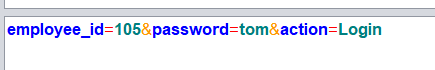
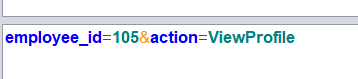
**Kịch bản:** Hacker sẽ cố gắng đọc cấu trúc Request thông qua các thao tác chức năng của Web, từ đó đoán ra cách thực hiện các chức năng khác mà không được cấp trong tài khoản sở hữu như Thêm, Sửa, Xoá,…

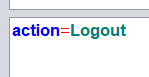
**Mục tiêu Lab:** Dùng employee Tom để thực thi chức năng xoá để xoá profile của tài khoản hiện tại

**Tiến hành:**

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

****





Từ đây ta có thể suy ra để thực thi tính năng xoá một tài khoản ta cần employee\_id và action sẽ là DeleteProfile (Cách đặt tên theo 3 action request trên)

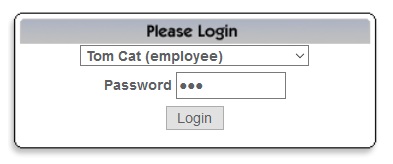
**2. Các bước tiến hành:**

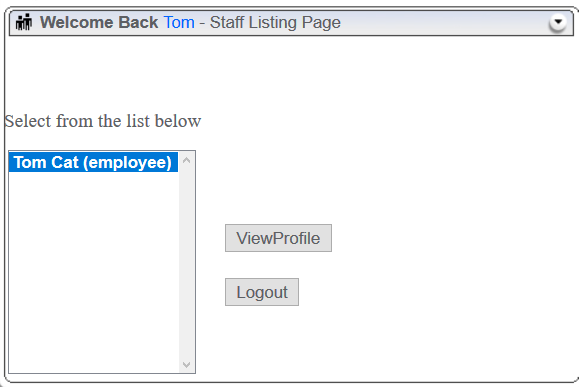
- Đăng nhập vào hệ thống với User: Tom – Pass: tom

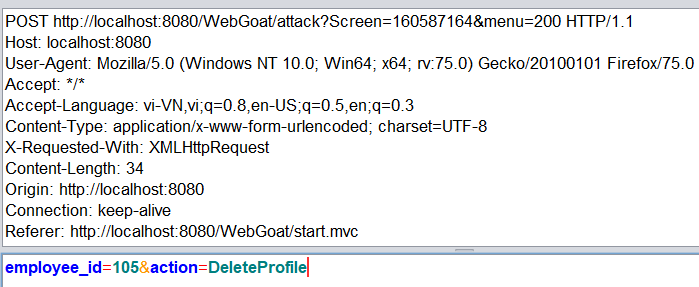
- Thực hiện tính năng ViewProfile trong trang chức năng sau đăng nhập

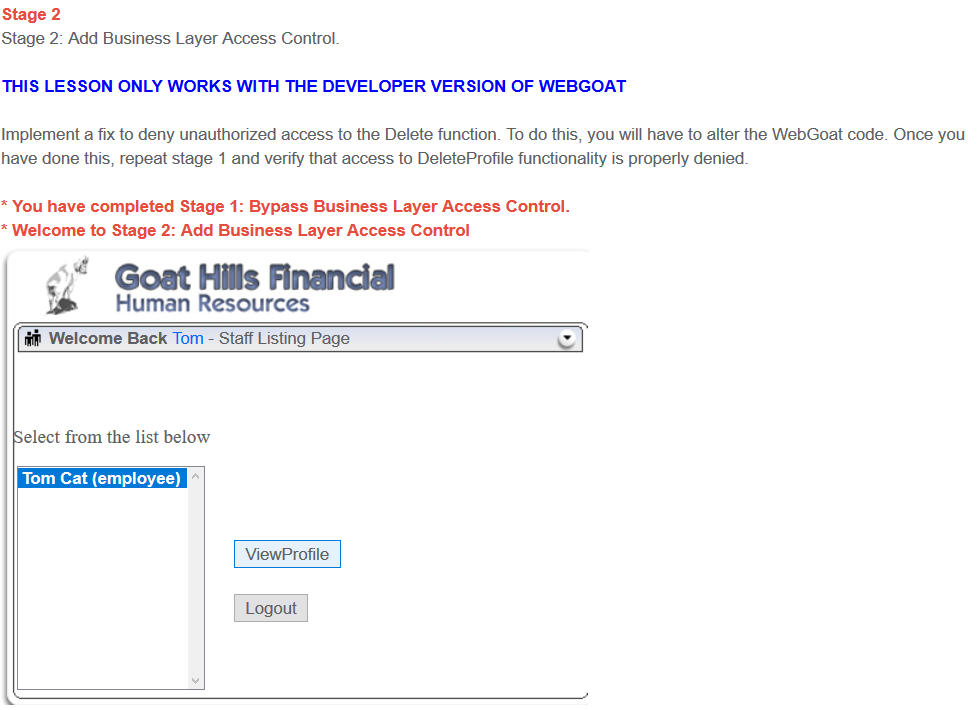
- Can thiệp vào Request chỉnh sửa action từ ViewProfile -> DeleteProfile

- Thực Thi Request

****

****

****

****