Software and Web application developers are responsible for secure coding and testing of their application. Database developers and administrators are responsible for data integrity and ensuring backups of the database are performed regularly. Still, network and system engineers and information systems security professionals also can help ensure Web application security through regular penetration testing.

Any form of testing, particularly penetration testing, on Web applications and Web servers is a critical step in ensuring the confidentiality, integrity, and availability (CIA) of the Web application or service. If e-commerce or privacy data is entered into the Web application, the company is bound by compliance laws and standards to ensure the confidentiality of customer data. Penetration testing should be performed whenever the Web application or service is updated or modified. The organization’s security policy should dictate that no production Web application can be implemented without proper penetration testing and security hardening. This is especially critical if your Web application requires customers to input private data.

Commercially available tools and Web sites are available to help secure your environment regardless of the platform. For instance, the CVE listing database (<http://cve.mitre.org/cve/cve.html>) contains abundant information about common software vulnerabilities and exploits. As a developer using an Apache Web Servers, you could serch the CVE listing using the keyword *Apache* to find all known Apache vulnerabilities and exploits. With this information in hand, you can include all software patches and security patches on your production Web servers to remediate critical and major software vulnerabilities before the application is released.

Ethical hacking is attacking a secure system with the purpose of uncovering vulnerabilities for its owner. An ethical hacker recommends specific countermeasures for remediating the vulnerabilities and eliminating the exploits. In this lab, you will be using 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 will find and exploit a cross-site scripting (XSS) vulnerability and conduct a SQL injection attack on the Web application’s SQL database. You will make your attacks using a Web browser and some simple command strings.

Learning Objectives

1. Identify Web application and Web server backend database vulnerabilities as viable attack vectors.
2. Develop an attack plan to compromise and exploit a Web site using cross-site scripting (XSS) against sample vulnerable Web applications
3. Perform a manual cross-site scripting (XSS) attack against sample vulnerable Web applications
4. Perform SQL injection attacks against sample vulnerable Web applications with E-commerce data entry fields.

The goal of an XSS attack is usually to gain administrator or some other elevated level of user privileges.

The Cross-site Scripting (XSS) is the malicious inserting of scripting code to extract data or modify a Web site’s code, application or content. Non-persistent XSS vulnerabilities are the most common, usually targeted via poisoned URL links sent to users. Persistent XSS vulnerabilities are a more serious variety where data has been saved to the server and can modify how applications or services operate. A reflective cross-site scripting attack is a non-persistent attack in which all input shows output on the user’s/attacker’s screen and does not modify data stored on the server.