Beau Goldberg

MART 461

Test Plan

In order to test my website for SQL Injection attacks and Cross Scripting Attacks the following tests can be made

* Input text in each text bar using html tags and see if it is handled correctly. Either an error should result due to html code in the text or it will encode the text to display the html instead of processing it.
* Add on true statements to the query to see if they can be broken into and fiddled with. If the statements are all handled as stored procedures than there should be no issue in this as all of the inputted data will be seen as a parameter and not be attached to the rest of the string.
* Use incorrect characters and formats when entering data to see if it is handled properly. If handled properly it will show an invalid format error. If it doesn’t it could potentially throw an error page that may reveal information for the hacker.
* Reach an error page to see if there is a general error message page or if the errors are being handled by the system. Having the errors completely handled by the system will allow for some information that may not want to be shown to be found.

We haven’t discussed some of the other attacks that can take place so this is about all I can think of to test against the issues we’ve discussed.