# Lab #5 – Assessment Worksheet

## Attacking a Vulnerable Web Application and Database

**Course Name and Number:** ______________________________________________

**Student Name:** ________________________________________________________

**Instructor Name:** ______________________________________________________

**Lab Due Date:** ________________________________________________________

### *Overview*

In this lab, you used the Damn Vulnerable Web Application (DVWA), a tool specifically designed with common vulnerabilities to help Web developers test their own applications prior to release. As an ethical hacker, you found and exploited a cross-site scripting (XSS) vulnerability and conducted a SQL injection attack on the Web application's SQL database. You made your attacks using a Web browser and some simple command strings. You documented your findings throughout the lab.

### *Lab Assessment Questions & Answers*

1. Why is it critical to perform a penetration test on a Web application and a Web server prior to production implementation?

2. What is a cross-site scripting attack? Explain in your own words.

3. What is a reflective cross-site scripting attack?

4. Based on the tests you performed in this lab, which Web application attack is more likely to extract privacy data elements out of a database?

5. If you can monitor when SQL injections are performed on an SQL database, what would you recommend as a security countermeasure to monitor your production SQL databases?

6. Given that Apache and Internet Information Services (IIS) are the two most popular Web application servers for Linux and Microsoft® Windows platforms, what would you do to identify known software vulnerabilities and exploits?

7. What can you do to ensure that your organization incorporates penetration testing and Web application testing as part of its implementation procedures?

8. What is the purpose of setting the DVWA security level to “low” before beginning the remaining lab steps?

9. As an ethical hacker, once you’ve determined that a database is injectable, what should you do with that information?