# ISEC 400 Lab 1

For this assignment, you will be discovering vulnerabilities in software using an example system that was written in NodeJS. Although the source code language may not be familiar, the concepts and vulnerabilities in the study of application security are the same. This exercise will use JuiceShop, an application specifically designed to be vulnerable.

## Getting started

You have a few options for playing around with JuiceShop. For pointers and details on the JuiceShop app, view <https://pwning.owasp-juice.shop/> guide that will help you out. The different ways you can access JuiceShop are as follows:

1. **Your own personal version of Heroku (recommended)** [This lab is to create your own]
2. Visit the main Heroku hosted version: <https://juice-shop.herokuapp.com/>
3. Use NetLab (instructions below)
4. Download and run it yourself (not recommended)
   * <https://owasp.org/www-project-juice-shop/>
   * <https://bkimminich.gitbooks.io/pwning-owasp-juice-shop/content/part1/running.html>
   * <https://github.com/bkimminich/juice-shop>

To access this application is via Franklin University’s NetLab system.

1. Visit <https://netlab.franklin.edu> and login with the credentials that were sent to you by your instructor
2. There are three virtual machined available that you can tab through to access.
   1. **A Kali Linux system** with a graphical user interface from which you can use a web browser to access the web-based JuiceShop application and launch your attacks. Kali Linux is preconfigured with tools that can help you to discover vulnerabilities in this application. User is “isec-student” and password is “isec-student”. The IP of this machine is 10.0.2.3.
   2. **A pfSense system** that acts as a firewall between the Kali Linux system and JuiceShop lab. It is configured to allow all traffic through and port forward 3000 to the Ubuntu server. Its WAN is configured to be on the 10.0.2.0 network, it has an IP of 10.0.2.2 on this network and acts as a gateway for the LAN network 10.0.0.0, of which its IP is 10.0.0.1. pfSense is useful if you want to see what traffic logs look like when you’re running your attacks.
   3. **An Ubuntu Server** that acts as the host for the JuiceShop application, which is running the NodeJS app on port 3000. The gateway for this machine is the pfSense box, so this machine has an internal IP of 10.0.0.5. The username and password for this system are the same as the Kali system, you have sudo capabilities, but there is no uplink to the internet.
3. To access the pfSense web-based graphical administration site, you can open a browser on the Kali system and navigate to <http://10.0.2.2> and login with the username “admin” and password “isec-student”.   
     
   **Note:** To fix a temporary misconfiguration in the lab system, login to that web interface, click the dropdown menu (hamburger menu) in the top right and navigate to Firewall 🡪 NAT. You will see a port forwarding rule for 10.0.0.2, edit this and change it to 10.0.0.5. The topology in the lab also errantly shows the IP as 10.0.0.2 instead of 10.0.0.5. This will be fixed in the future.
4. To access the JuiceShop application you would open a web browser on the Kali system and navigate to <http://10.0.2.2:3000> to access the NodeJS app. This functions like a normal web application would, so play around.

## Complete the following lessons

To get started for the future labs, you will deploy your own personal Heroku version of JucieShop.

1. Create a free Heroku account via <https://signup.heroku.com/> using your Franklin University email address.
2. Go to the JuiceShop GitHub page and scroll down to the “Setup” section of the ReadMe and choose “Deploy to Heroku” button after you are logged into the account you just created.
3. Using the JuiceShop guide linked in the getting started section of this document, find the ScoreBoard on your personal JuiceShop setup. Include a screenshot in your lab submissions.
4. After reading about the JuiceShop project’s purpose, write a 1-page review on how why you think the software is helpful for Information Security analysts.

## Submission instructions

Create a Word document for your submission that includes the URL of your persona Heroku version of JuiceShop as well as a screenshot of your browser open to the ScoreBoard that you found and the write-up. Submit the Word document to the dropbox for Lab 01.

Looking into the JuiceShop project, I can say that it seems to be incredibly helpful, especially for those who are just starting out with security. The purpose is to help go through different vulnerabilities in a manner that is easy to follow along with and understand. The scoreboard is split up into multiple challenges that work through the vulnerabilities a person may find in software security and rewards people with a score and completion percentage to make the tutorials more game like and play off the need for completion some people have.

Prior to this lab, I have gone through the JuiceShop before and stand by my initial thoughts that this would be very useful to work through and can be beneficial to our schooling and even future work. The OWASP project site even states that it is a sophisticated insecure web application, so it is a safe way of learning about vulnerabilities and security.

The scoreboard that we see is a great idea as it lays out different challenges a person can do and gives them instructions on how it works. Taking the score as the person goes through helps give them an incentive to complete challenges and learn more about security.

A screenshot of a computer

Description automatically generated with medium confidence

Citation:

*Owasp Juice Shop*. OWASP Juice Shop | OWASP Foundation. (n.d.). Retrieved February 12, 2023, from [https://owasp.org/www-project-juice-shop/#](https://owasp.org/www-project-juice-shop/)

*Owasp Juice Shop*. OWASP Juice Shop. (n.d.). Retrieved February 12, 2023, from <https://demo.owasp-juice.shop/#/score-board>