Project 3: Website Hacking

In this project we will be using pen testing techniques to break or manipulate the following website: lucy.mscs.mu.edu. The type of pen testing used will be considered a White Box attack because we, the pen testers, have complete access to the source code. In addition, we know that sql injection, cookie manipulation, and admin access will be allowed to attack the site.

Information leak? ( error message including hints about how to attack )

Banner grabbing? ( Find what webserver is being used. Vulnerabilities may be present current operating system )

This website seems to be very vulnerable to snooping. Using the Wireshark, http requests are seen publicly. This is a major vulnerability when the user is submitting sensitive information. For example, an order on lucy.mscs.mu.edu could be exploited, like a person’s credit card information, address, or name.

Administrative pages also expose vulnerabilities for this website. Appending “/admin” to certain URL pages allows admin access to be established. This allows for significant data manipulation. For example, prices can be changed, and product names can be changed.