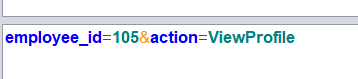
**Kịch bản:** Hacker sẽ cố gắng đọc cấu trúc Request thông qua các giá trị về id, pass,… được gửi đi nhằm thay đổi chúng để kết quả nhận được đúng với ý đồ của Hacker

**Mục tiêu Lab:** Dùng employee Tom để xem Profile của người khác

**Tiến hành:**

**1. Xem Cấu trúc Request để suy đoán cách hệ thống thực thi:**



Vậy thì Id hiện tại là 105 vậy ta sẽ mò id bằng Puzzer để tim Id có thể xem, có thể là 106 107,…

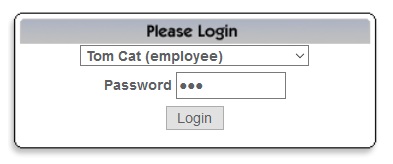
**2. Các bước tiến hành:**

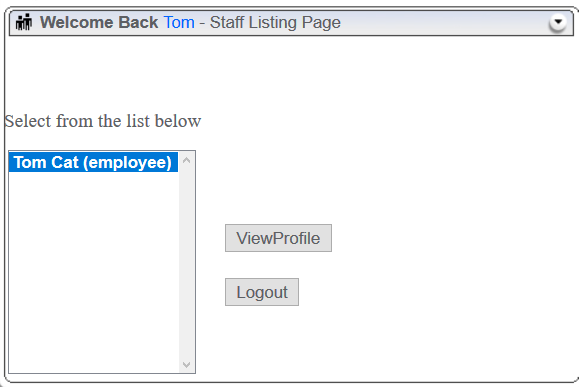
- Đăng nhập vào hệ thống với User: Tom – Pass: tom

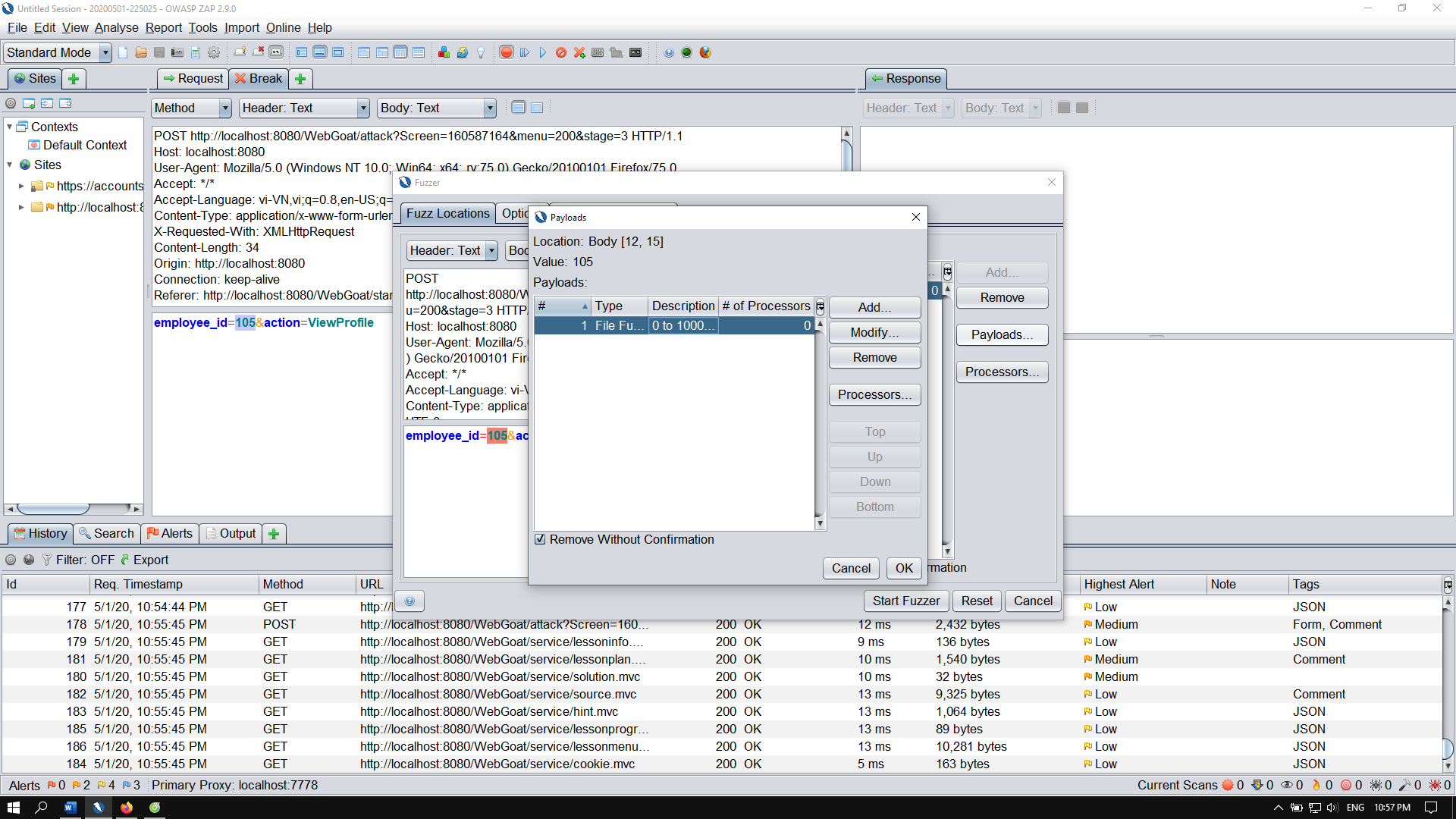
- Thực hiện tính năng ViewProfile trong trang chức năng sau đăng nhập

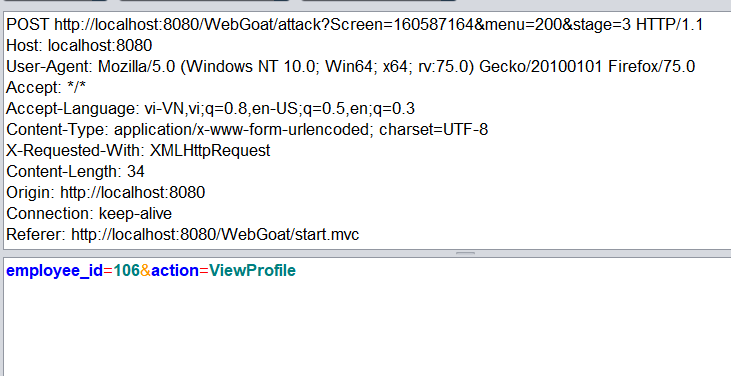
- Can thiệp vào Request, dùng chức năng Puzzer của ZAP để mò Id (Kết quả có được: 106)

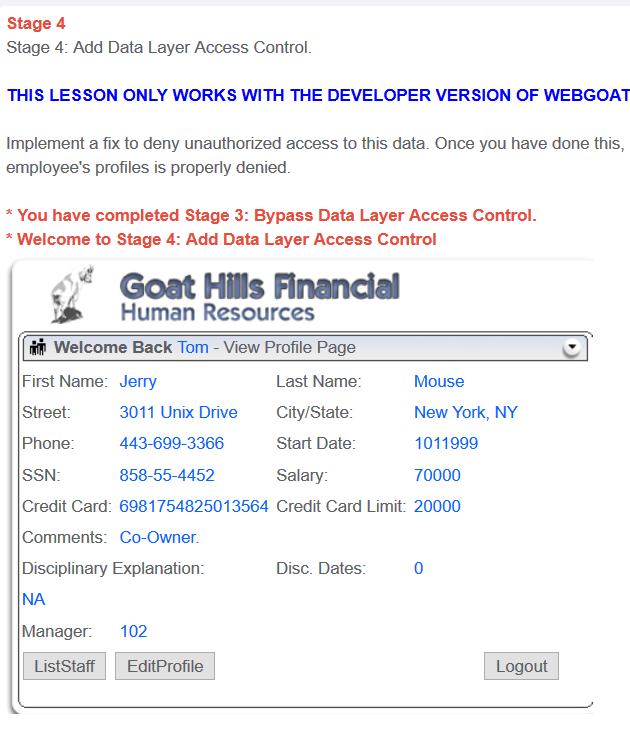
- Kiểm tra Response

****

****



****

****