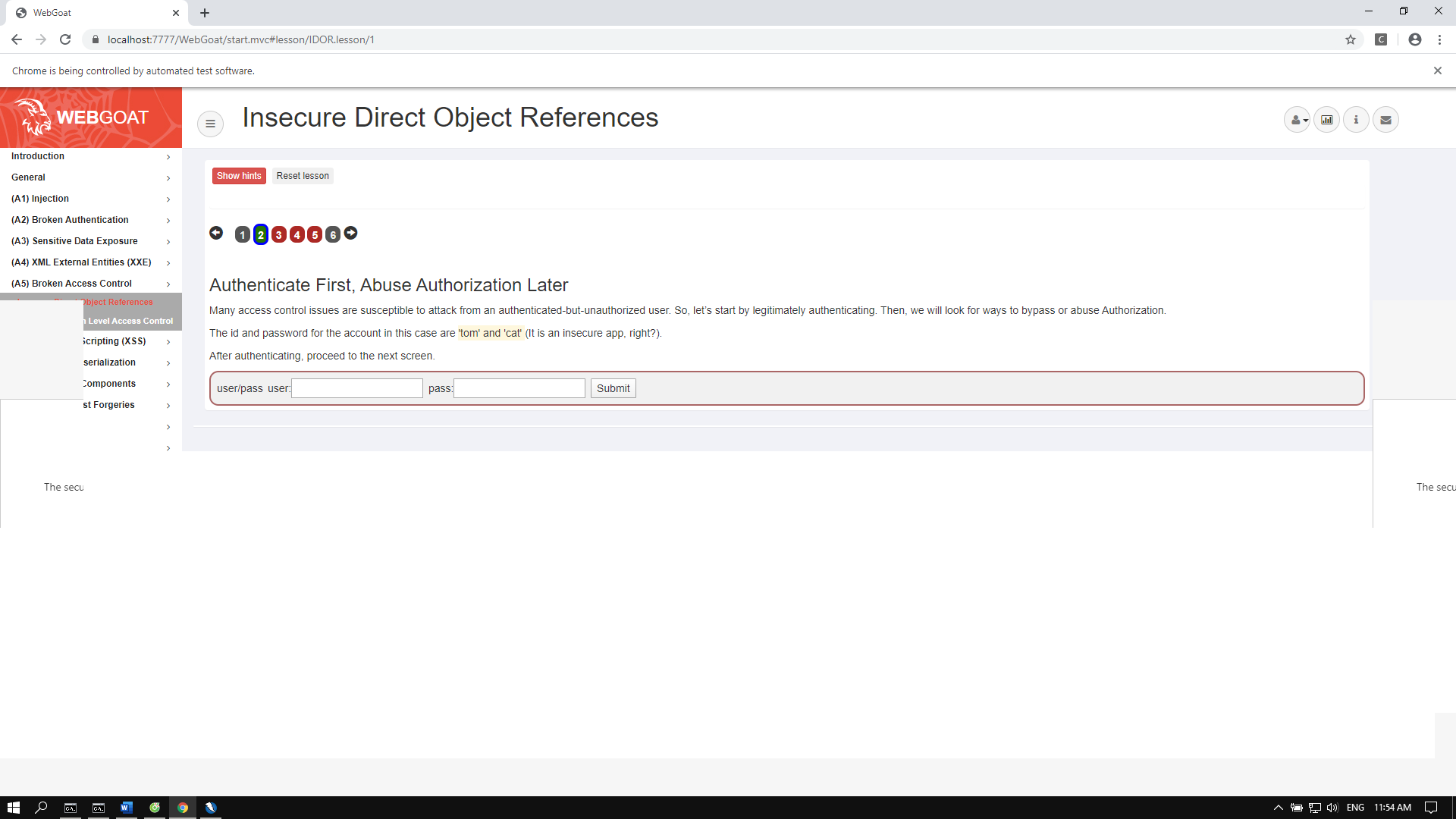


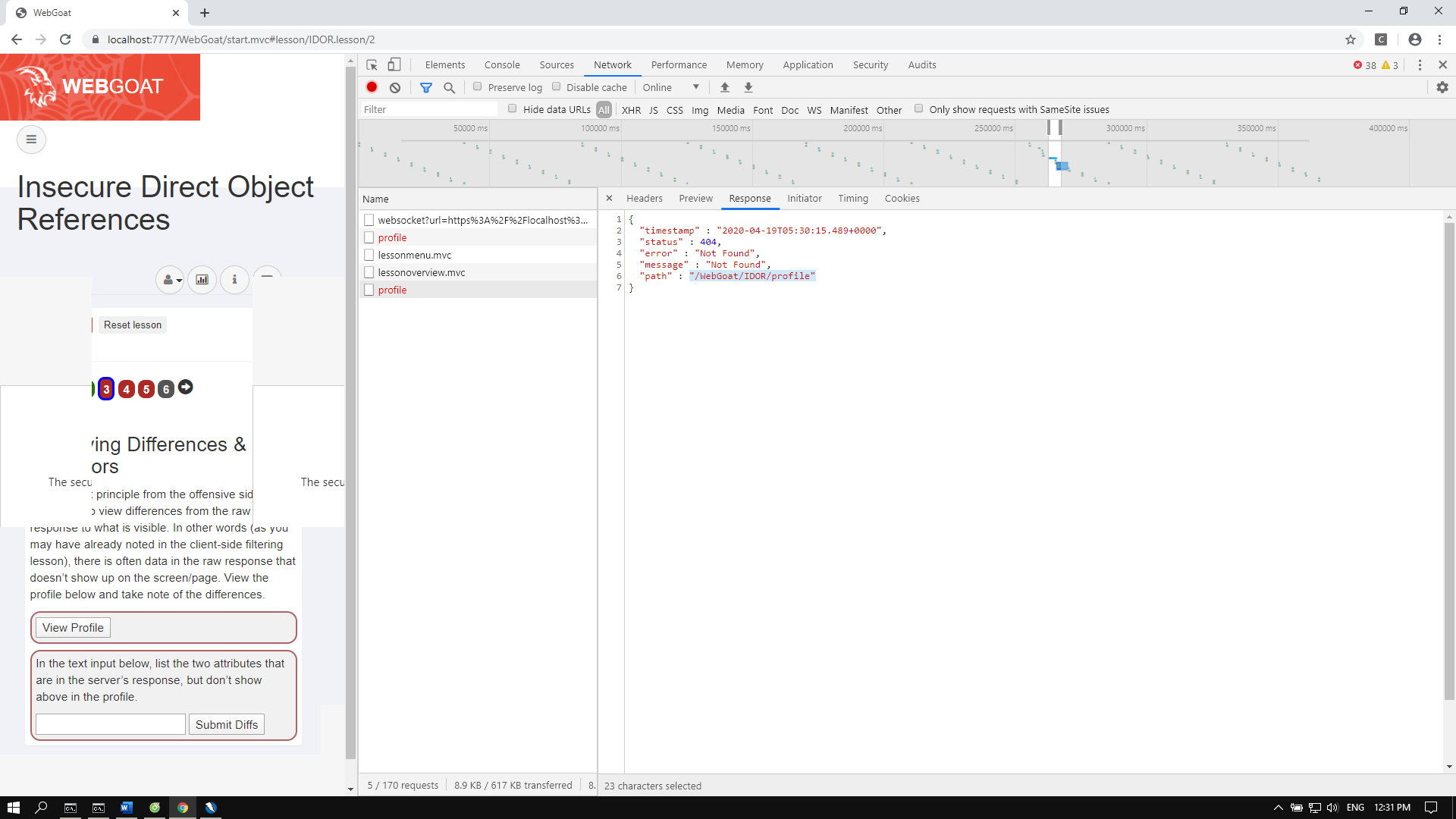




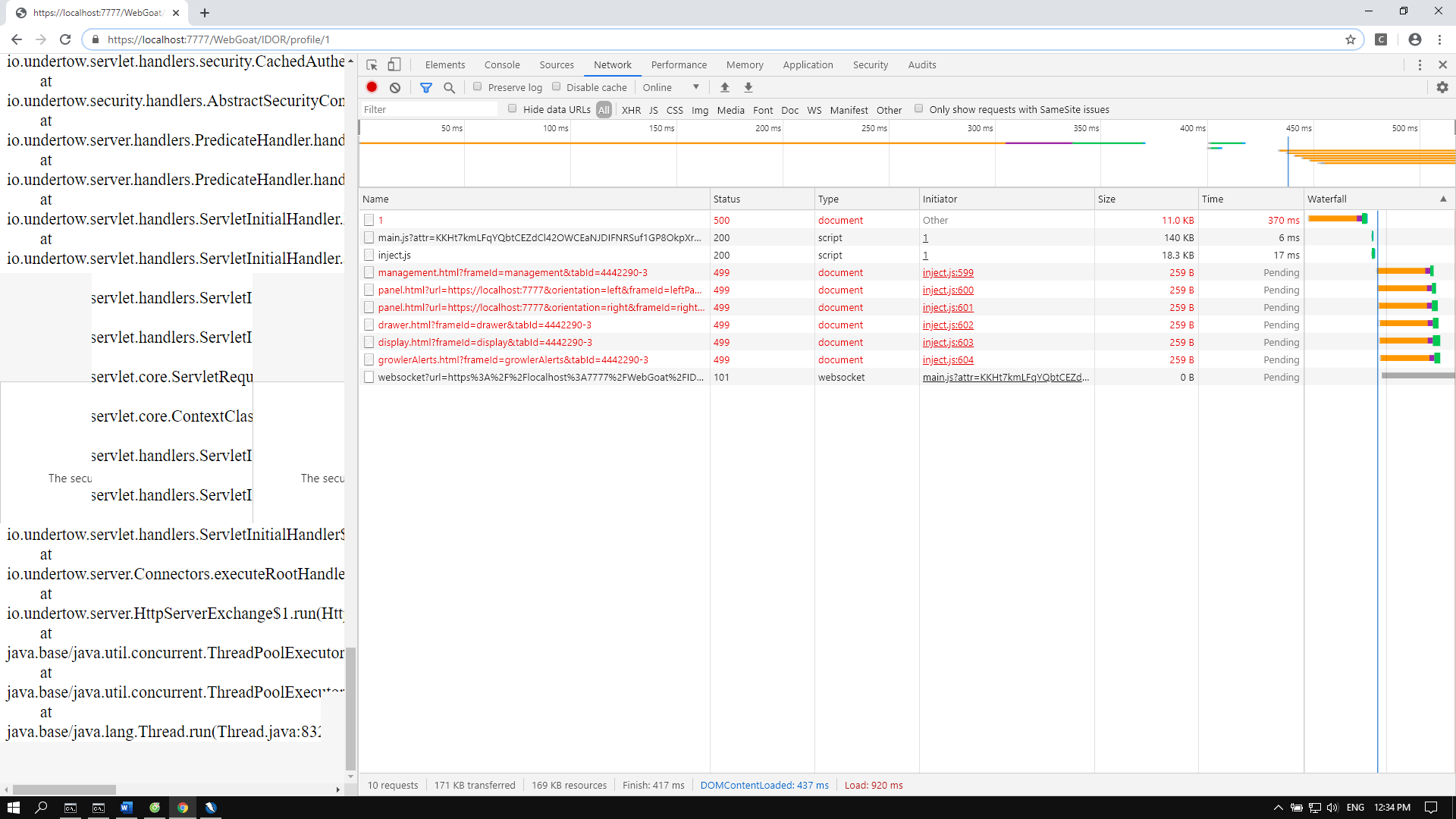






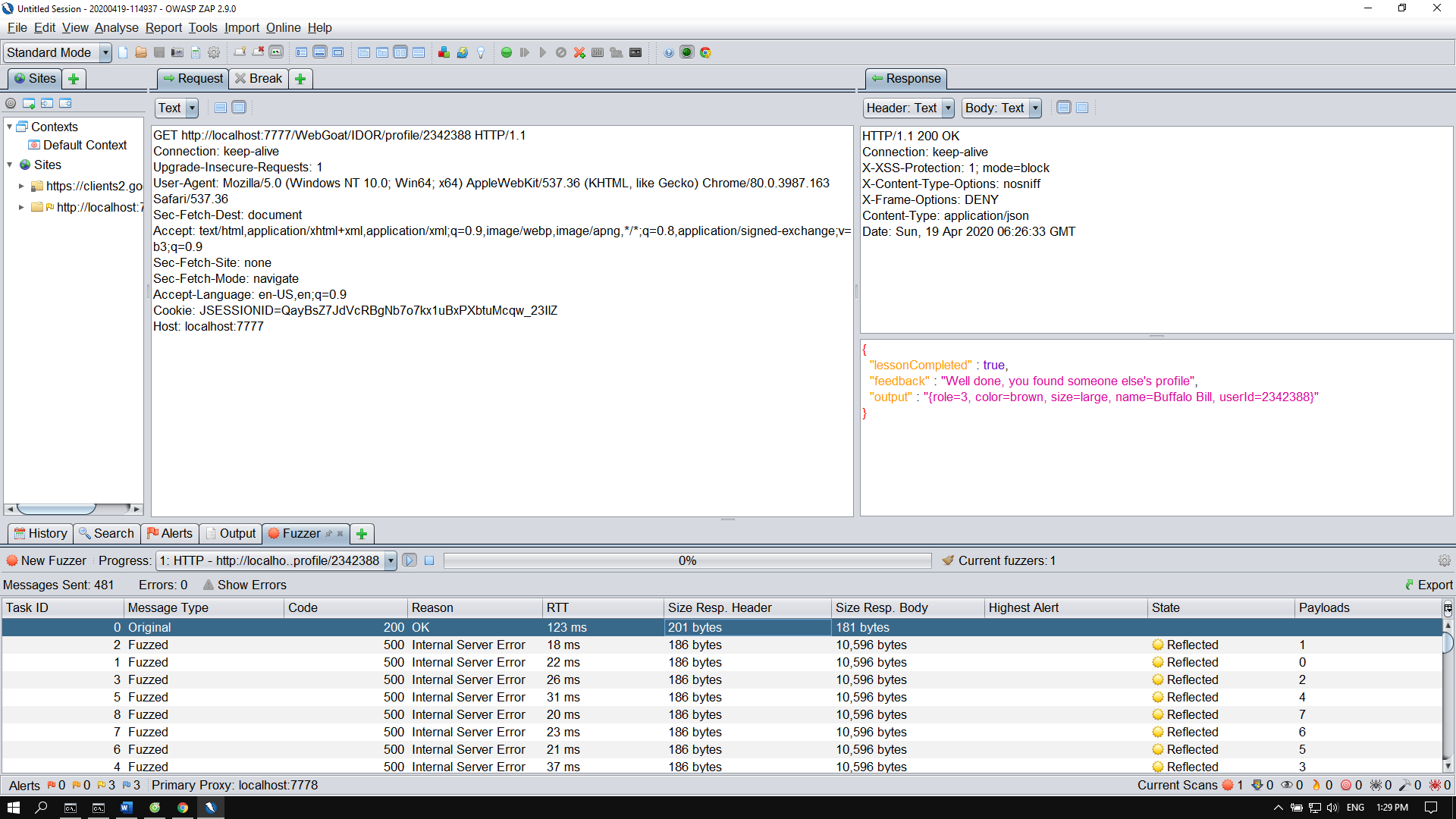


* Link: localhost:7777/WebGoat/IDOR/profile/{id}

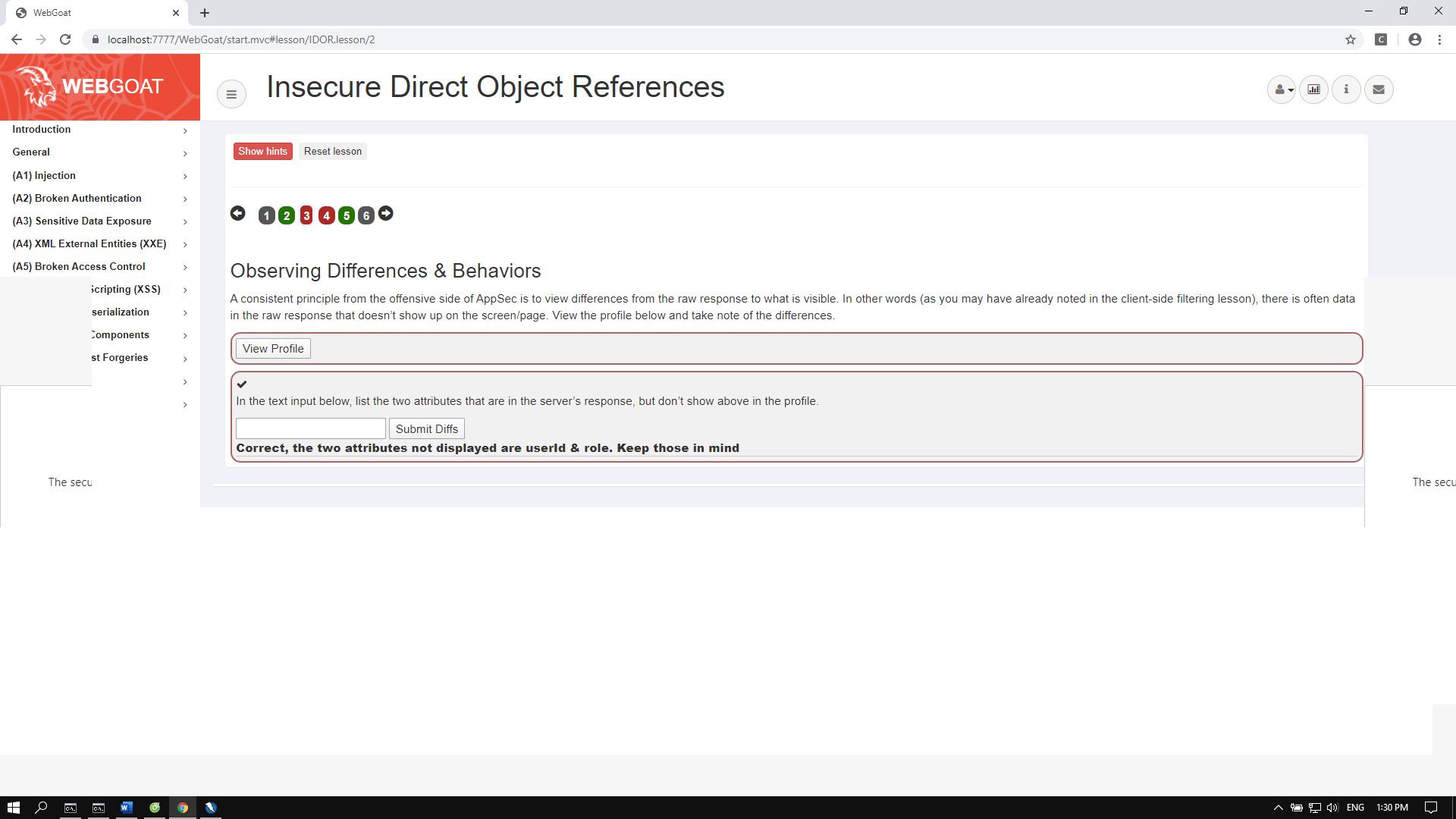


Test từng ID vì câu này bị lỗi nên không thể dùng nút view profile bằng url này được vì hệ thổng sẽ trả về 1 url không có id. Vậy nên theo Google-sama, id = 2342388 => localhost:7777/WebGoat/IDOR/profile/2342388

Vậy nên nếu theo đúng quy trình ta sẽ tìm được id này tại chức năng puzzers của ZAP ta sẽ phải thử hơn 2 triệu request lên server, ở đây em sẽ lấy luôn là 2342388 để không mất nhiều thời gian. Dưới đây là hình ảnh của chức năng Puzzers nếu vẫn muốn làm đúng quy trình và không dùng Google-sama sẽ ngốn tầm 5 giờ để Puzzers có thể test hết tất cả các id có thể từ 1 - 9999999



* role, userId là 2 thuộc tính không liên quan tới màu, kích thước và tên



Tương tự nhờ Puzzers ta sẽ tìm ra id info của chính ta là

