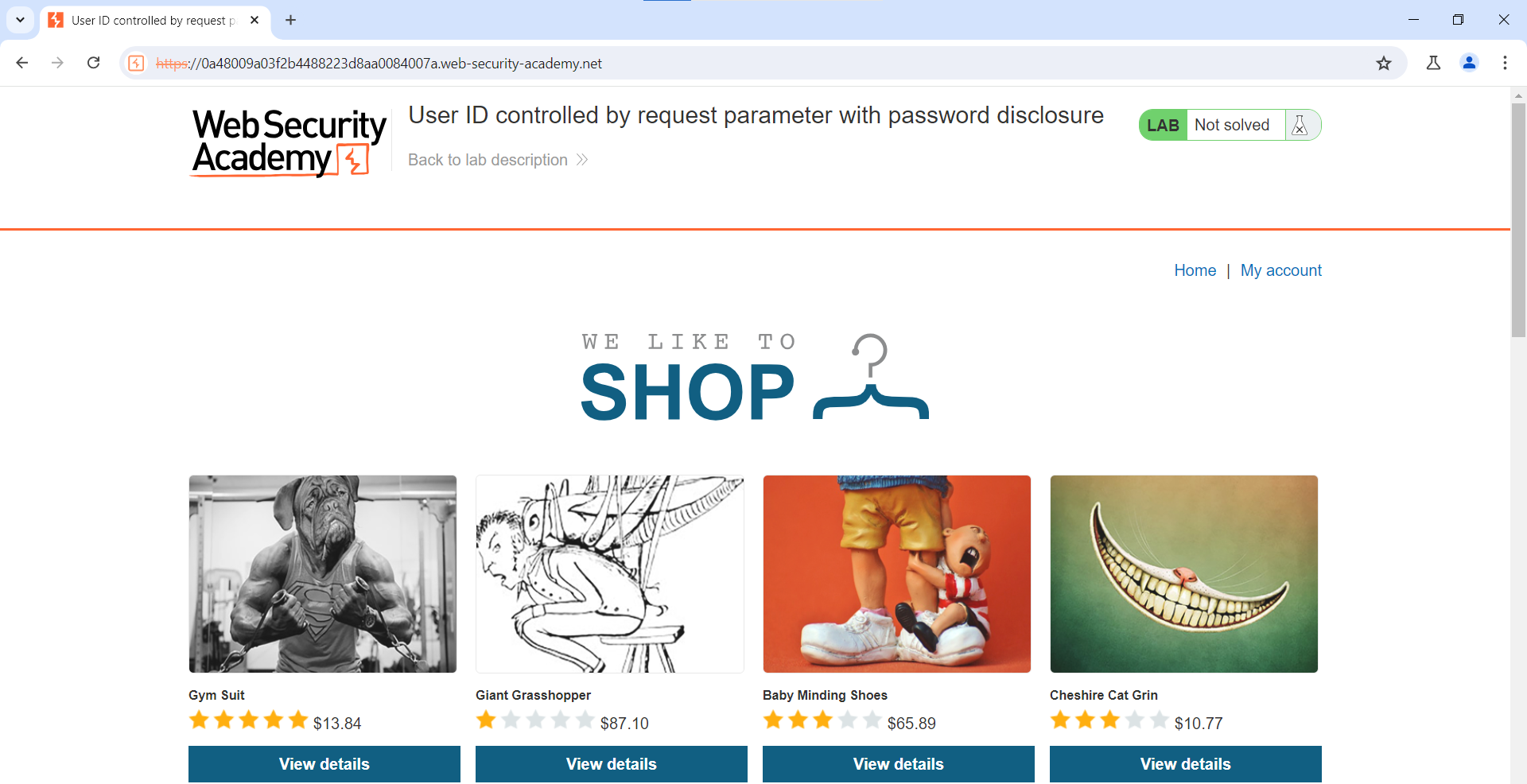
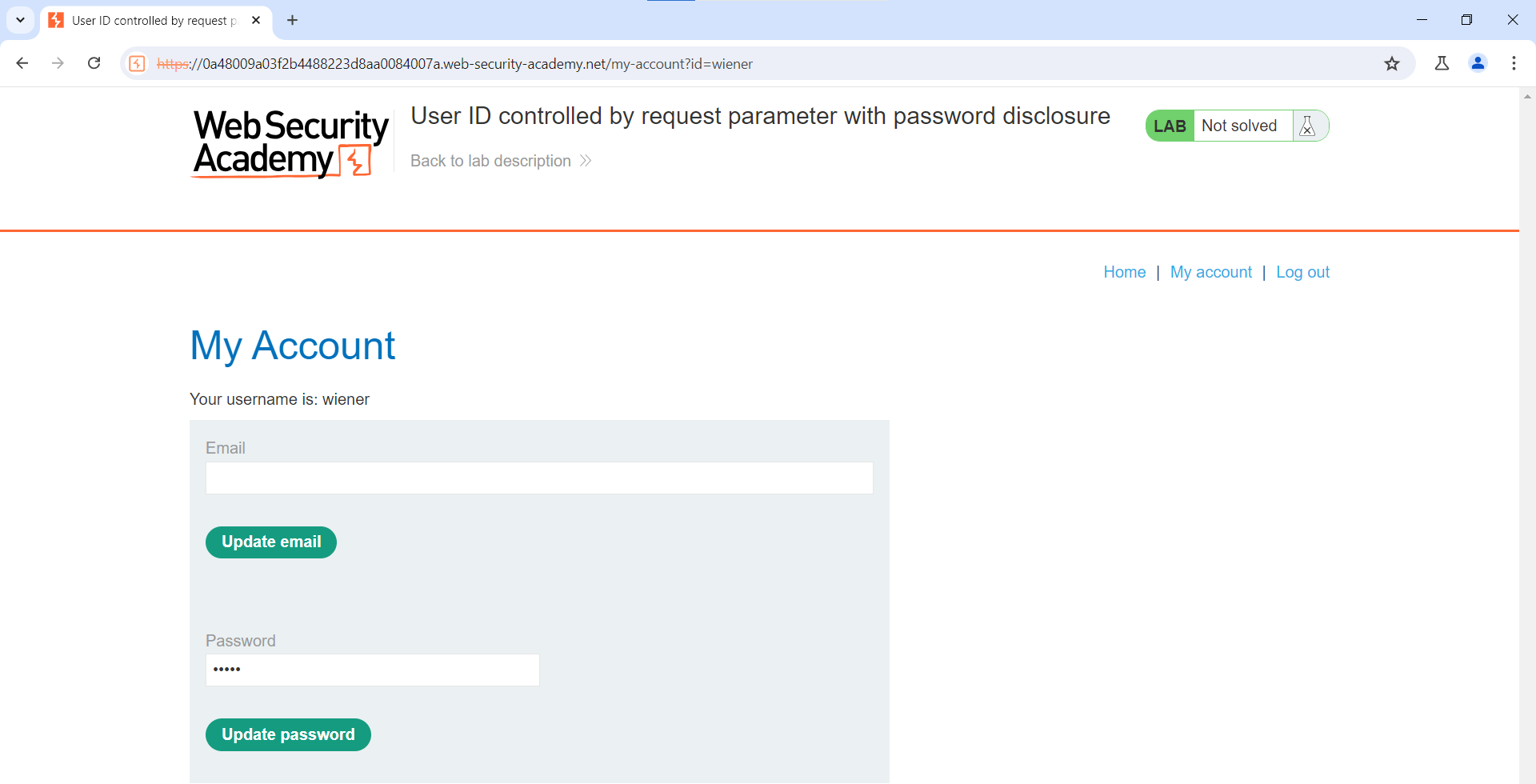


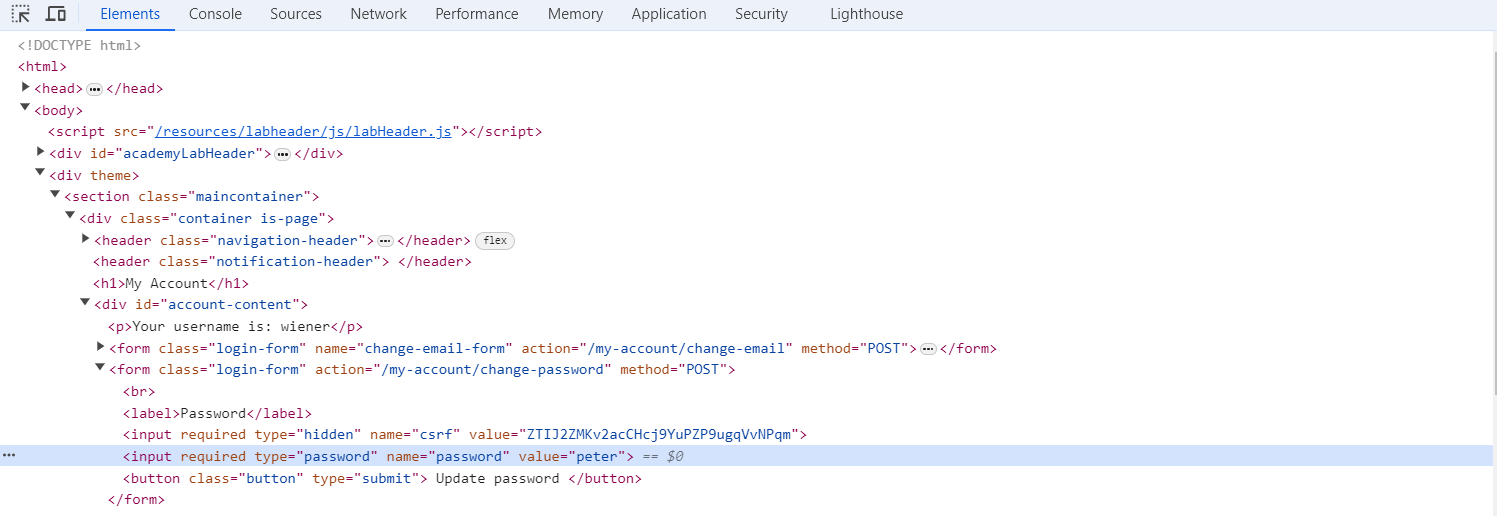
* Mục tiêu: Leo thang đặc quyền theo chiều ngang để truy cập vào tài khoản admin thông qua tài khoản wiener và xóa tài khoản carlos.



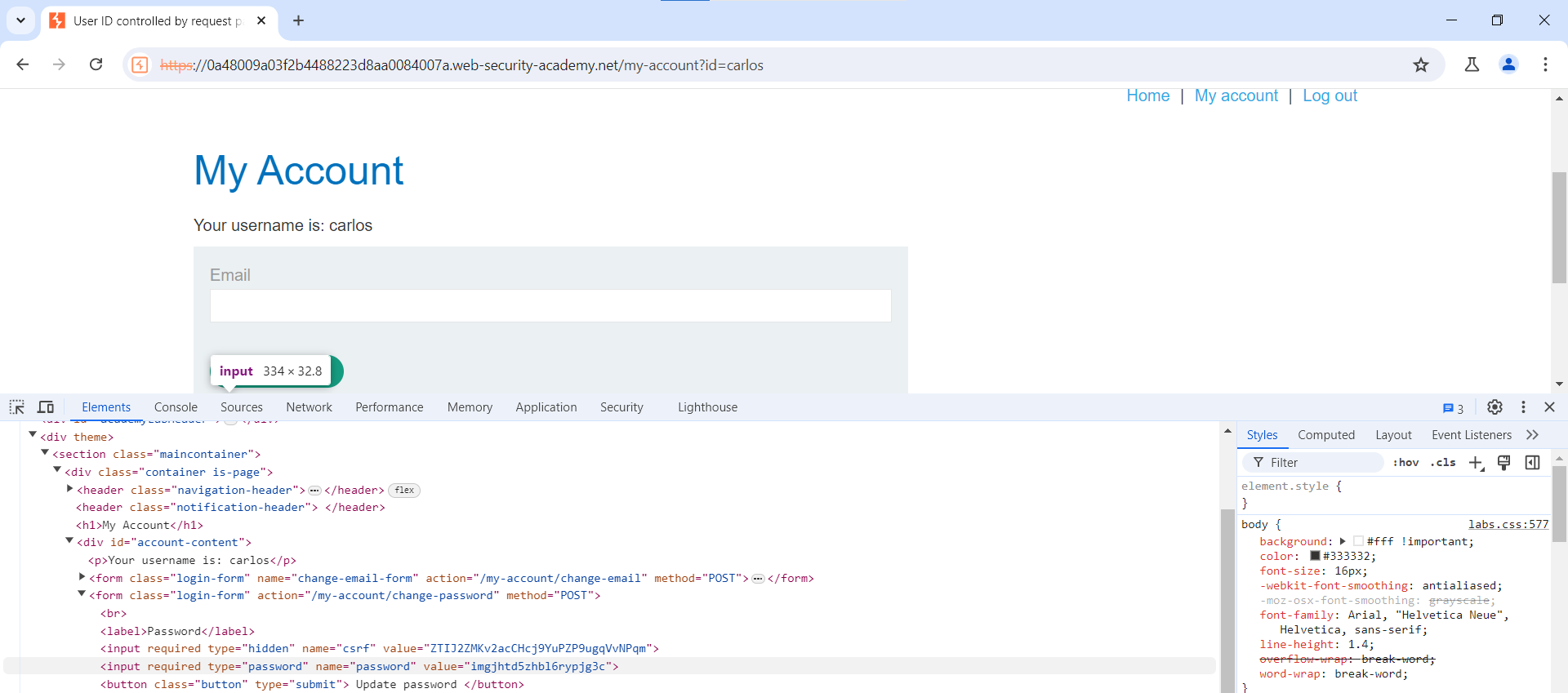
* Đăng nhập tài khoản wiener



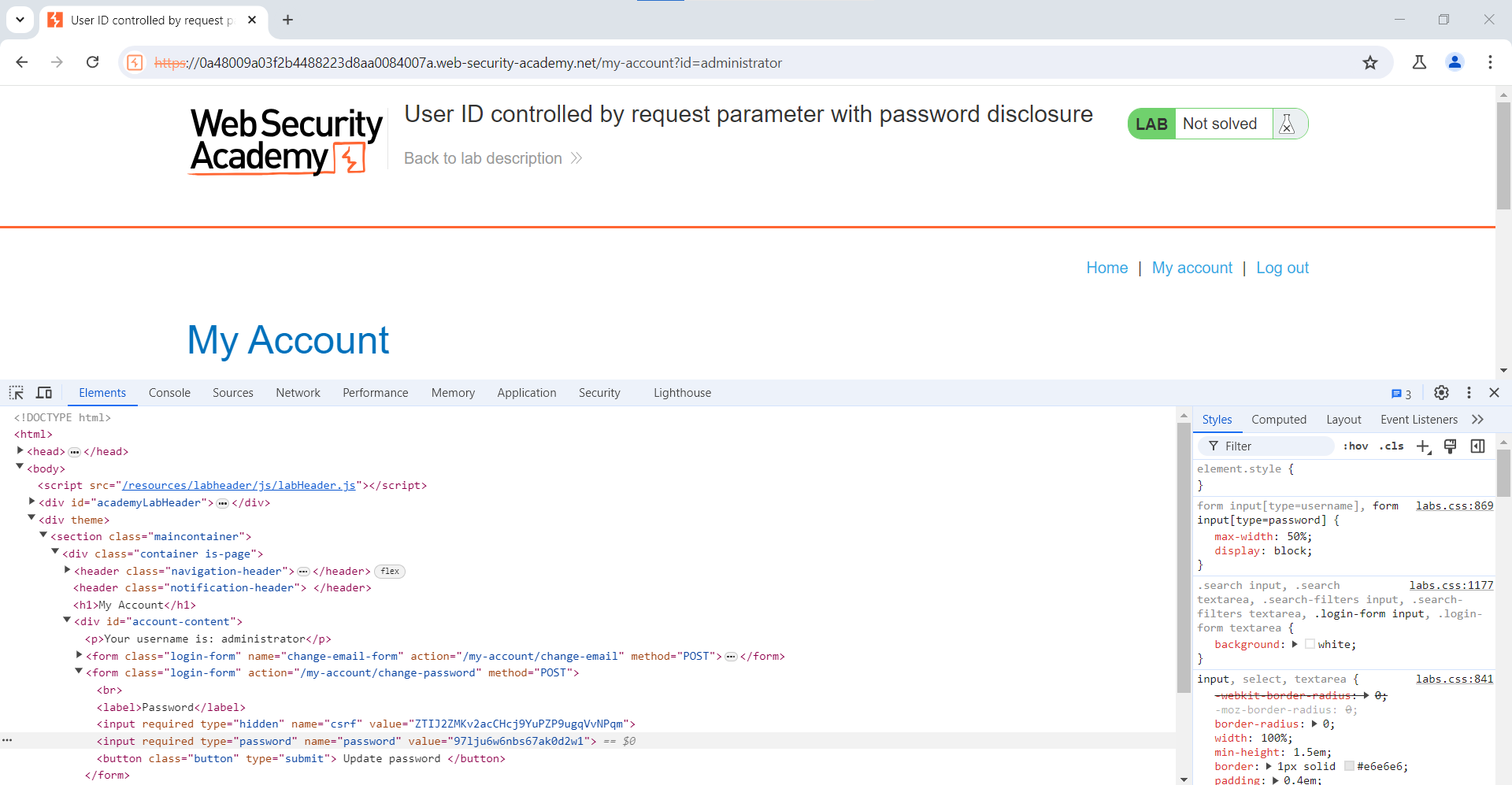
* Phát hiện Password hiện tại được lưu dưới dạng ẩn



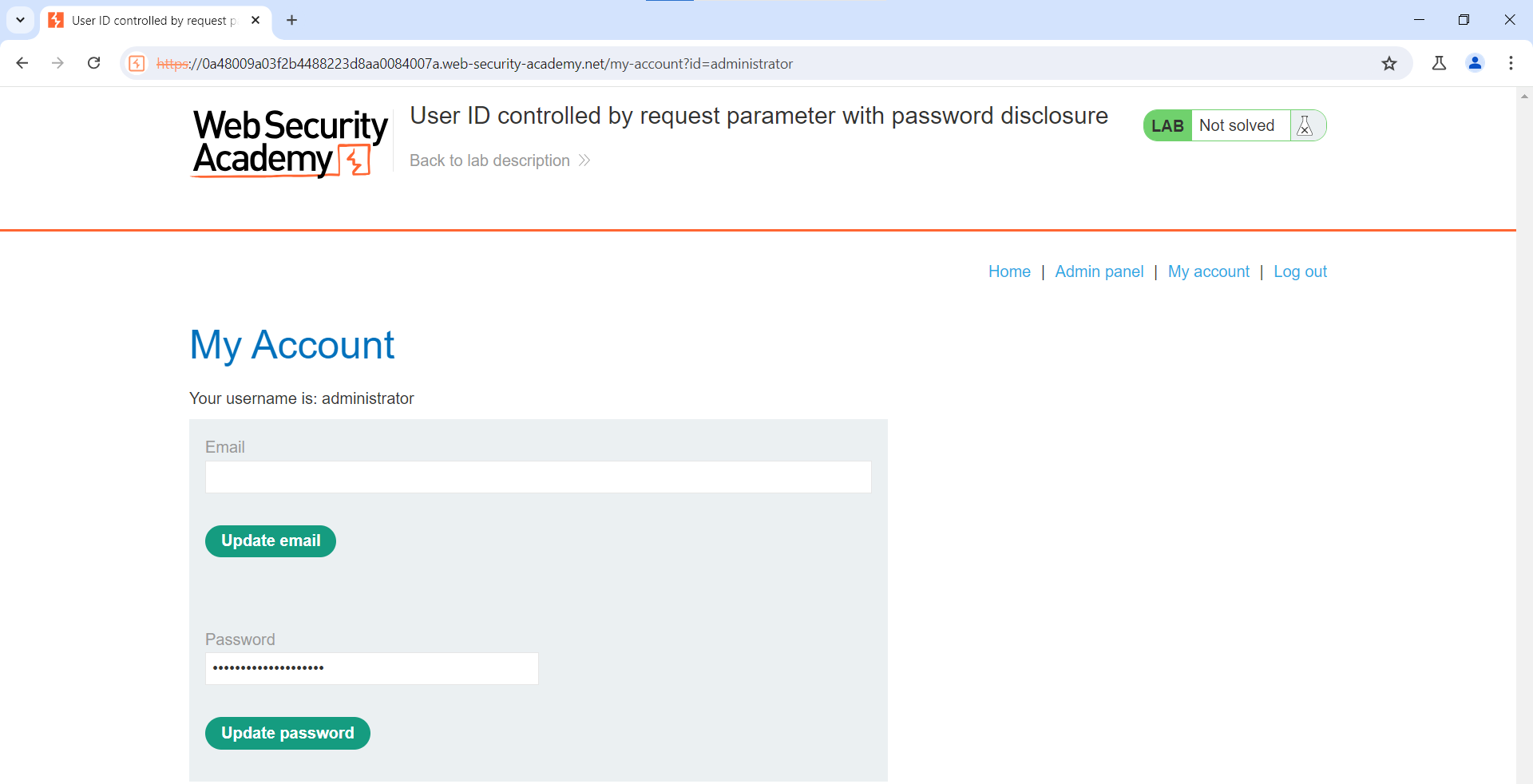
* Inspect thì hoàn toàn đọc được.
* Phát hiện trên URL có xuất hiện trường “id=wiener”
* Thử thay thế trường dữ liệu này thành carlos xem có vào được tài khoản đó không



* Vào được tài khoản của carlos và biết được mật khẩu của người dùng này
* Tuy nhiên, ta cần phải vào tài khoản của admin thì mới xóa được tài khoản carlos
* Thử các id khác nhau để vào tài khoản admin
* Username: administrator
* Password: 97lju6w6nbs67ak0d2w1



* Đăng xuất và đăng nhập tài khoản admin



* Truy cập vào trang quản lý người dùng và xóa tài khoản carlos

