Bài này có chức năng đặt lại mật khẩu. Mặc dù nó không chứa race condition, bạn có thể khai thác cơ chế mã hóa bằng cách gửi các yêu cầu canh thời gian cẩn thận.

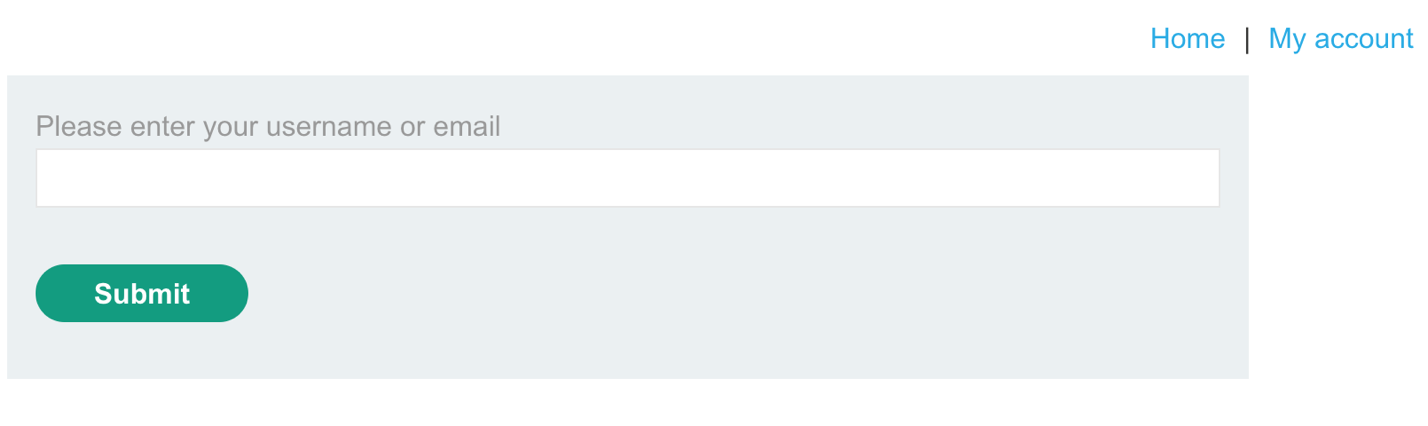
Để làm được bài này:

* Tìm hiểu cách trang web tạo token đặt lại mật khẩu
* Lấy được token đặt lại mật khẩu của người dùng carlos
* Đăng nhập carlos
* Truy cập giao diện admin và xóa người dùng carlos

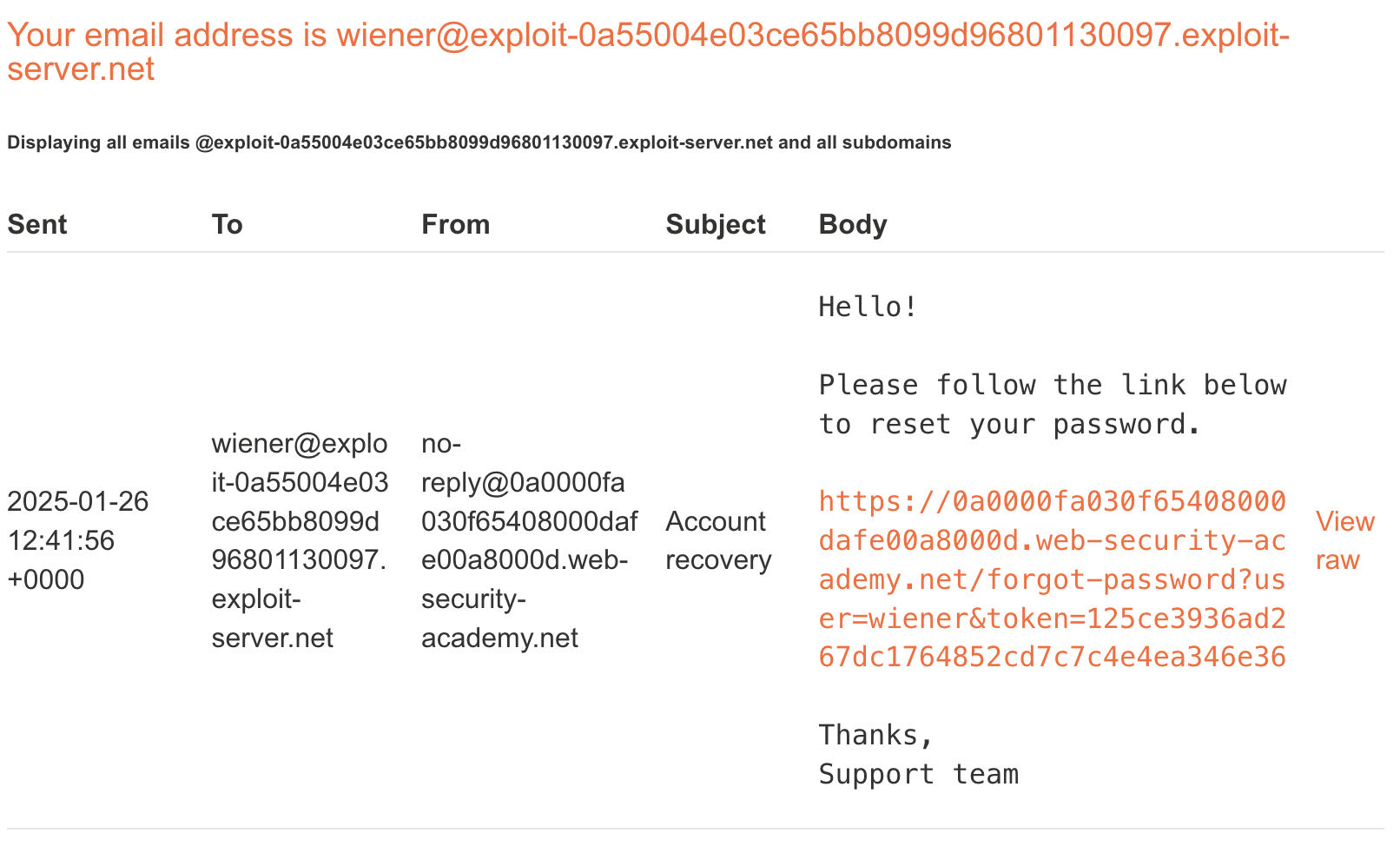
Chọn Forgot password



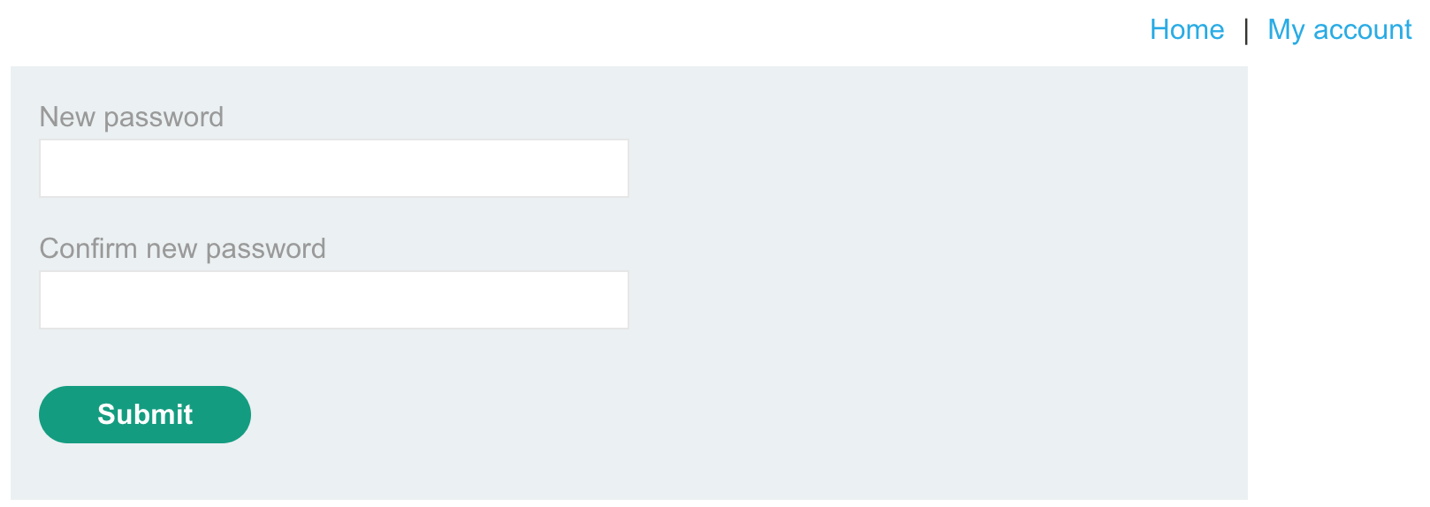
Nhập tên người dùng



Kiểm tra đường dẫn đặt lại mật khẩu ở email



Nhấp đường dẫn trên



Kiểm tra lại token:

125ce3936ad267dc1764852cd7c7c4e4ea346e36

Gửi 1 nhóm các yêu cầu đặt lại mật khẩu ở chế độ song song.

Quan sát thấy vẫn có sự trì hoãn giữa mỗi phản hồi và bạn nhận được các token khác nhau. Kết luận rằng các yêu cầu của bạn được xử lí theo chuỗi hơn là song song.

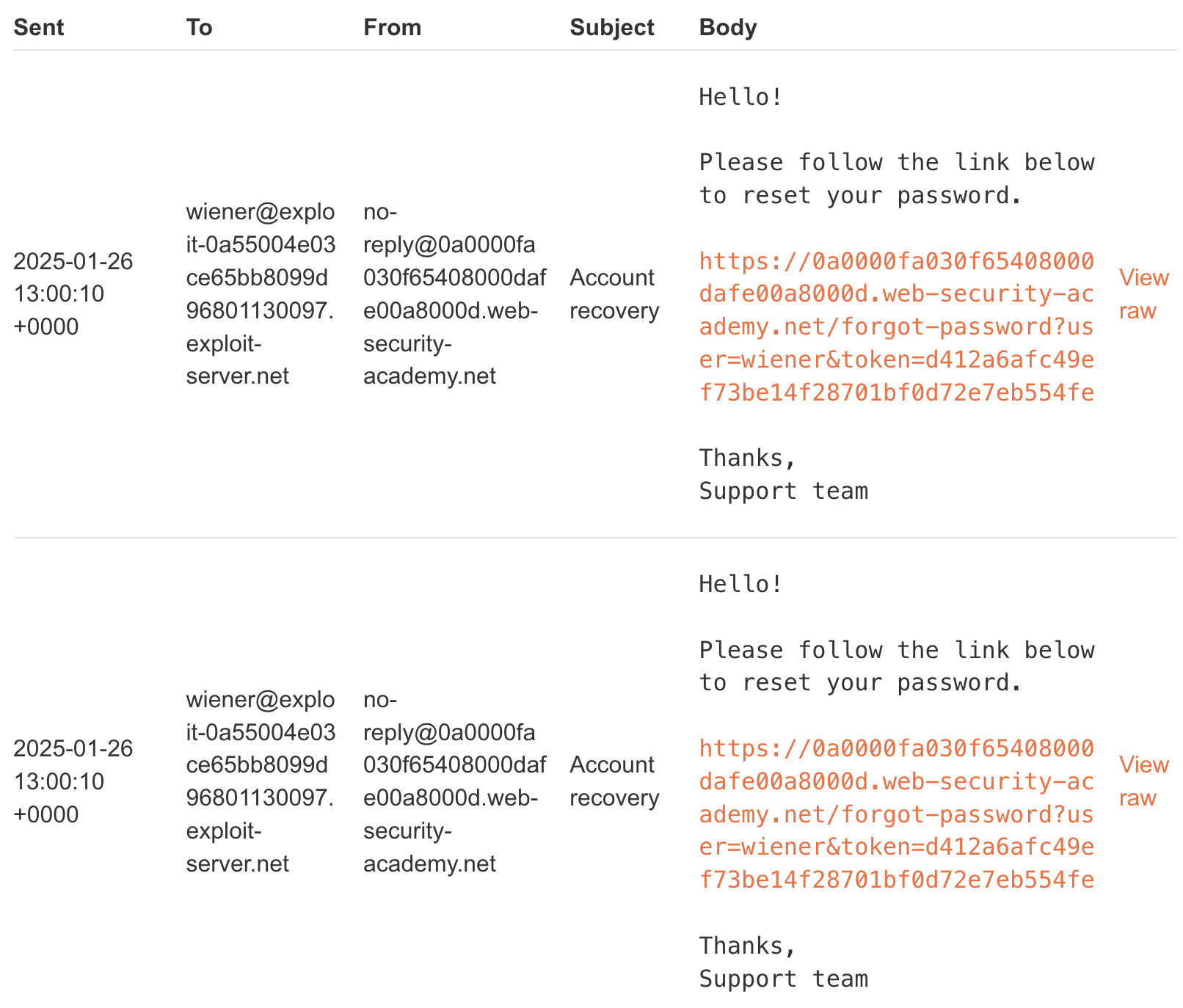
Để ý thấy session cookie để php là backend. Điều đó có nghĩa là máy chủ chỉ xử lý 1 yêu cầu vào 1 thời điểm mỗi phiên.

Gửi yêu cầu GET /forgot-password đến Burp Repeater, xóa session cookie và gửi lại nó.

Máy chủ sẽ cấp cho chúng ta 1 cookie mới

Trong nhóm yêu cầu, chỉnh sửa session cookie và mã csrf khác nhau, tên người dùng vẫn để là wiener

Kiểm tra lại hộp thư, chúng ta nhận được 2 mã token đặt lại mật khẩu giống nhau:



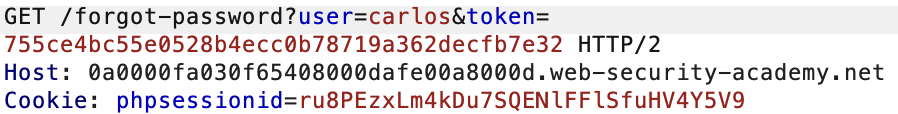
Kết luận rằng token tạo dựa trên timestamp.

Trong nhóm yêu cầu, chúng ta đổi yêu cầu thứ hai username=carlos

Khi đó người dùng carlos cũng sẽ nhận được 1 email giống với wiener

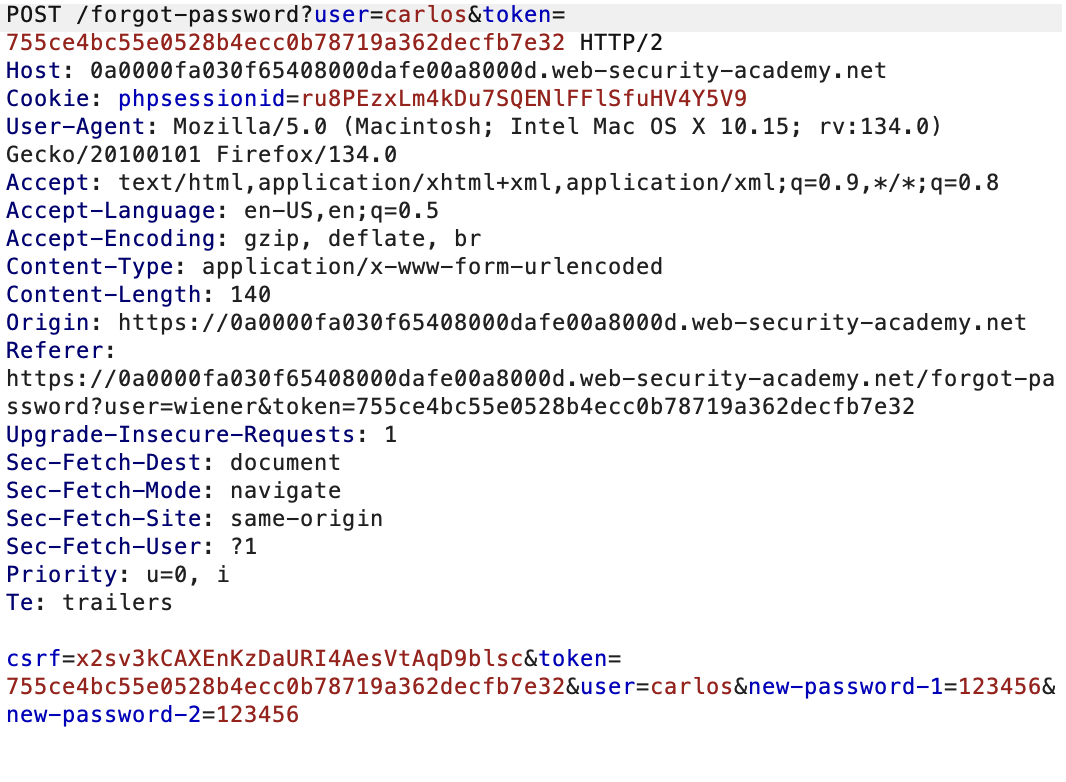
Phải bật intercept lên để chỉnh sửa các tham số

Chúng ta gửi 1 email xác nhận có token giống như wiener, nhưng tên để là carlos

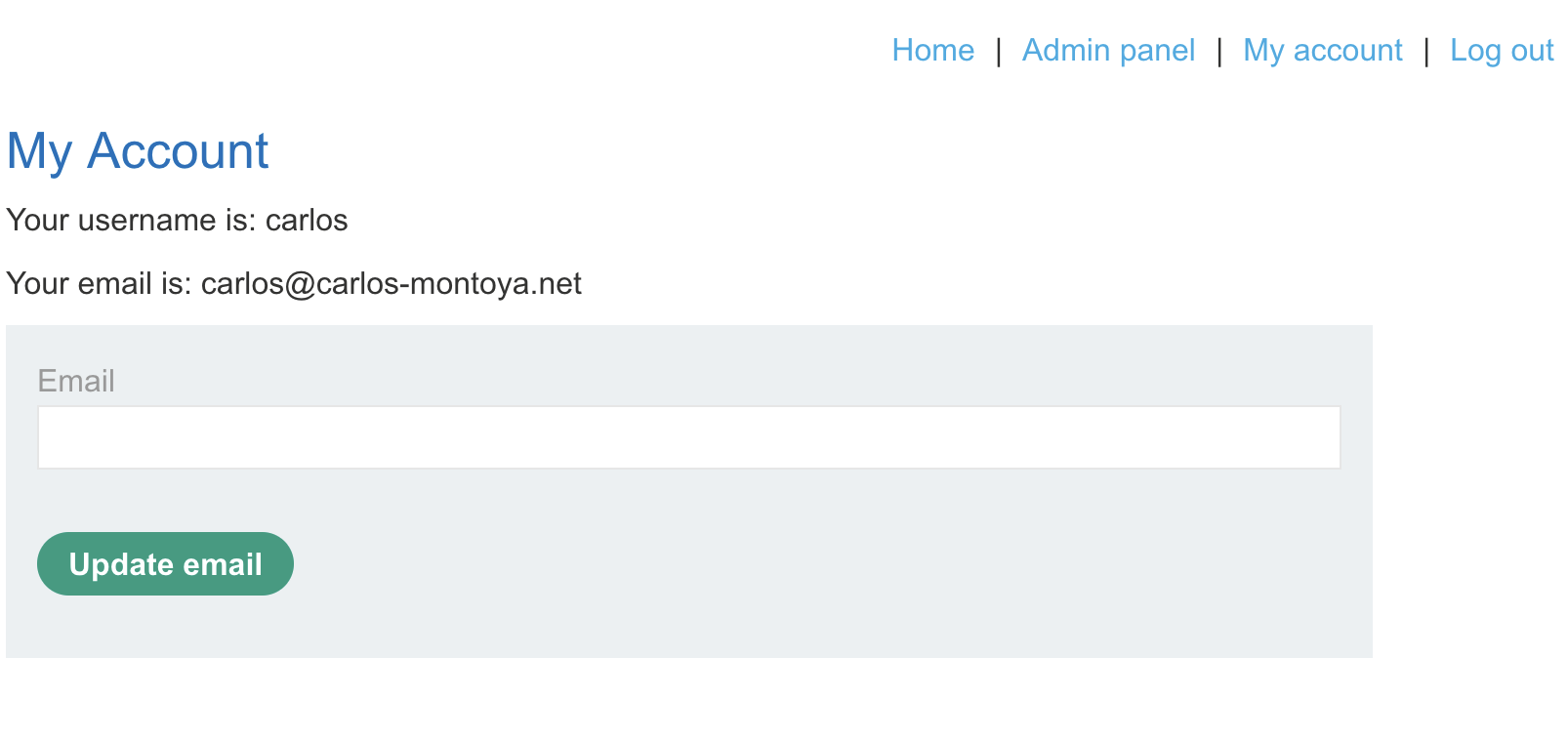


Nhớ đổi lại phpsessionid sao cho phù hợp

Nhập mật khẩu mới



Đặt lại mật khẩu thành công, đăng nhập carlos



Xóa người dùng carlos