CYBR 3510 "Systems Security"

SQL Injection

1. Modify the /root/index.php file so that the web application displays “Welcome to my web server”. (1 point)

A screenshot of a computer

Description automatically generated

1. Open the phpMyAdmin and login using the root account. (1 point) A screenshot of a computer

   Description automatically generated
2. Create a new table name as “login\_details” under the “test” database and set three column names as “login\_ID”, “username”, and “password”. (set the type of username and password as text and set the login\_ID as the primary key) (1 point)

A screenshot of a computer

Description automatically generated

1. Insert several records into the login\_details table so that we have several username and password pairs in our database. (1 point)

A screenshot of a computer

Description automatically generated

1. Edit the index.php file so that the web application can get connected to the “test” database. (1 point)

A screenshot of a computer

Description automatically generated

1. Edit the index.php file, so that we have a form to allow us to input username and password information with a submit button. (1 point)

A screenshot of a computer

Description automatically generated

1. Link the submit button to the database so that if we enter a valid username and password, it will return the result that indicate a successful login. (1 point)

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

1. Try the invalid user name or password and observe the returned result. (1 point)

A screenshot of a computer

Description automatically generated

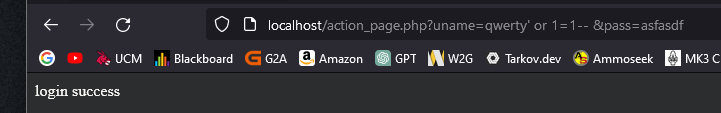
1. Try the most basic SQL injections using ‘ or 1=1 -- . (1 point)

A screenshot of a computer

Description automatically generatedA screenshot of a video game

Description automatically generated

1. If the get function is used to receive the username and password, can we directly inject malicious code in the URL and success? (1 point)



1. Change the get function to the post function, then repeat the step 8~10 and summarize the results. (3 points)

A screenshot of a computer

Description automatically generated

You can get the same outcome without the input shown in the URL

1. Using the addslashes() function after the post function. Now if we try to use ‘ or 1=1-- to launch the SQL injection, can we succeed? Why? (2 points) A screenshot of a phone

   Description automatically generated

It no longer works because the input will be seen as a single string and not execute the code