BASICS

Deliverable for this lab: take two screenshots. Screenshot 1: registered user on Juiceshop. screenshot 2: Burp Suite screen that shows you intercepted the request to juiceshop.

1.1 Accounts

Create accounts on:

- Github.com
- Heroku.com
- Runkit.com (you can login with your github account)
- Netlify.com
- https://portswigger.net/web-security/dashboard

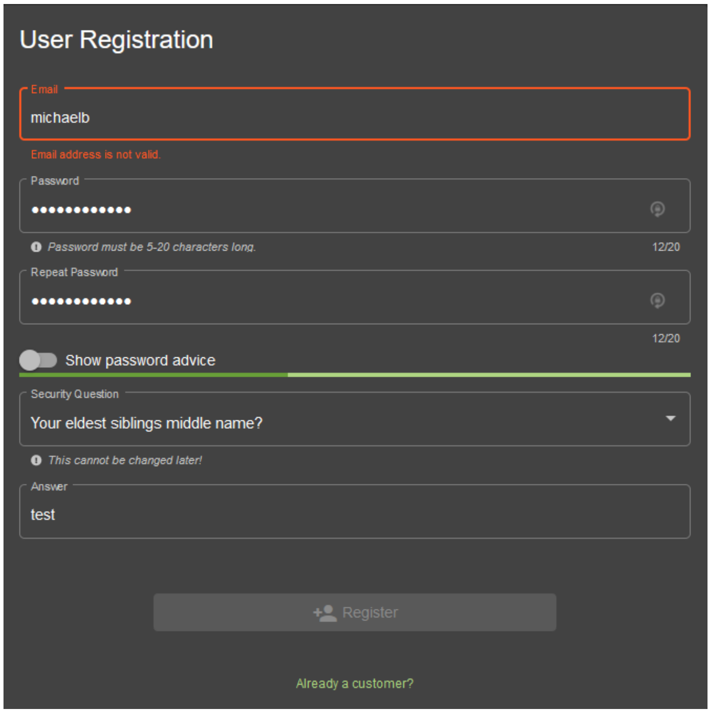
1.2 Burp suite: getting started

Through this exercise you will start to get to know Burp Suite as a proxy to intercept and alter requests. This is a skill that you will need throughout the course.

Install Burp Suite (https://portswigger.net/burp/communitydownload) and watch https://portswigger.net/burp/documentation/desktop/tutorials/intercepting-http as an introduction to Burp Suite.

1.3 Burp suite: first exercise

Go to http://juiceshop-websec.herokuapp.com . This is a vulnerable web application that was deployed for this class. The challenge is to bypass the Javascript validation checks and register with a username that is **NOT** an email address as shown in the below image. Can you succeed in registering?



User Registration

Email: michaelb

Email address is not valid.

Password: ●●●●●●●●●●●●

Password must be 5-20 characters long. 12/20

Repeat Password: ●●●●●●●●●●●●

12/20

Security Question: Your eldest siblings middle name?

This cannot be changed later!

Answer: test

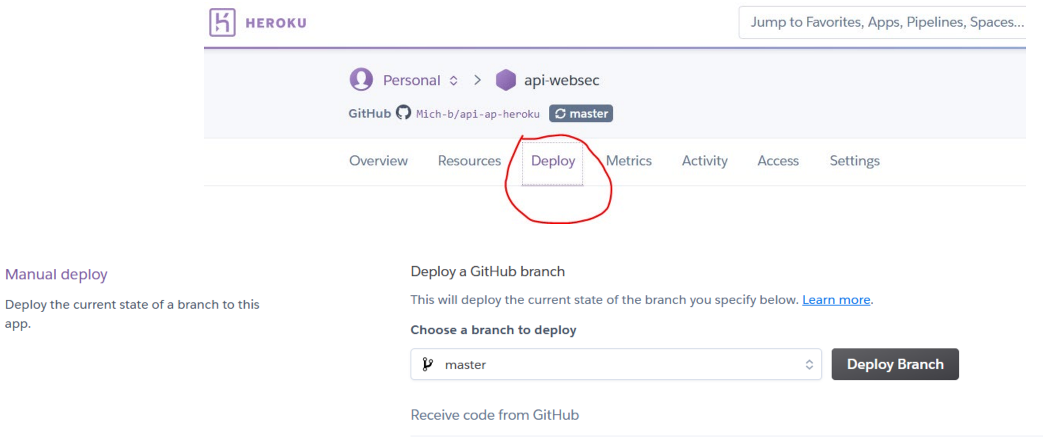
1.4 Heroku deployments from Github

Through this exercise you will deploy a simple REST API that you will need during the exercise about the Same Origin Policy.

Fork the repository https://github.com/Mich-b/api-ap-heroku.

In your forked repository (Github.com => my repositories), go to the api-ap-heroku repository and click ‘deploy to heroku’. You should now have an API that returns a simple string ‘This API works’.

Get familiar with how you can easily redeploy an application on Heroku by clicking the ‘Deploy branch’ button in the Deploy menu after changing the text ‘This API works’ to ‘I modified this API’ in your Github repository (api-ap-heroku/blob/master/index.js):



Deploy the current state of a branch to this app.

Deploy a GitHub branch

This will deploy the current state of the branch you specify below. Learn more.

Choose a branch to deploy: master