Web Application Penetration Testing Methodology

3 Hr 30 Min Remaining

Instructions Resources Help  100%

Module 08: Web Application Penetration Testing Methodology

Objective

The objective of this lab is to provide expert knowledge of web application vulnerabilities and web applications attacks such as:

* SQL Injection
* Parameter tampering
* Cross-Site Scripting (XSS)
* Dictionary Attacks
* Shell Upload
* Directory Traversal

Scenario

A web application is an application that is accessed by users over a network such as the Internet or an intranet. The term may also mean a computer software application that is coded in a browser-supported programming language (such as JavaScript, combined with a browser-rendered markup language like HTML) and reliant on a common web browser to render the application executable.

Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as a client. The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity, as is the inherent support for cross-platform compatibility. Common web applications include webmail, online retail sales, online auctions, wikis and many other functions.

Web hacking refers to exploitation of applications via HTTP which can be done by manipulating the application via its graphical web interface, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI. Methods that can be used to hack web applications are SQL Injection attacks, Cross Site Scripting (XSS), Cross Site Request Forgeries (CSRF), Insecure Communications, etc.

As an expert *Penetration Tester* and *Security Administrator*, you need to test web applications for cross-site scripting vulnerabilities, cookie hijacking, command injection attacks, file upload vulnerabilities, etc. and secure web applications from such attacks.