Csrf

**Lab: CSRF vulnerability with no defense**

Problem: This lab's email change functionality is vulnerable to CSRF.

Goal: To solve the lab, craft some HTML that uses a [CSRF attack](https://portswigger.net/web-security/csrf) to change the viewer's email address and upload it to your exploit server.

Solution:

1-A screenshot of a computer

Description automatically generated

2-A screenshot of a computer

Description automatically generated

3-

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

4-

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Lab: CSRF where token validation depends on request method**

Problem: This lab's email change functionality is vulnerable to CSRF. It attempts to block CSRF attacks, but only applies defenses to certain types of requests.

Goal: use your exploit server to host an HTML page that uses a [CSRF attack](https://portswigger.net/web-security/csrf) to change the viewer's email address.

Solution:

1-A screenshot of a computer

Description automatically generated

2-

A screenshot of a computer

Description automatically generated

3-

A screenshot of a computer

Description automatically generated

4-A screenshot of a computer

Description automatically generated

5-A screenshot of a computer

Description automatically generated

6-A screenshot of a computer

Description automatically generated

**Lab: CSRF where token validation depends on token being present**

Problem: This lab's email change functionality is vulnerable to CSRF.

Goal: use your exploit server to host an HTML page that uses a [CSRF attack](https://portswigger.net/web-security/csrf) to change the viewer's email address.

Solution:

1-

A screenshot of a computer

Description automatically generated

2-

A screenshot of a computer

Description automatically generated

3-A screenshot of a computer

Description automatically generated

4-A screenshot of a computer

Description automatically generated

5-

**Lab: CSRF where token is not tied to user session**

Problem: This lab's email change functionality is vulnerable to CSRF. It uses tokens to try to prevent CSRF attacks, but they aren't integrated into the site's session handling system.

Goal: To solve the lab, use your exploit server to host an HTML page that uses a [CSRF attack](https://portswigger.net/web-security/csrf) to change the viewer's email address.

Solution:

1-csrf=FrIqfNjOwCbJKZAuHlRTxNQVf4BuDLhb🡪wiener

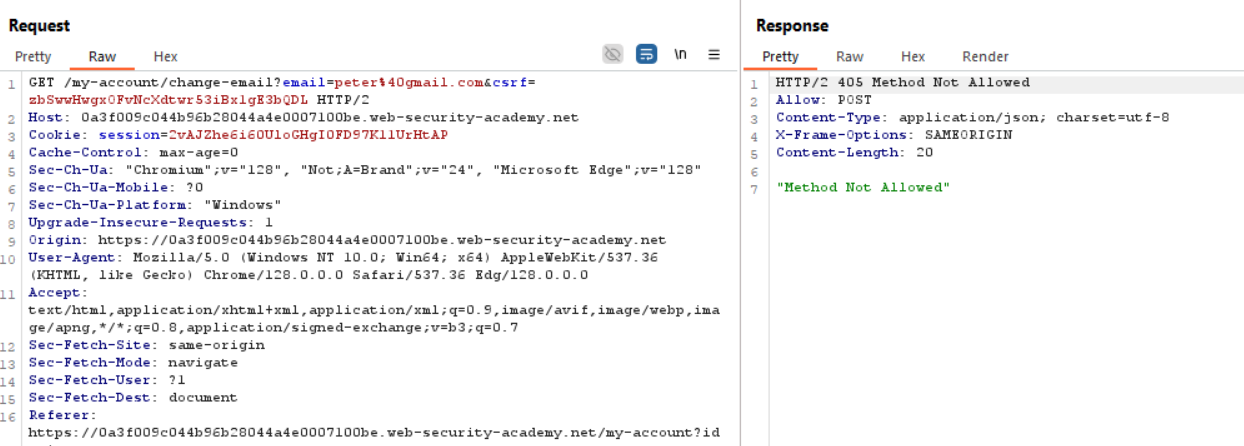
csrf=jH0bV3kKc2W5Q8bOd7FSCcf9Ic44lodF🡪carlos

2-

A screenshot of a computer

Description automatically generated

3-



4-we cant do this