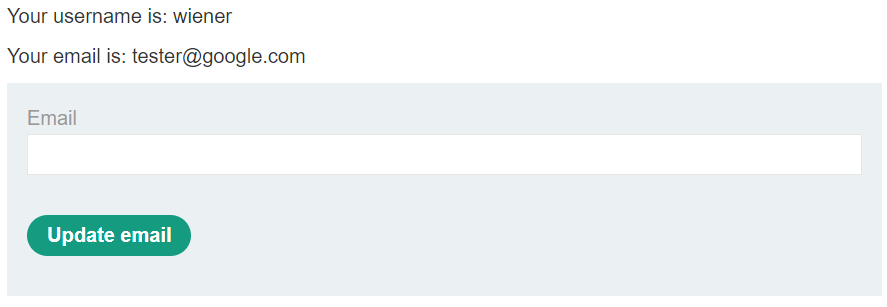
**WEEK 6:**

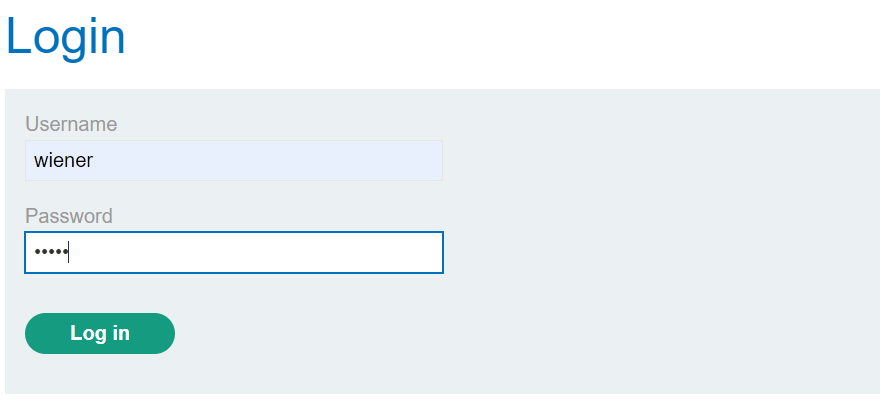
**Cross-Site Request Forgery (CSRF)**

1. **CSRF vulnerability with no defenses**

****

* To solve the lab, craft some HTML that uses a CSRF attack to change the viewer’s email address and upload it to your exploit server.
* You can log in to your account using the following credentials: wiener: peter login into wiener: peter, intercept the update mail request go in engagement tool and generate csrf, make sure u change the email, click copy HTML and paste it into exploit server, store it and deliver it to victim to solve the lab.

1. **CSRF where token is not tied to user session**

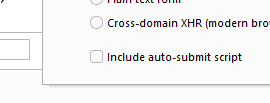
****

* You have two accounts on the application that you can use to help design your attack. The credentials are as follows:

wiener: peter  
carlos: montoya

* Intercept the update mail request send it to the repeater drop the request into the engagement tool and generate csrf, make sure u change the email, click copy HTML paste it into the exploit server, store it, and deliver it to the victim to solve the lab.

1. **CSRF where token is tied to non-session cookie**



* Use your exploit server to host an HTML page that uses a CSRF attack to change the viewer’s email address.
* You have two accounts on the application that you can use to help design your attack. The credentials are as follows:
* Wiener: peter  
  carlos: montoya
* Intercept the update mail request send it to a repeater and drop the request go into the engagement tool generate csrf go into the options button unclick Include auto-submit script regenerate and copy the HTML and paste it into the exploit server and now paste

**IDOR (Insecure Direct Object Reference)**

* **Solve the lab by finding the password for the user carlos, and logging into their account.**
* **T**he GET request which is the area inside the red rectangular is a request to download a file. According to the request I can download 2.txt which consists of my texting transactions. 2.txt is a parameter that changes with each request and increments by one with every new request.
* So, the value of a parameter is used directly to retrieve a file.

