# CYB 240 Module Three Lab Worksheet

Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

## Lab: SQL Injections (SQLi)

| **Prompt** | **Response** |
| --- | --- |
| In the lab section “Analysis of the Vulnerability,” **Step 20**, insert your name at the command line below the output and include it in your screenshot. |  |
| In the lab, we demonstrated the dangers of unsecured input and how it can lead to SQLi. The lab also demonstrated how escaping can be used to mitigate an SQLi password bypass attack. Explain the steps of escaping and why it was successful in mitigating the SQL injection attack. | Escaping worked because it added backslashes before special characters like quotes, turning harmful input into harmless text. This prevented the SQL query from being manipulated and stopped the login bypass. |

## Lab: Performing SQL Injection to Manipulate Tables in a Database

| **Prompt** | **Response** |
| --- | --- |
| In the lab section “Stealing Data and Creating a Backdoor,” **Step 7**, insert your last name as the user that is created. Also use the name in Step 8. Take a screenshot after Step 8. |  |
| Metasploit is an open source free tool that is shipped with Kali Linux. The tool can also be added to other distributions of Linux. How can this tool be used by security analysts to help secure computer systems that they are responsible for maintaining? | Metasploit is a great user-friendly tool that can be used for a variety of purposes in security. For example, by brute-forcing sql, we can see if our systems administrative controls, as well as firewalls are properly configured. Password strength (while simple) is very important as well! |

## Lab: Session Stealing (Stored XSS)

| **Prompt** | **Response** |
| --- | --- |
| In the lab section “Alice Gets Owned,” **Step 12**, insert your name in the comment field and then take a screenshot of the dialog. |  |
| In the lab, you learn to exploit stored XSS. What steps can be taken on a form that would prevent the ability of a stored XSS to execute, and how should they be implemented? | There are numerous ways to implement prevention methods against XSS exploitation. One of them is by using Content Security Policy (CSP). CSP tells our browser which scripts, styles, and resources are safe to load, blocking anything unexpected or malicious. |