# ISEC 400 Lab 4

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.

## Complete the following lessons

1. Using the “PWNING OWASP JUICE SHOP” book as your **guide choose two additional challenges you haven’t completed yet** and complete them. It is okay if they are related to other challenges you have completed. 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.

The first challenge I chose was weird crypto as it looks at the shop and informs it about an algorithm or library not being used the way it is supposed to. The challenge involves forging a coupon code that gives a discount which is something that I find quite interesting as this is something that could be harmful for small businesses. The second one I chose was forged coupon which is creating the coupon that weird crypto mentions so that means I am going to start with the coupon forging then lead into the weird crypto.

Forges Coupon:

To start we are taking note of an old coupon that was acquired in another challenge, access a salesman’s forgotten backup file, so we do not have to go through the entire process. The old coupon we see is coupons\_2013.md.bak with the Gc7sn pattern being the amount of discount. From the Juiceshop twitter account we can find the code; k#pDmgC7vo that is valid until the 30th of April this year. Now looking at the active code we can separate is into the two parts, k#pDm which is the activated part, and gC7vo which is the discount. Now we can go ahead and login using the login from previous lab, [bjoern@owasp.org](mailto:bjoern@owasp.org) and the ‘— added to it so anything can be in the password spot. Now that we are logged in, we start to add to our cart. We can quickly run through adding in an address with whatever and choosing whatever for the delivery and we arrive at my payment options. A screenshot of a computer

Description automatically generated

We can find out through the dependencies in the package.json.bak that the code is converted using zeromq base-85 encoding. This means we can check the code from twitter to see what it actually says. By installing the node z85 package we can do a quick run to see that it stands for APR23-20 if we switch out the ending vo with sn we get APR23-10 so we know that the percentage is altered in this area. The -d is used to decrypt so we can enter APR23-80 to get the code for 80% off.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

This took me some time to figure out, but it was quite fun to work out once I understood what to do.

Now we can move back to weird crypto as we now know the crypto problem there is as we just went through it. On the weird crypto challenge, we can click the link and be sent to a send feedback box which we can fill out now know that it uses base85 and z85. Luckily, we are still logged in and bjoern so we can fill out the feedback with the buzzwords base85 and z85 and finish this task.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

After working through the first problem this one was a quick and easy one to do as we were already logged in and had the necessary words that we learned. I think it would be harder if I did them in the order I chose them but overall, it was a fun lab and I plan to play more with juice shop on my own.