**Kịch bản:** Nếu không phân loại tài khoản mà user được phép xem và sửa đổi thì Hacker sẽ khai thác lỗ hỏng này và chén các đoạn Script vào tài khoản người khác

**Mục tiêu:** Edit Profile của Jerry sao cho Street Field được chỉnh sửa là <script>alert("document.cookie");</script>

**Giải thích:** Sau khi thay đổi như trên, Nếu người dùng Jerry thật đăng nhập và xem thông tin, đoạn Script mà Tom thêm vào đó sẽ được thực thi trong trường hợp này là thông báo, Tom hoàn toàn có thể Thêm đoạn Script nhằm đánh cắp Cookie của Jerry

**Tiến hành:**

- Đăng nhập với tài khoản Tom

- Search Jerry

- Edit Profile và Update

