Mike Kowalczyk

Code path 480 assignment week 9

BLUE:

The two vulnerabilities in the blue target were session hijacking and SQL injection.

Session Hijacking: I had to add hacktools/change\_session\_id.php to get the answer for this oneGraphical user interface, application, Word

Description automatically generatedGraphical user interface, application, Word

Description automatically generated

SQL: This one I added id=' OR SLEEP(5)=0--'

In order to get the site to load for 5 seconds before bringing me there

Graphical user interface, application, Word

Description automatically generated

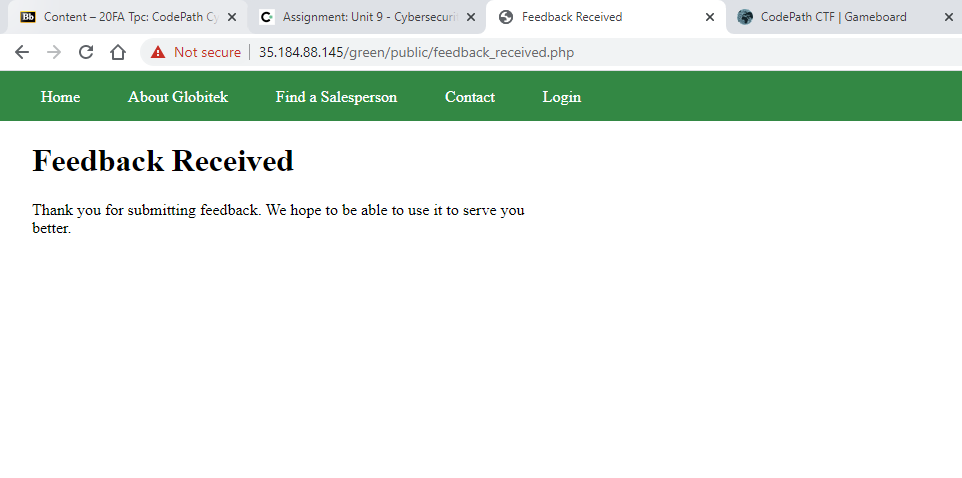
GREEN: Green had cross-site scripting (xss) and Username Enumeration

Username Enumeration: the failed scripts were different from a username that exists and one that does not Graphical user interface, application, Word

Description automatically generatedGraphical user interface, application, Word

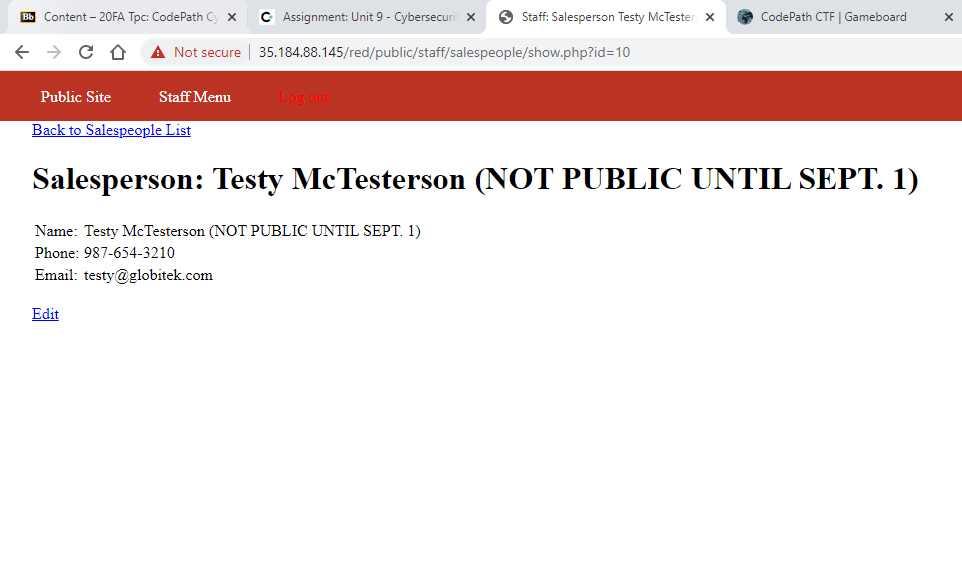
Description automatically generated

Cross-site scripting (xss): I had to put that script in the feedback section for it to give me alerts when someone logs in and checks the feedback tab



RED: Red had IDOR and CSRF

IDOR: I changed the id at the end to 10



CSRF: I was able to change pattttttt Bizarrd when I had an html file opened that was scripted to change the first and last names of the salesman clicked on.