# Chapter 56
# Web Application Vulnerabilities and Their Countermeasures

**Kannan Balasubramanian**
*Mepco Schlenk Engineering College, India*

## ABSTRACT

*The obvious risks to a security breach are that unauthorized individuals: 1) can gain access to restricted information and 2) may be able to escalate their privileges in order to compromise the application and the entire application environment. The areas that can be compromised include user and system administration accounts. In this chapter we identify the major classes of web application vulnerabilities, gives some examples of actual vulnerabilities found in real-life web application audits, and describes some countermeasures for those vulnerabilities. The classes are: 1) authentication 2) session management 3) access control 4) input validation 5) redirects and forwards 6) injection flaws 7) unauthorized view of data 8) error handling 9) cross-site scripting 10) security misconfigurations and 10) denial of service.*

## INTRODUCTION

A web application is broken up into several components. These components are a web server, the application content that resides on the web server, and typically there a backend data store that the application accesses and interfaces with. This is a description of a very basic application. Most of the examples in this chapter will be based on this model. No matter how complex a Web application architecture is, i.e. if there is a high availability reverse proxy architecture with replicated databases on the backend, application firewalls, etc., the basic components are the same.

The following components makeup the web application architecture:

- The Web Server;
- The Application Content;
- The Datastore.

DOI: 10.4018/978-1-5225-3422-8.ch056

Just as there are components to a web application architecture, there are software components in more complex Web applications. The following components make up a basic application that has multi-user, multi-role functionality. Most complex web applications contain some or all of these components:

- Login;
- Session Tracking Mechanism;
- User Permissions Enforcement;
- Role Level Enforcement;
- Data Access;
- Application Logic;
- Logout.

## SECURING WEB SERVICES

In this section we discuss how to secure Web servers, services, and application (Cross, et al., 2007). The problems associated with Web-based exploitation can affect a wide array of users, including end users surfing Web sites, using Instant Messaging (IM), and shopping online. End users can also have many problems with their Web browsers.

The following issues are covered in this section:

- How to recognize possible vulnerabilities;
- How to securely surf the Web;
- How to shop and conduct financial transactions online safely.

This chapter looks at File Transfer Protocol (FTP)-based services. FTP has long been a standard to transfer files across the Internet, using either a Web browser or an FTP client. Because of the highly exploitable nature of FTP, this chapter looks at why it is insecure, how it can be exploited, and how to secure it. We will also look at a number of other methods for transferring files, such as Secure FTP (S/FTP) and H SCP. While FTP remains a common method of transferring files on the Internet, SCP has superseded it as a preferred method among security professionals for transferring files securely.

The last section deals with Lightweight Directory Access Protocol (LDAP), its inherent security vulnerabilities, and how it can be secured. In this section we address many of the issues with LDAP, and look at how it is used in Active Directory, directory, and other directory services. By exploring these issues, you will have a good understanding of the services and Internet technologies that are utilized in network environments.

## WEB SECURITY

When considering Web-based security for a network, knowledge of the entire Internet and the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack is a must. This chapter looks at Web-based security and topics including server and browser security, exploits, Web technologies such as ActiveX, JavaScript, and CGI, and much more.