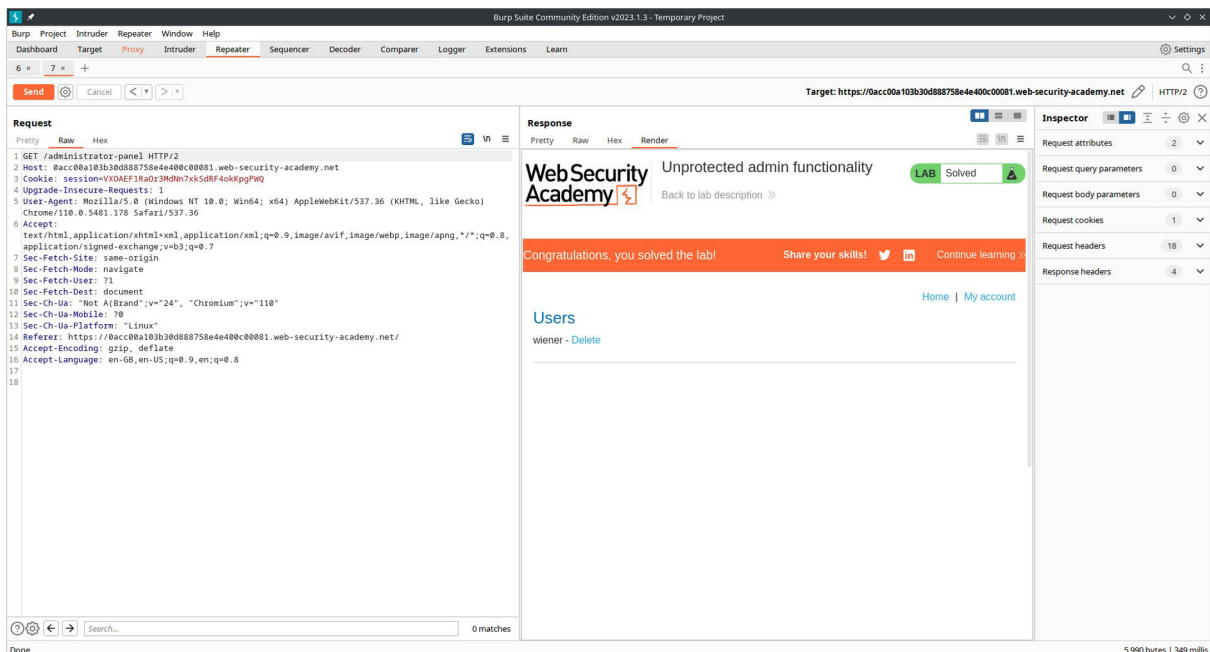
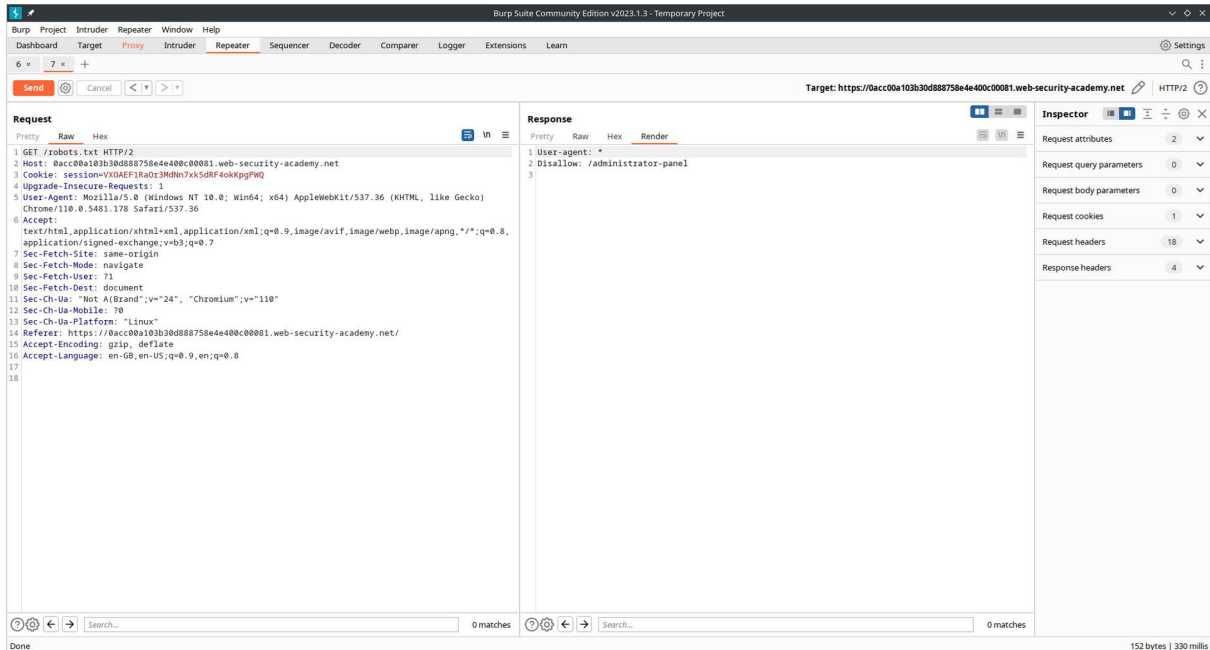


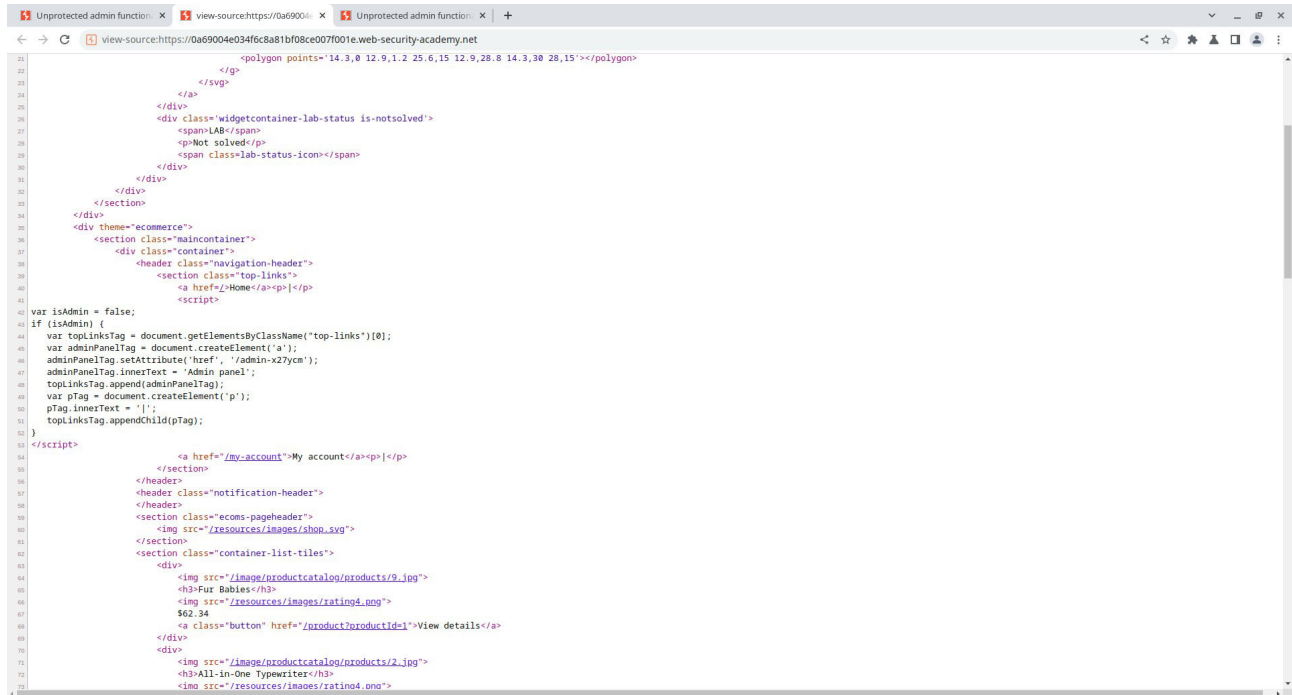
Lab: Unprotected admin functionality

Open the burpsuite and turn on the intercept in the proxy. Append the value /robots.txt to the url and forward the value to the repeater and we get the path to the admin panel that is /administrator-panel. Now append this value the actual url and you will be able to delete the user carlos.

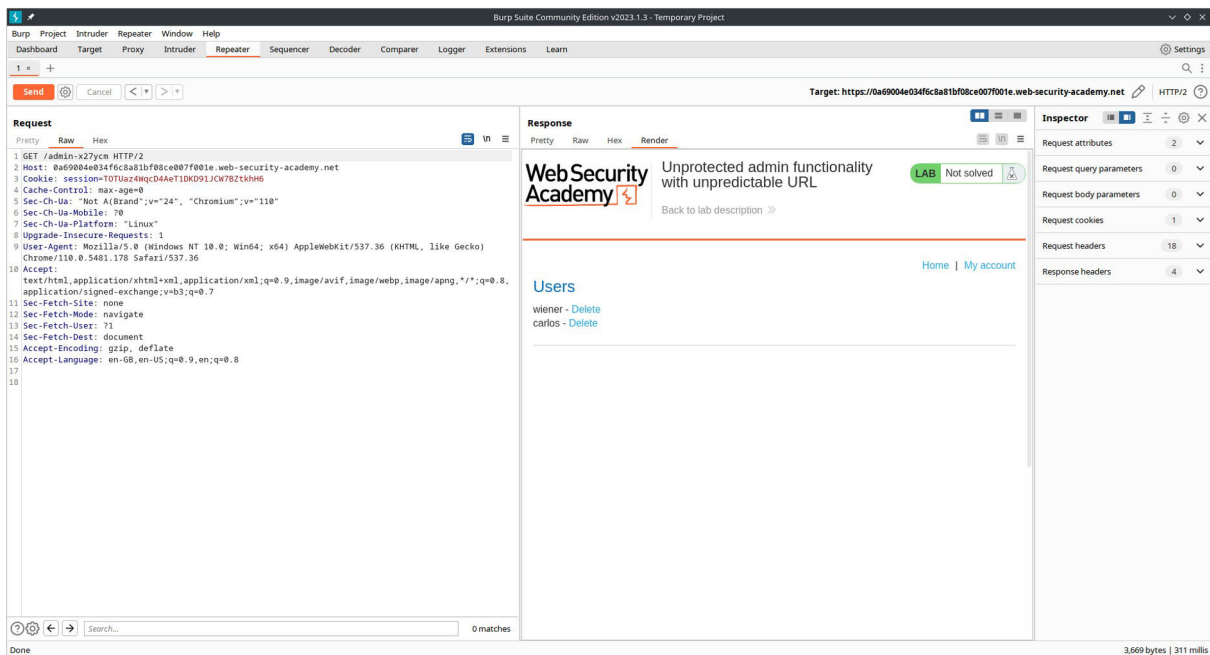


Lab: Unprotected admin functionality with unpredictable URL

Open the burpsuite and turn on the intercept in the proxy. Append the value /robots.txt to the url and forward the value to the repeater and this it doesn't work. So try checking the javascript source code of the page to get to the admin functionality. There you can get the value /admin-xy27cm. Now append this value the actual url and send forward this traffic to the repeater and you will be able to delete the user carlos.



```
21 </g>
22 </svg>
23 </a>
24 </div>
25 <div class="widgetcontainer-lab-status is-notsolved">
26 <span>LAB</span>
27 <p>Not solved</p>
28 <span class="lab-status-icon"></span>
29 </div>
30 </div>
31 </div>
32 </div>
33 </section>
34 </div>
35 <div theme="ecommerce">
36 <section class="maincontainer">
37 <div class="container">
38 <header class="navigation-header">
39 <section class="top-links">
40 <a href="/home">Home</a><p></p>
41 </script>
42 </div>
43 </div>
44 </div>
45 </div>
46 </div>
47 </div>
48 </div>
49 </div>
50 </div>
51 </div>
52 </div>
53 </div>
54 </div>
55 </div>
56 </div>
57 </div>
58 </div>
59 </div>
60 </div>
61 </div>
62 </div>
63 </div>
64 </div>
65 </div>
66 </div>
67 </div>
68 </div>
69 </div>
70 </div>
71 </div>
72 </div>
73 </div>
```

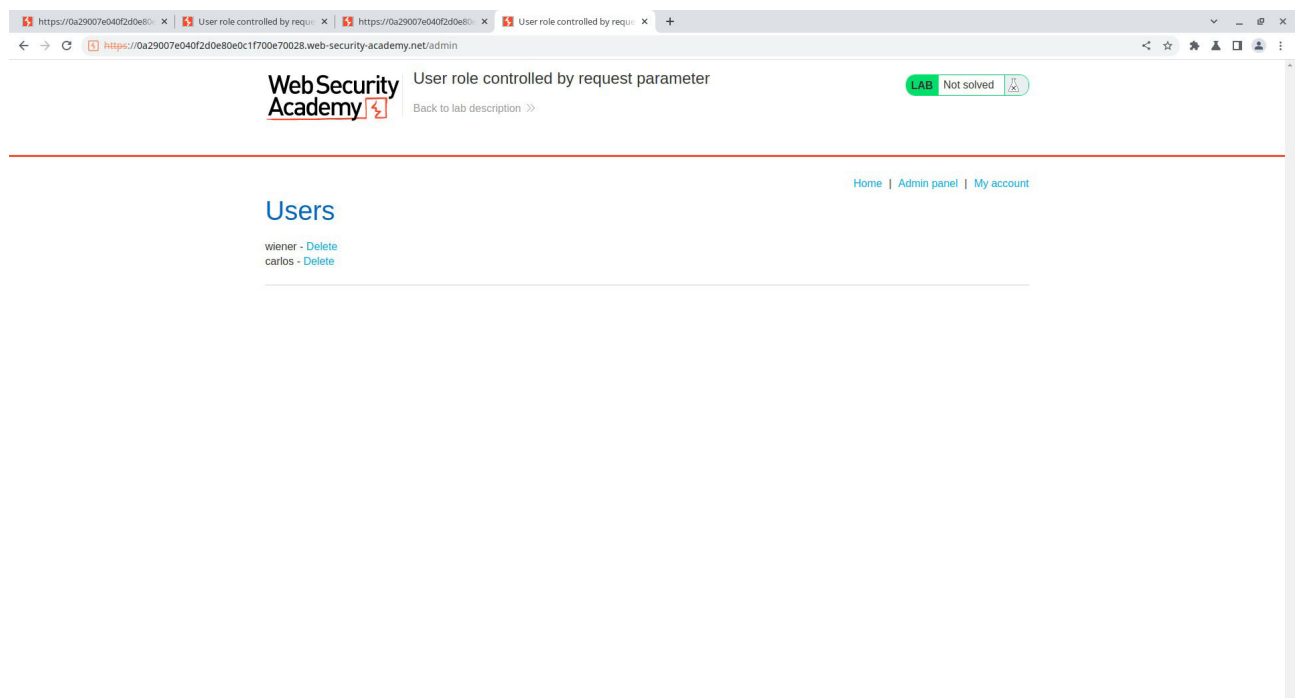
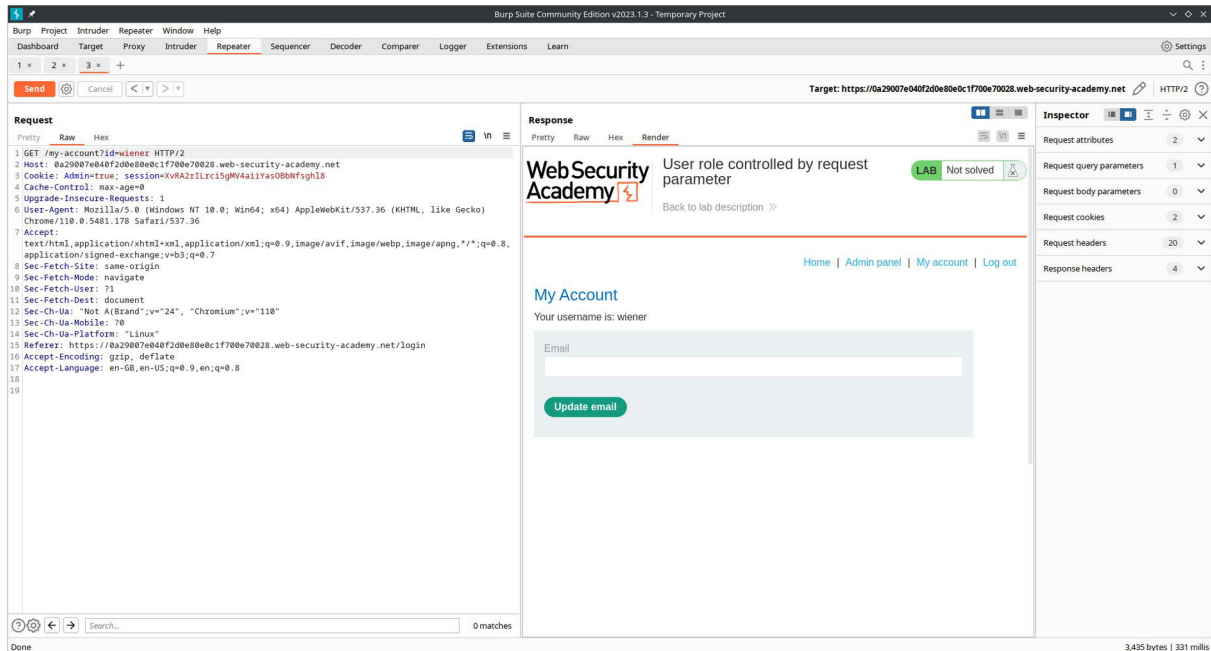


The screenshot shows a web browser window with the following content:

- Browser Tabs:** Three tabs are open, all titled "Unprotected admin function...". The active tab shows the URL `https://0a69004e034f6c8a81bf08ce007f001e.web-security-academy.net/admin-x27ycm`.
- Page Header:**
 - Logo:** WebSecurity Academy
 - Title:** Unprotected admin functionality with unpredictable URL
 - Status:** LAB Solved (indicated by a green badge)
 - Link:** Back to lab description >>
- Red Banner:** A red banner with the text "Congratulations, you solved the lab!".
- Share Section:** A section with the text "Share your skills!" and social media icons for Twitter and LinkedIn, followed by a "Continue learning >>" link.
- User Status:** A message "User deleted successfully!" is displayed.
- Users List:**
 - Section Header:** Users
 - User Entry:** wiener - Delete (with a blue "Delete" link)
- Footer:** A dark taskbar at the bottom of the screen shows various application icons and the system clock indicating 1:11 PM on 02/03/24.

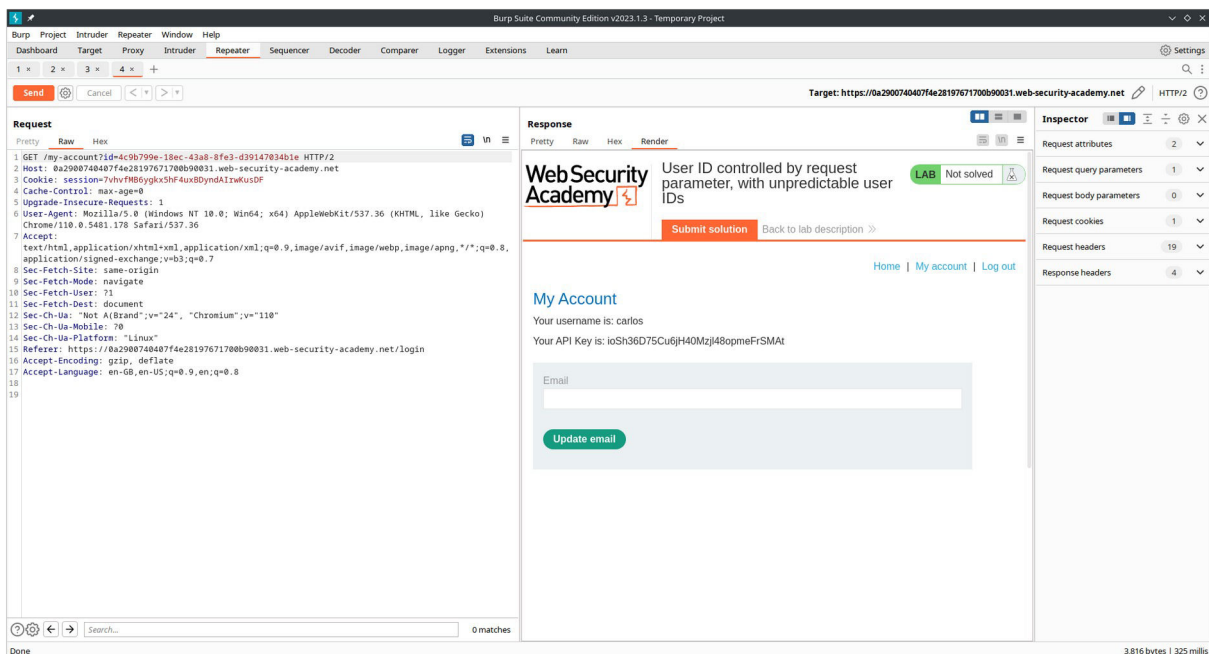
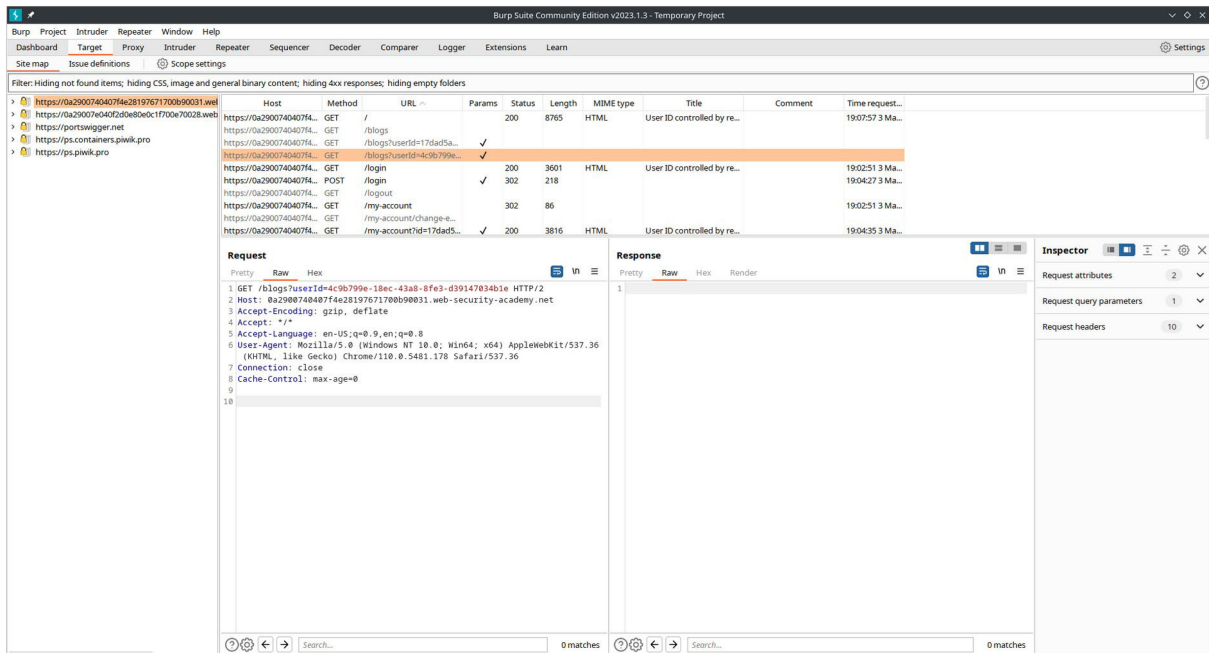
Lab: User role controlled by request parameter

Open the burpsuite and turn on the intercept in the proxy. Login in with the given credentials and check the request in the target tab. Now forward the my-account request to the repeater and change the id to wiener. Send the modified request and the admin panel will be displayed and now you will be able to delete the user carlos.



Lab: User ID controlled by request parameter, with unpredictable user Ids

Open the burpsuite and turn on the intercept in the proxy. Check for any post by the user carlos so that we can manage to get the id of him. Click a post by him and store request to fetch his id. Now login with the given credentials and forward this request to the repeater. We can change the value of the id from the id that we identified from carlos post request. Send the modified request and the admin panel will be displayed and now you will be able to delete the user carlos.



Lab: User ID controlled by request parameter with password disclosure React js gen_key func

Open the burpsuite and turn on the intercept in the proxy. Login in the given credentials and you will have your password store in the my account section. Forward this request to repeater and modify the id to administrator. Send the modified request and the admin panel will be displayed and now you will be able to delete the user carlos.

The screenshot shows the Burp Suite interface with the 'Site map' tab selected. A list of intercepted requests is displayed. The selected request is a GET to `/my-account?id=wienner` with a status of 200. The response is a web page titled 'My Account' with a form to update email. The form has fields for 'Email' and 'Password' and a 'Update email' button. The page also shows the username 'wienner'.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is being modified in the 'Request' tab. The 'Response' tab shows the resulting HTML output, which is a 'My Account' page. The page shows the username 'administrator' and a form to update email. The form has fields for 'Email' and 'Password' and a 'Update email' button. The page also shows the username 'administrator'.

User ID controlled by request parameter with password disclosure

LAB Not solved

WebSecurity Academy

User ID controlled by request parameter with password disclosure

Back to lab description >>

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

Login

Username

administrator

Password

Log in

User ID controlled by request parameter with password disclosure

LAB Not solved

WebSecurity Academy

User ID controlled by request parameter with password disclosure

Back to lab description >>

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

Users

wiener - [Delete](#)

carlos - [Delete](#)