Kristen Trunnelle

IST 590

May 29, 2018

For this week’s lab I immediately noticed that all three of the vm’s had id=userid# in the url link when clicked on each one, both on the client and the staff side. While the staff side shows Testy McTesterson and Lazy Lazyman (Fired for Stealing) on all three browsers under the staff login, Testy McTesterson’s last name includes (NOT PUBLIC UNTIL SEPT. 1) on the green browser unlike the other two, I didn’t know if this was a vulnerability or not but soon found the other first vulnerability. I saw how the id=# was visible under the staff menu for salespeople, users, and countries with the id=10 or 11 showing Lazy’s and Testy’s info on the staff menu sites but on the public sites was where the vulnerability was found. On the red browser, under salespeople when I clicked them and changed the id= from 1-9 it shows the 9 salespeople and when I typed in id=10 or id=11 since the blue and green browsers didn’t have any salesperson for that number it took me right back to the central page showing all the salespeople. On the red browser however, it allowed me to type id=10 to show me Testy Testerson’s name, phone number and email address along with Lazy Lazyman (Fired for Stealing)’s information when I typed in id=11 as well which is an IDOR vulnerability that is not supposed to be available to the public to see.

Since I saw the name of the users on the accounts I hit the logout button on each browser and tried typing in a user name (of a given user) for username and a wrong password, a wrong username and password, both fields blank, pperson and a wrong password, and a username for a user that exists on the websites with the StaR!49\*whiz password hoping and thinking I could catch a user enumeration vulnerability, but none worked. I thought I would get an error message telling me incorrect password or username for a right password or username but none. The only error messages were that it was an unsuccessful login and that neither field could be left blank. In the LICEcap video, though I did get a message saying my account would lock and I would be unable to login for 5 minutes, I still kept trying passwords and usernames and the times dropped from 5 minutes to 2 minutes and on 2 minutes I put in the correct username and password and I was surprised it let me as the account should have remained locked the full 5 minutes.

For the username and password boxes I also tried using a sql / to escape the username box and try a password along with a or 1 = 1 statement trying to see if the login was where a sql injection flaw would be, but that didn’t work for me either. I looked under inspect on each browser for the logins to see if I could notice anything. I saw some method=post and changed to get, changed hidden to text and inserted a value=”admin” to try to see if I could get in as that was what I did to get some CTF’s but none of those worked. I looked under the cookies under application to see the phpsessionid but nothing looked out of place to me. I tried putting the phpsessionid value and other values from under elements under inspect into a bsae64 decoder but got nothing. I noticed how I could submit feedback on the browsers and my comments would appear, that I could edit and change features under users, salespeople, and countries and create new values for those sections but did not know or wasn’t able to figure out any other vulnerabilities despite looking at the sites for hours. I also tried using jmonroe99 as the username in the login boxes as the hint page mentioned using that user to get a vulnerability, but I got nothing. I even tried changing pperson (Patty’s username) to jmonroe99 but it wouldn’t let me make a username since that already existed. I felt like the hints were not that useful to me, that I needed more guidance and hints to find more vulnerabilities. I did not even recognize the IDOR vulnerability at first. I initially thought CTF flag signs would appear if caught a vulnerability.

So since I only got one vulnerability, the only concept review question I can answer is:

Which attacks were easiest to execute? Which were the most difficult? The IDOR was the easiest and only obvious one to me as each page where could click a user, salesperson, or country on both the client and staff side would show the id= at the top and could be changed.