# ISEC 400 Lab 2

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/>

* **Your own personal version of Heroku (recommended)**
* Visit the main Heroku hosted version: <https://juice-shop.herokuapp.com/>
* Use NetLab (instructions below)
* 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

1. Using the “PWNING OWASP JUICE SHOP” book as your guide choose one challenge from the **“Broken Authentication”** area (pg. 96 for a list of these options, section 3.4) and complete it. Then, pick one challenge from the **“Broken Access Control”** area (pg. 113 for a list of these options, section 3.8) and also complete that. The book will guide you through these, depending on the challenges you choose you may have to:
   1. View the source of documents in order to look for form elements
   2. Employ the “console” view of a browser (such as the Web Developer toolbar [generally F11 key shortcut]) and modify values that are being submitted in forms. Note that in Chrome, you can search for elements such as “form” or “option” by pressing Ctrl-F in the console window in Elements view.
2. Explain the challenges you chose, what you did for each challenge (take a screen shots along the way to paste it into your solution document) and create a write-up about your experience. Using screenshots here is recommended. A recommended free-for-personal-use screen capture tool is PicPick (<http://www.picpick.org/en/download_free>). This will let you capture just a region of your screen and easily paste the results.

## Submission instructions

Create a properly cited Word and formatted document for your submission that includes the steps you took to complete the challenges you chose, with screenshots along the way for each significant moment of finding. Submit the Word document to the dropbox for the lab.

<https://3000-juiceshop-juiceshop-1zq4xwm666r.ws-us90.gitpod.io>

The challenge I chose for the broken authentication is the reset password for Bjoern’s OWASP account with the forgot password mechanism and the truthful answer to his security question as it is quite interesting to see how our careless posts to social media can come back to bite us.

We start by going to the forgot password and providing the [bjoern@owasp.org](mailto:bjoern@owasp.org) email as we know we are changing the owasp account. It then shows the security question so we can head to bjoern’s twitter. After twitter forced me to login, I clicked on the media option and scrolled until I found a post where Bjoern tells the name of the cat. I can now use the cat’s name Zaya and change the password. I quite enjoyed this as it was fast and I could see a picture of a cute cat.

Graphical user interface

Description automatically generated

The challenge for broken access control I chose was the view basket as it sounded interesting and made me think of when you are at the store and you look over and you see a person buying a crazy combination of items.

We start by logging in as any user so I will use the user prior as we just changed the password. We then add any items into the cart so I chose 5 random items that caught my eye. I then went to the devtools and went to application, session storage and found the bid and the value 6 which I changed to 5 then I clicked onto the basket. This was a fun little challenge to do and I can see why juiceshop is so popular. I never went far into devtools but after this I may look into it more.

A screenshot of a computer

Description automatically generated

Citation:

Juiceshop. (n.d.). Retrieved March 12, 2023, from <https://juiceshop-juiceshop-1zq4xwm666r.ws-us90.gitpod.io/>

Kimminich, B. (n.d.). *Challenge solutions*. Challenge solutions · Pwning OWASP Juice Shop. Retrieved March 12, 2023, from <https://pwning.owasp-juice.shop/appendix/solutions.html#access-the-administration-section-of-the-store>