

Lab #8 – Assessment Worksheet

Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you performed simple tests to verify a cross-site scripting (XSS) exploit and an SQL injection attack using the Damn Vulnerable Web Application (DVWA), a tool left intentionally vulnerable to aid security professionals in learning about Web security. You used a Web browser and some simple command strings to identify the IP target host and its known vulnerabilities, and then attacked the Web application and Web server using cross-site scripting (XSS) and SQL injection to exploit the sample Web application running on that server.

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. Which Web application attack is more likely to extract privacy data elements out of a database?
5. What security countermeasures could be used to monitor your production SQL databases against injection attacks?

2 | Lab #8: Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities

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

7. Who is responsible for the CIA of production Web applications and Web servers?