SCENARIO

This 's email change feature contains a race condition that enables you to associate an arbitrary email address with your account. Someone with the address carlos@ginandjuice.shop has a pending invite to be an administrator for the site, but they have not yet created an account. Therefore, any user who successfully claims this address will automatically inherit admin privileges.

# PROCEDURE

1. Open the application and inspect it properly to look for possibilities of any potential collision and we see that there exists an user login functionality.
2. Log in with the provided credentials and study the request in BurpSuite’s Repeater and make 2 copies of it for **POST /my-account/change-email request.**
3. Change the email parameter of one request to [anything@exploit-<YOUR-EXPLOIT-SERVER-ID>.exploit-server.net](mailto:anything@exploit-%3cYOUR-EXPLOIT-SERVER-ID%3e.exploit-server.net) and the email parameter of the other request to [carlos@ginandjuice.shop](mailto:carlos@ginandjuice.shop).
4. Send the requests in parallel and if we received a confirmation email in which the address in the body is carlos@ginandjuice.shop, click the confirmation link to update your address.

## PAYLOAD

**REMEDIATION**