**Single-endpoint race conditions**

Tính năng thay đổi email của thử thách này chứa lỗ hổng race conditions cho phép bạn liên kết 1 địa chỉ email bất kỳ với tài khoản của bạn.

Người dùng có email carlos@ginandjuice.shop được nhận lời mời trở thành quản trị viên của trang web, nhưng họ vẫn chưa tạo tài khoản mới. Do đó, bất kì người dùng nào sở hữu địa chỉ email này sẽ tự động kế thừa đặc quyền của admin.

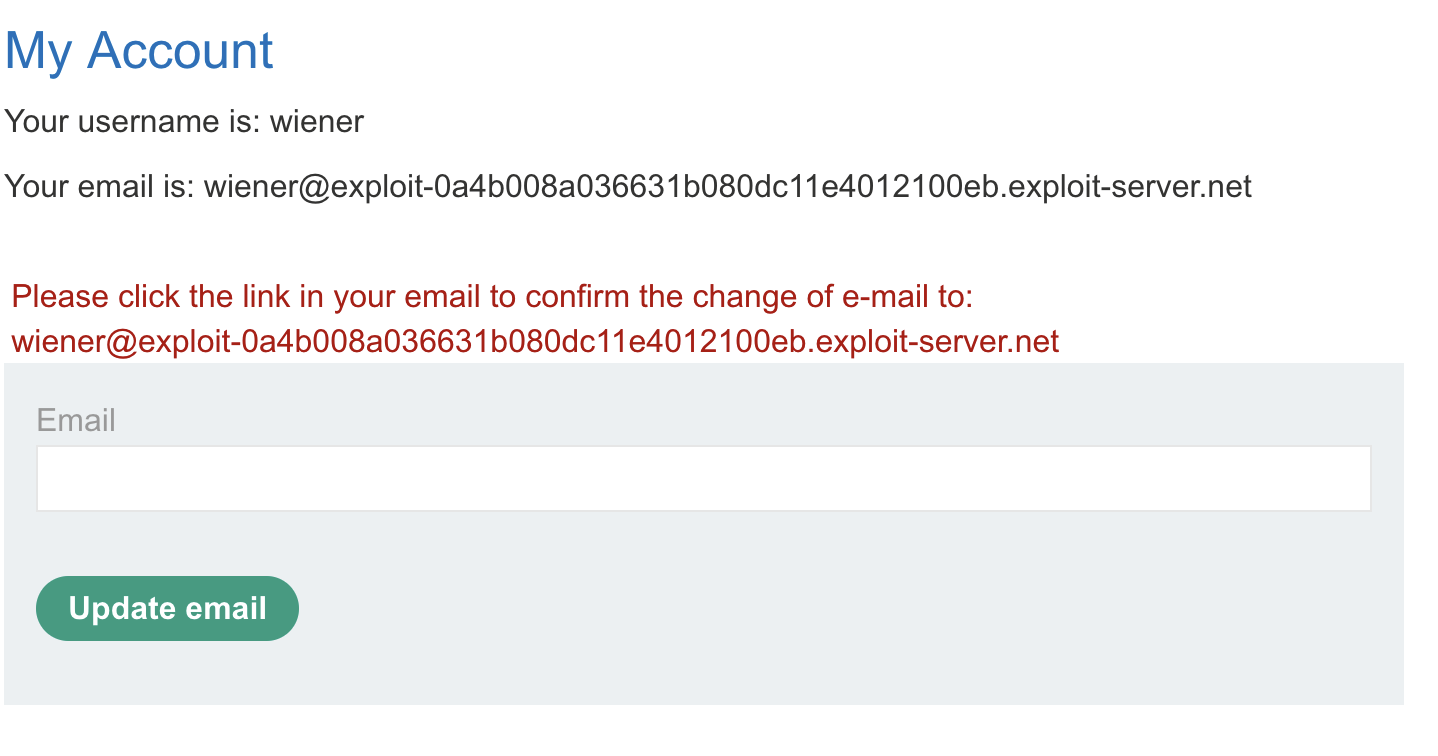
Để làm được bài này:

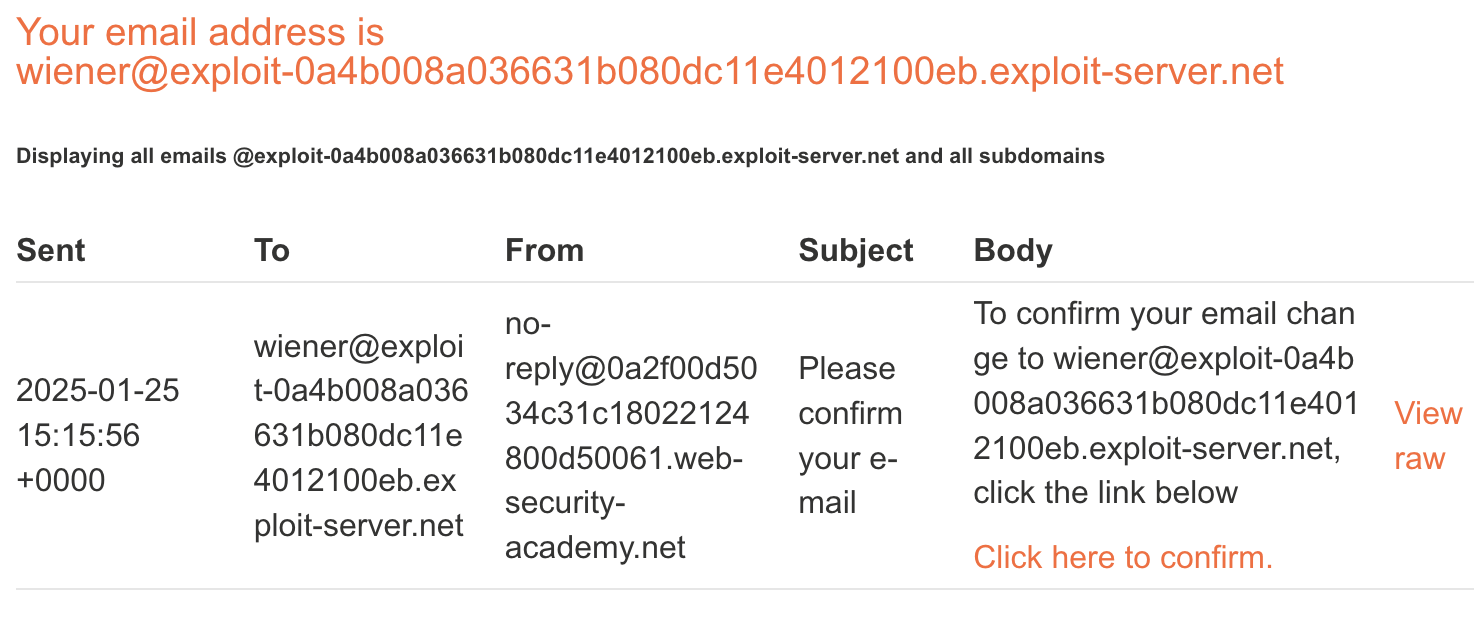
1. Xác định race condition cho phép bạn sở hữu 1 địa chỉ email bất kỳ
2. Thay đổi địa chỉ email của bạn thành carlos@ginandjuice.shop
3. Truy cập giao diện admin
4. Xóa người dùng carlos

Bạn có 1 máy chủ mail để nhận tất cả thư gửi đến

Tài khoản đăng nhập là wiener:peter

Đăng nhập và thay đổi email của bạn là anything@exploit-<YOUR-EXPLOIT-SERVER-ID>.exploit-server.net. Quan sát thấy email xác nhận được gửi đến email mới





Bấm xác nhận thì email được cập nhật thành công



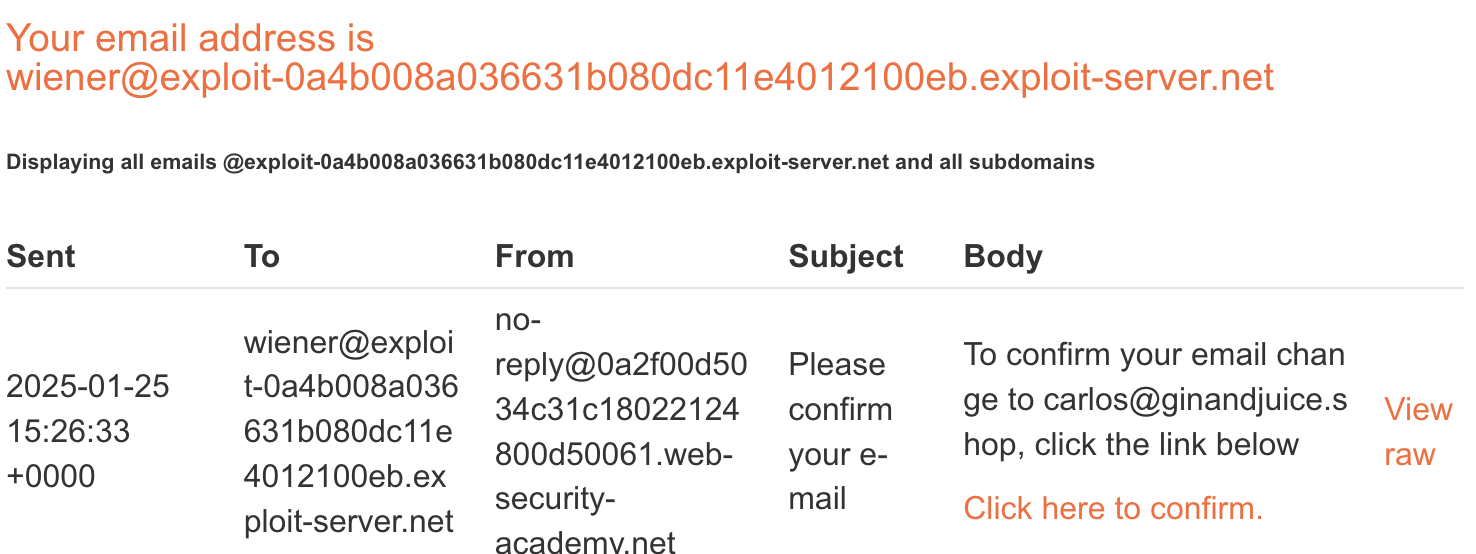
Tạo 1 nhóm 2 yêu cầu POST /my-account/change-email có 2 email khác nhau:

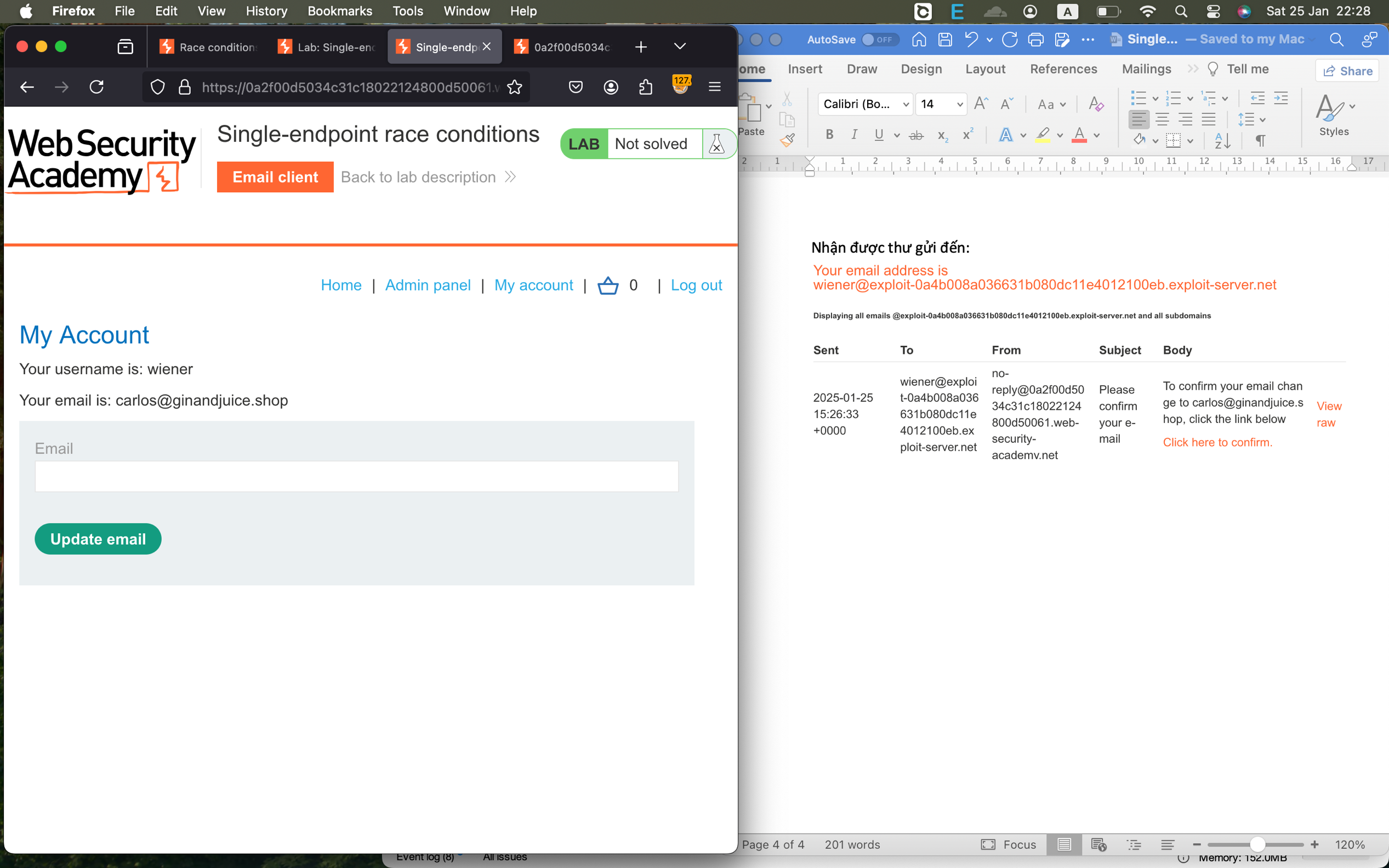
wiener@exploit-0a4b008a036631b080dc11e4012100eb.exploit-server.net

carlos@ginandjuice.shop

Gửi nhóm yêu cầu ở chế độ song song

Nhận được thư gửi đến:





🡪 Đổi mật khẩu thành công