Hours spent: 3
Blue:
Vulnerability #1: SQL Injection -Desc: I changed the URL, from 1 at the end to ‘ and it was able vulnerable to an attack

#Vulnerability #2: Session Hijacking -Desc: this one did not work on my computer,

Green:
Vulnerability #1: Enumeration -Desc: When a username is correct, but the password isn't, "log in was unsuccessful" is displayed in bold. This could help the hacker determine which are real usernames and which are fake!

Vulnerability #2: Stored XSS -Desc I inserted the alert “barbara found the xss” into the feedback in contact us. After logging in and clicking on feedback it should have shown the alert “barbara found the xss”

Red
Vulnerability #1: IDOR -Desc: I went to the sales persons. I changed the id and tried all the numbers until i got to people who were not featured at first.

Vulnerability #2: CSRF -Desc:I created a html called form.html where I had it change the first name to alabama and last name to city and number to 123 for the 3rd salesperson

Challenges: computer display is limited so couldn’t the vm to load blue 2