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?
   Performing a penetration test allows one working in the field to check to see if there are any vulnerabilities in the web application and server, then patch them to reduce the risk on launch.

2. What is a cross-site scripting attack? Explain in your own words.
   A cross site scripting attack attempts to use web forms to execute third party code. This allows an attacker to force a web application to operate outside of norms, and potentially gain access to data they should not have access to.

3. What is a reflective cross-site scripting attack?
   A reflective XSS attack bounces the attack off a web server to make a trusted user execute the script from within a trusted environment.

4. Which Web application attack is more likely to extract privacy data elements out of a database?
   An SQL injection attack is more likely to extract private data, although it may take a number of attempts to successfully pull it off.

5. What security countermeasures could be used to monitor your production SQL databases against injection attacks?
   You should implement regex rules and other configuration to prevent execution of injected sql code, and restrict access to certain tables based on credentials. Also, it’s probably a good idea to use a user and password on a MySQL database that isn’t root, root. Just sayin’.
6. What can you do to ensure that your organization incorporates penetration testing and Web application testing as part of its implementation procedures?
   If you are in a position of management, you can implement policies for your development staff and employees involved in projects that security should be a major part of the process. If you are not, discussions with supervisors or generally fostering a culture of security and responsibility could make a useful contribution.

7. Who is responsible for the CIA of production Web applications and Web servers?
   IS personnel are primarily responsible for confidentially, integrity, and availability concerns during production, while the end users must work to preserve the security built in once the system is live.