Bookstore

Introduction

* First to find some of the information we would need to scan the IP of the Bookstore
* Then it will show us what ports are running and the website of it.

Website

* We will visit the website by using the port number .
* Once we visited the website we can see it is a Rest API meaning we can just look for the API direct in the website.
* After looking around the Rest API for information we can then explore the actual Bookstore page.
* The most interesting place to look at the bookstore website would be the login page.
* We would probably do the inspect tool incase there is anything interesting.

Console

* So what we found that there is something with the debugger and pin for a console.
* Means that there probably a problem which will allows us to get the pin for the console.
* Looking through the assets of the js since one of the message did something about it.
* In the Js script it says something about the previous API version being vulnerable so we will use that to our advantage.
* So we would go back to using the IP and port but put the API version to 1 of the bash history instead of the present version.
* And we would find the debug pin for the console which we will enter into the console pin to gain access.

Import and User

* Now we have the console for us to access so we need to figure out how to connect our terminal with console on the website
* Since the console is able to use netcat we can connect it by using netcat listener in the terminal by using port 4444,
* The terminal commands I used for the Netcat would be on github Payload
* We now have a copy of shell to be technical reverse shell which allow us to find the User and Root Flag.
* Though now we just ‘ls’ in the command and use the command ‘cat user.txt’ which will give us the Flag of the User.

Root Flag

* For the root flag could not grab the flag of it since we need a “Magic Number” to bypass the security.
* We now probably need to use another program to reverse engineer to find the code
* Though I was not able to do that because of technical problems with the VPN for Kali and Attackbox was being buggy.