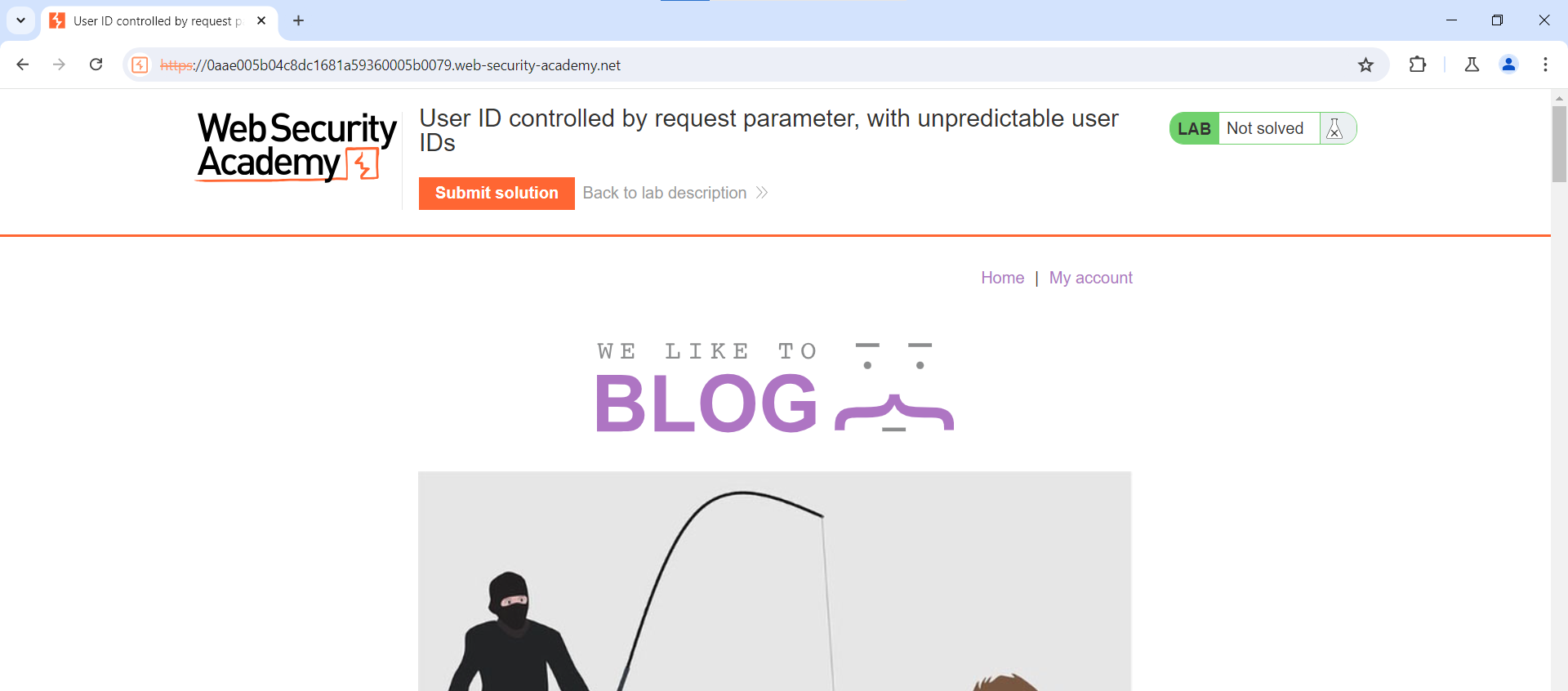
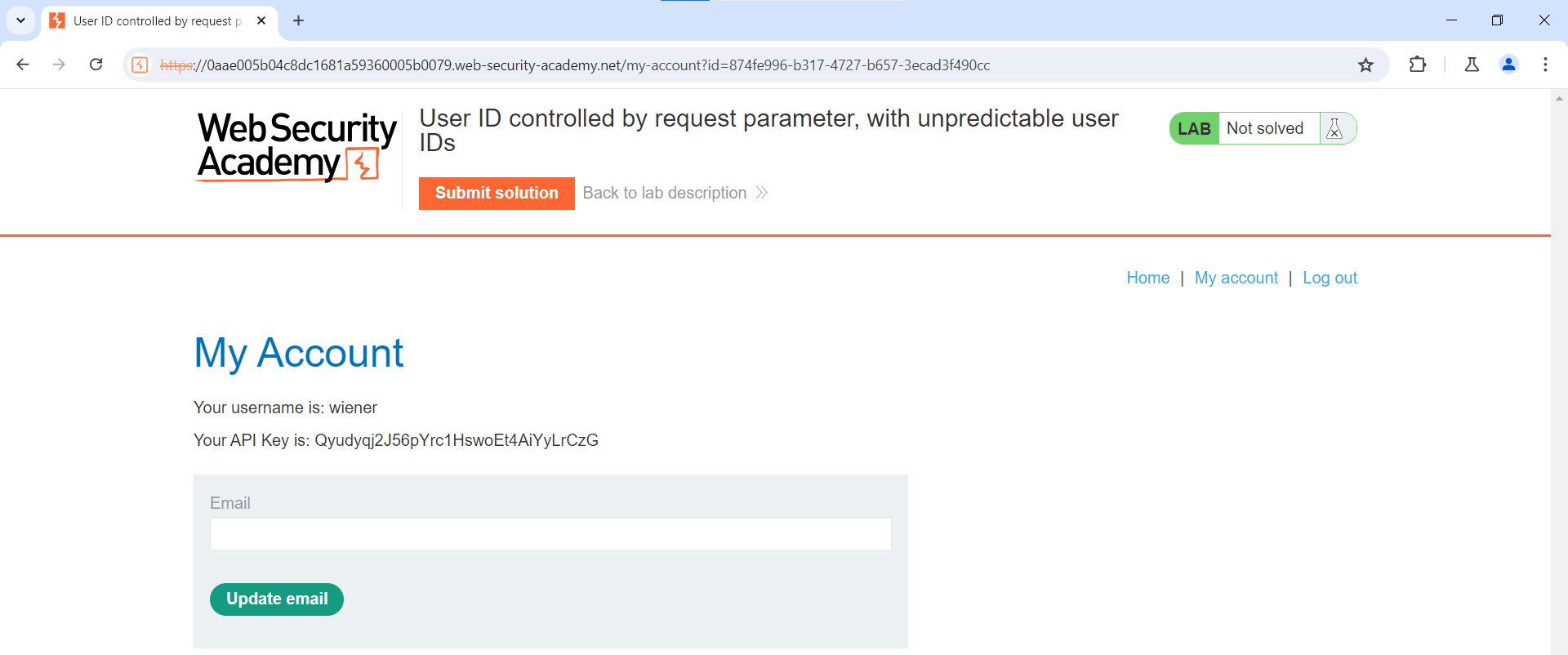


* Mục tiêu: Leo thang đặc quyền ngang từ tài khoản wiener sang tài khoản carlos



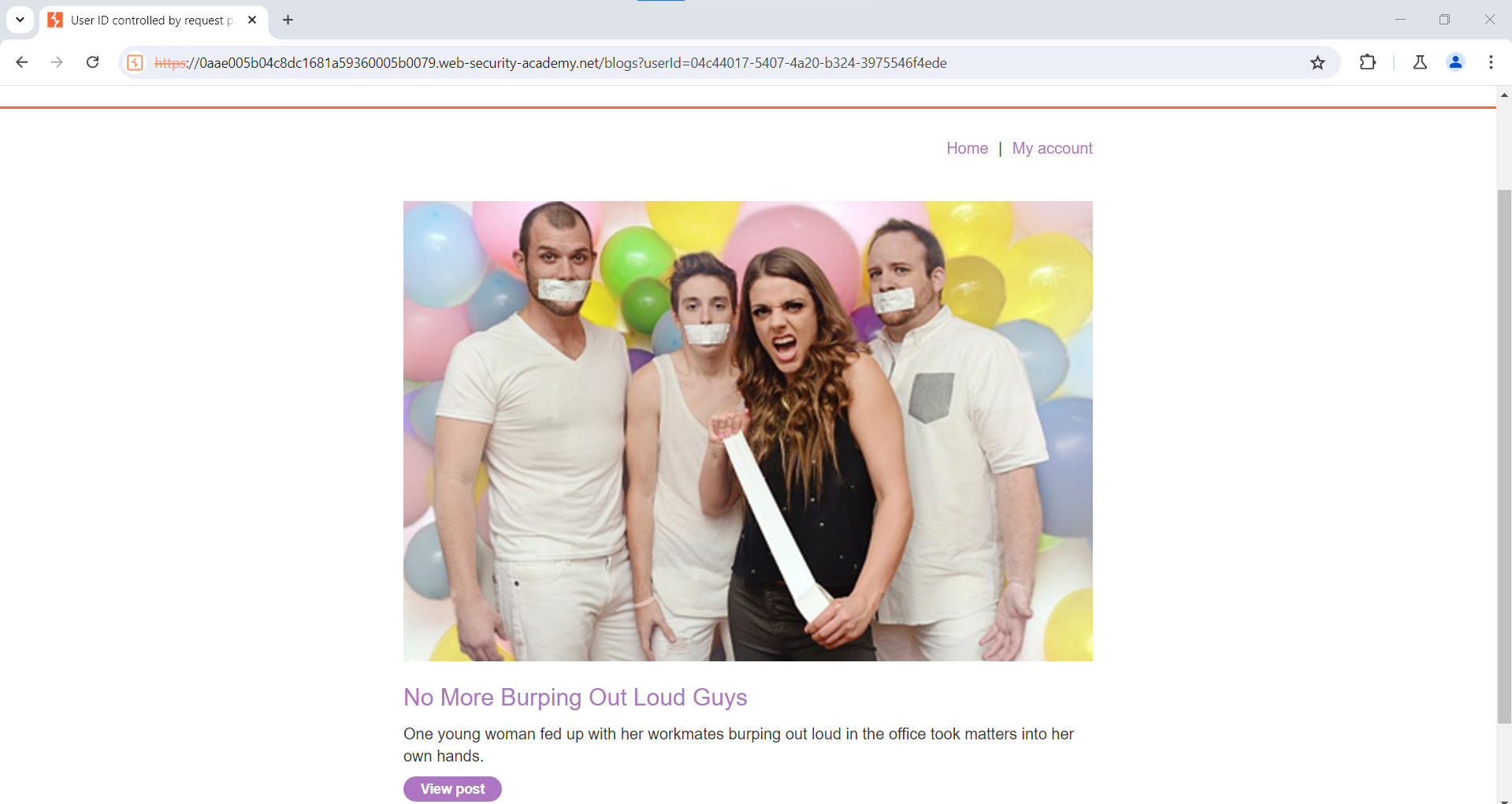
* Thử đăng nhập vào tài khoản admin để kiểm tra các chức năng



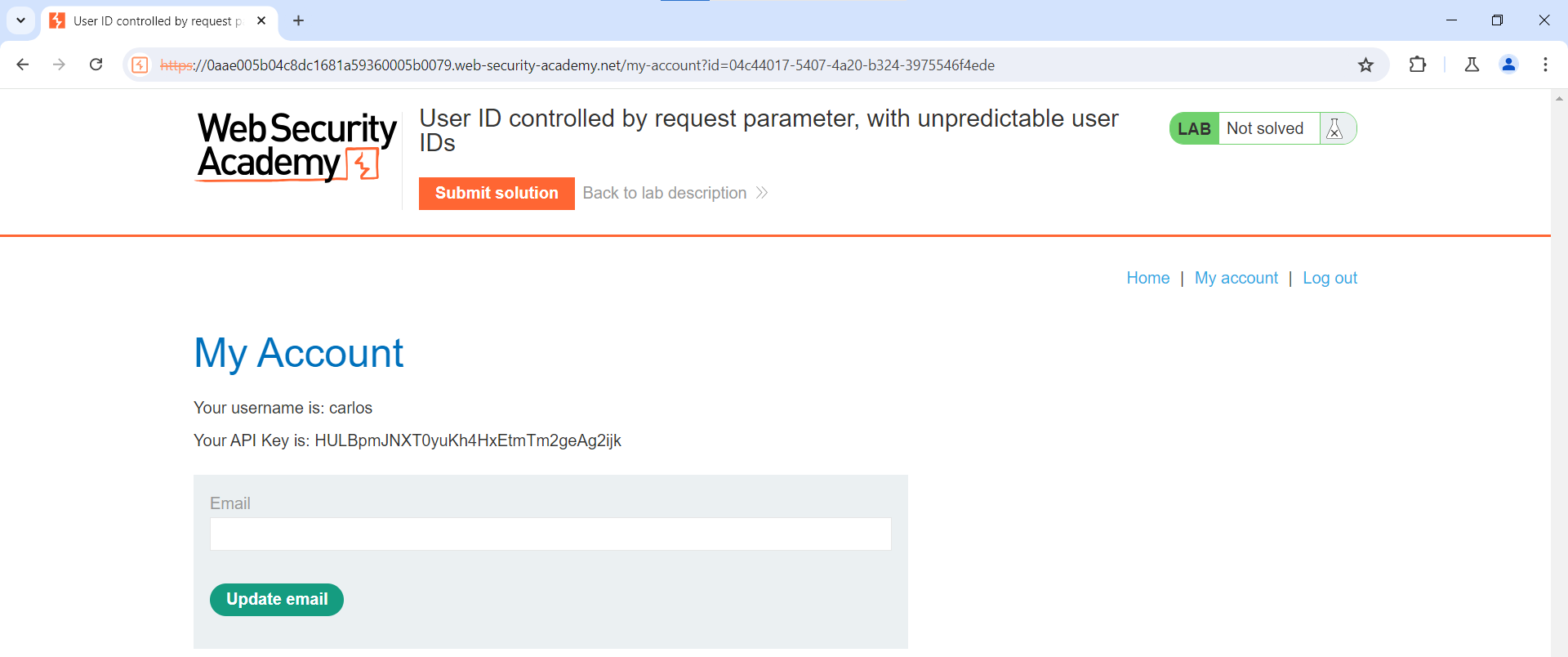
* Tìm thấy trên URL có trường id, tuy nhiên trường dữ liệu này không thể dự đoán được.
* Thử vào các bài post trên trang chủ thì tìm được bài viết của carlos.



* Chữ “carlos” dường như có thể ấn vào được.



* Xuất hiện các bài post mà người dùng này đã đăng tải lên web.
* Chú ý vào URL thì ta thấy có xuất hiện trường userId và trường này có format khá giống trường id ở trang my-account.
* Ta sẽ thử copy và thay thế trường id bên trang my-account xem có vào được tài khoản carlos không



* Đã lấy được thông tin tài khoản carlos.
* Submit API Key và hoàn thành bài lab.

