**Lesson 2.3 – Server Exploits**

**\*\*Instructions:** Please change the text color of your responses to red text. Please organize the endings to each page.

**Activity 2.3.1 – Securing Ecommerce Data**

1. Explain what you see when the page loads in the browser and tie each observed behavior to the corresponding line of code. (Step #5)
2. What do you think would happen if you load this web page in a browser, enter the name jdoe, and click the button? (Step #6-C)
3. What do you think would happen if you click the button without entering a name? (Step #6-D)
4. Double-click the file HelloWorldButton.html to render the HTML in the web browser. Did it behave the way you thought it would? (Step #7)
5. Document the XSS reflected exploit script and then describe what you observed. (Step #14)
   1. Save a screenshot of the result.
6. Document the XSS reflected exploit script and then describe what you observed. (Step #15)
   1. Save a screenshot of the result.
7. Describe what you observed with security set back to High. (Step #17)
8. Select/highlight the few lines of code that prevent the XSS reflected exploit (but not the entire script) and save a screenshot of the script. (Step #20)
9. Predict what columns (categories of data) are in the users table. (Step #26)
10. Document this first SQL injection exploit code and then describe what you observed. (Step #29)
    1. Save a screenshot of the result.
11. Observe the results after the first authentic result (where user\_id is 1). Document the second SQL injection exploit code and then describe what you observe. (Step #30)
    1. Save a screenshot of the first page of the results.
12. Document the third SQL injection exploit code and describe what you observe. (Step #31)
    1. Save a screenshot of the result
13. Describe what you observe when you set the site security level to High. (Step #33)
14. Select/highlight the few lines of code that prevent the SQL injection exploit (but not the entire script) and take a screenshot of the script. (Step #36)

**COMPLETE OPTIONAL EXTENSION: RESEARCH**

1. XSS
   1. How often does it occur today?
   2. What are some XSS exploits and ramifications that companies have experienced in recent years?
2. SQL Injection
   1. How often does it occur today?
   2. What are some SQL Injection exploits and ramifications that companies have experienced in recent years?

**CONCLUSION**

1. How can you apply the security measures presented in this activity to the Bikes, Boards, and Beyond website?
2. Data cleansing is a common protection measure that companies implement today. Do you think it’s acceptable to try out some XSS and SQL Injections for fun thinking it won’t harm anyone? Explain your thinking.