Hanah Deering

2-2 Activity: SQL Injection Coding

CS 405: Secure Coding

Southern New Hampshire University

A screenshot of a computer

Description automatically generated with medium confidence

At first, I was a little bit intimidated with the code files provided because I was quite unsure what was being asked to be implemented, which essentially made this project a little bit more difficult for me. I was able to use an amazing resource (w3resource.com) which gave me a better overall picture of exactly what SQL Injection is. Since SQL Injection can bypass a firewall, some ways in which SQL statements are injected, in turn making systems vulnerable, are through:

1. Injected through user input
2. Injected through cookies contains attack strings
3. Injected through Server Variables

The process I implemented was to display an error if there is a suspected SQL Injection. You will either get a pass or fail. After many fail-run attemps, I used std::regex numInjection(" or [1-9]+=[1-9]+;"); and std::regex wordInjection(" or '[a-zA-Z]+'='[a-zA-Z]+';"); and everything finally ran! An error message will be displayed if there is an injection detect. With the final run attempt, everything passed!