[1. CSRF vulnerability with no defenses 2](#_Toc212727229)

[2. CSRF where token validation depends on request method 3](#_Toc212727230)

[3. CSRF where token validation depends on token being present 4](#_Toc212727231)

[4. CSRF where token is not tied to user session 6](#_Toc212727232)

[5. CSRF where token is tied to non-session cookie 7](#_Toc212727233)

[6. CSRF where token is duplicated in cookie 9](#_Toc212727234)

[7. SameSite Lax bypass via method override 10](#_Toc212727235)

[8. SameSite Strict bypass via client-side redirect 12](#_Toc212727236)

[9. SameSite Strict bypass via sibling domain 15](#_Toc212727237)

[10. SameSite Lax bypass via cookie refresh 20](#_Toc212727238)

[11. CSRF where Referer validation depends on header being present 22](#_Toc212727239)

[12. CSRF with broken Referer validation 23](#_Toc212727240)

# CSRF vulnerability with no defenses

A screenshot of a computer

AI-generated content may be incorrect.

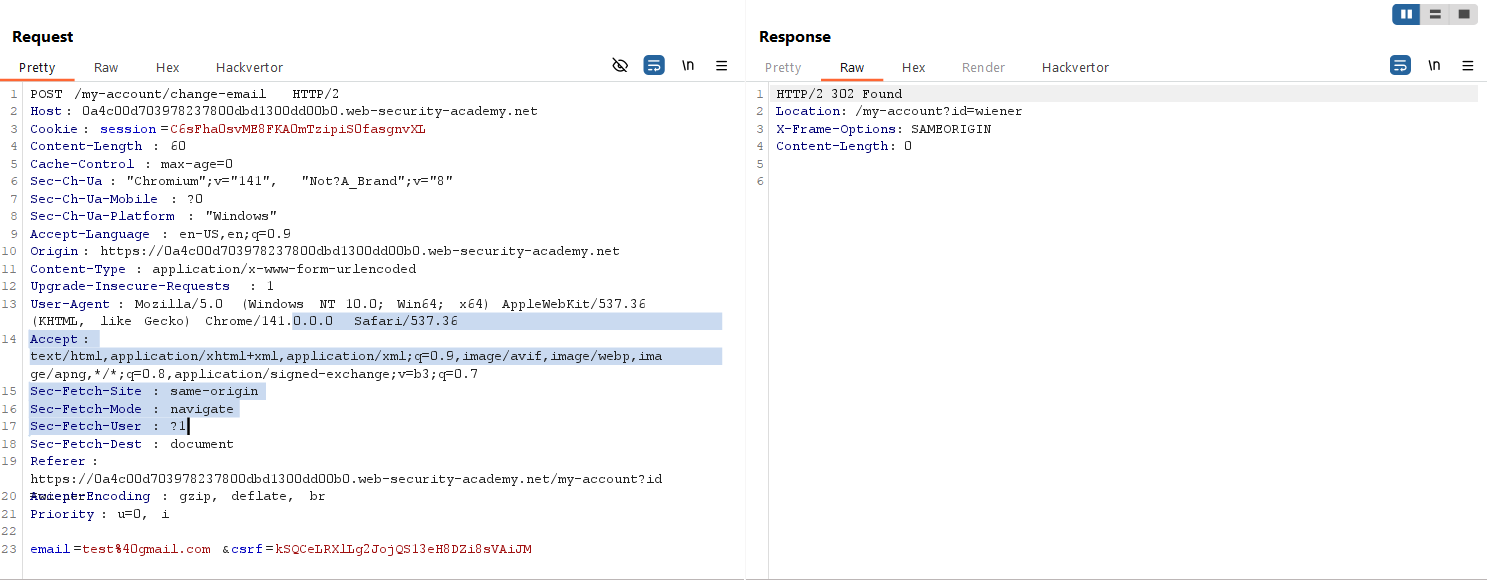
A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# CSRF where token validation depends on request method



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

# CSRF where token validation depends on token being present

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# CSRF where token is not tied to user session

Trên tài khoản của wiener:peter, capture request update email để lấy csrf token.

A screenshot of a computer

AI-generated content may be incorrect.

Trên tài khoản carlos:montoya, capture request update mail và thay csrf token ở trên và xác nhận rằng token vẫn hoạt động.

A screenshot of a computer

AI-generated content may be incorrect.

Giờ thì tạo dùng 1 csrf token mới để đưa vào trong POC generate CSRF rồi deliver đến victim để solve lab.

# CSRF where token is tied to non-session cookie

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A white rectangular object with a white line

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer code

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# CSRF where token is duplicated in cookie

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer code

AI-generated content may be incorrect.

# SameSite Lax bypass via method override

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

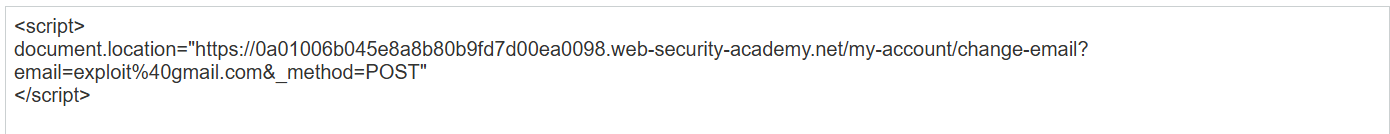
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



# SameSite Strict bypass via client-side redirect

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer code

AI-generated content may be incorrect.

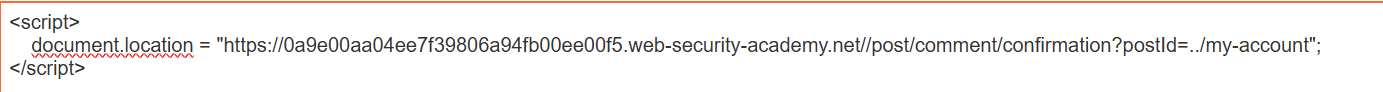
A computer code with black text

AI-generated content may be incorrect.



A close up of a text

AI-generated content may be incorrect.

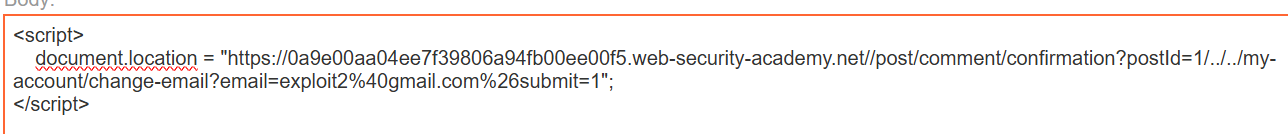


A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



# SameSite Strict bypass via sibling domain

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Confirm the CSWSH vulnerability:

A white background with text

AI-generated content may be incorrect.

Store => view exploit => check in collaborator

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Notice that your session cookie was not sent with the request.

In the response, notice that the website explicitly specifies SameSite=Strict when setting session cookies. This prevents the browser from including these cookies in cross-site requests.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Copy url with the GET request then paste in address bar:

A screenshot of a chat

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A close-up of a text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# SameSite Lax bypass via cookie refresh

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

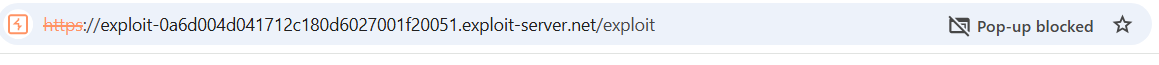
/social-login

From the proxy history, notice that every time you complete the OAuth flow, the target site sets a new session cookie even if you were already logged in.

A screenshot of a computer

AI-generated content may be incorrect.

Note that we've opened the /social-login in a new window to avoid navigating away from the exploit before the change email request is sent.



A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

When prompted, click the page. This triggers the OAuth flow and issues you a new session cookie. After 5 seconds, notice that the CSRF attack is sent and the POST /my-account/change-email request includes your new session cookie.

# CSRF where Referer validation depends on header being present

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A computer code on a white background

AI-generated content may be incorrect.

# CSRF with broken Referer validation

A screenshot of a chat

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Dùng hàm history.pushState()

