Assessment Worksheet

Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities

Student Name: Ndaw, Maam Awa

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?
   It is critical to perform a penetration testing on a Web application and a Web server prior to production implementation because it is a critical step to ensure confidentiality, integrity, and availability of the Web application and service.

2. What is a cross-site scripting attack? Explain in your own words.
   A cross-site scripting is a form of preventable web attack using arbitrary HTML or JavaScript code through a Web application for testing and security in order to reduce the likelihood of exposure attack.

3. What is a reflective cross-site scripting attack?
A reflective cross-site scripting attack refers to when an attacker attempts to use scripting commands in the URL itself, or through a device, such as a Web form, to gain administrator, or some other elevated level of user privileges in an attempt to force the victim’s server to display the desired data on-screen.

4. Which Web application attack is more likely to extract privacy data elements out of a database? SQL injection attacks are used to extract privacy data elements out of a database by inserting real SQL query commands into Web forms.

5. What security countermeasures could be used to monitor your production SQL databases against injection attacks?

Security countermeasures that could be used to monitor the production SQL databases against injection attacks include encrypting the data elements that reside in long-term storage of the SQL database. Database Administrators should also monitor SQL databases for unauthorized or abnormal SQL injections and write scripts that send off alarms as well as sending network management alerts.

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

To ensure that an organization incorporates penetration testing and Web application testing as part of its implementation procedures, the company’s security policy should dictate that no production web application, whether residing inside or outside of the firewall, be implemented without proper penetration testing and security hardening.

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

Web application developers and software developers are responsible for the secure coding and testing, which includes penetration testing of web applications and web servers, a critical step in ensuring the Confidentiality, integrity, and availability of the Web application and service.