CHAPTER 2

Before Starting

To follow the steps in this guide, you'll need access to an ACE Web Application Firewall and Manager installation. This guide provides an overview of how to install the appliance on your network. For complete information on installing the ACE Web Application Firewall and Manager, see the *Cisco ACE Web Application Firewall Administration Guide*. The following sections describe what you'll need in order to perform the appliance set up and other policy configuration steps described in this guide.

Set Up Requirements

Before you can start configuring a web application security policy, the ACE Web Application Firewall appliance needs to be installed on your network, as described in Chapter 3, "Performing the Initial Setup." To perform this task, you will need the following information:

- The IP address of the default IP gateway for the network
- The IP address of the primary DNS server for the network
- A hostname for the ACE Web Application Firewall registered with the local network's DNS server (recommended)
- The password for the root account on the ACE Web Application Firewall appliance

  If this is a new installation and you do not know the root password, please contact your support representative.
- A static IP address for the ACE Web Application Firewall appliance

  You only need one IP address to run the ACE Web Application Firewall and Manager on a single appliance chassis (the configuration described in this guide). However, you will need two IP addresses to run the Manager and Firewall on separate appliances.

Tools for Generating Traffic

Configuring and testing the policy as described in this guide requires several third-party tools. After you configure the ACE Web Application Firewall, you'll want to send test requests to it. You can use your preferred web browser to send the requests described in this book.

Several examples involve HTTP cookie editing. To edit cookies, you can use the "Add N Edit Cookies" add-on for Firefox (https://addons.mozilla.org/en-US/firefox/addon/573). For Internet Explorer, tools such as IECookiesView (http://www.nirsoft.net/utils/internet_explorer_cookies_view.html) or CookieEditor (http://www.proxoft.com/CookieEditor.asp) are available.

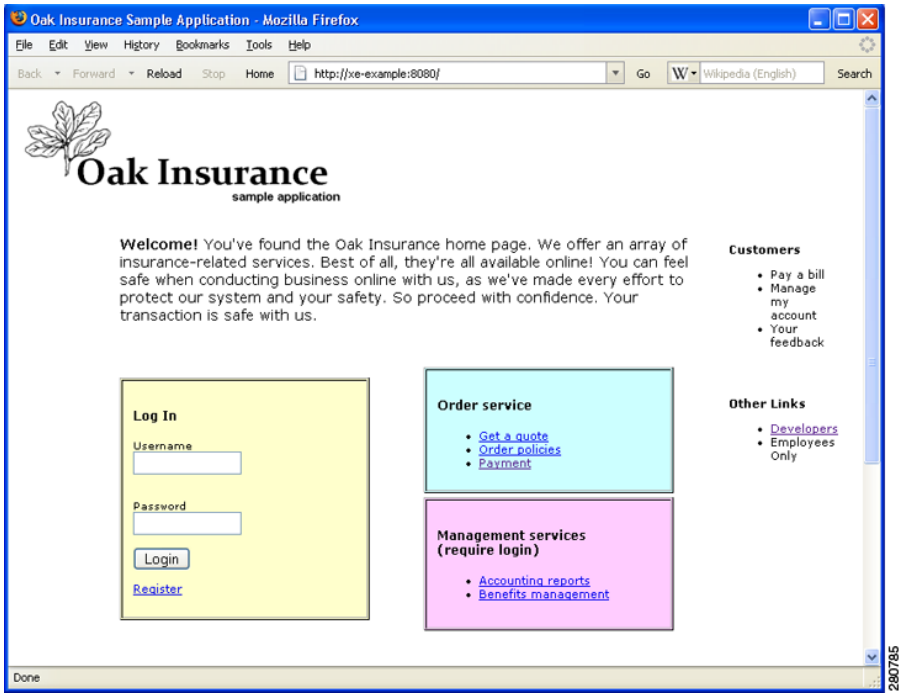
You'll also need a tool that allows you to view HTTP headers. The examples in this book use the Live HTTP Headers add-on for Firefox. For Internet Explorer, the Fiddler tool is available from Microsoft (http://www.fiddlertool.com/fiddler/).

About the Sample Application

This guide describes how to configure the ACE Web Application Firewall for a particular backend application. The sample application used in this guide (Figure 2-1) is the web portal for a fictional insurance company, Poison Oak Insurance Company. The application is designed for Poison Oak's customers, partners, and internal employees. For instance, customers can use the application to request an insurance quote, submit an order, or pay a bill. Employees can retrieve business accounting reports or benefits information.

Unfortunately for Poison Oak's imaginary users, the web application is riddled with security vulnerabilities, including vulnerabilities to buffer overflow, SQL injection, and cross-site scripting attack. The vulnerabilities are used in this guide to demonstrate the capabilities of the ACE Web Application Firewall. Following the steps in this guide, you will configure the ACE Web Application Firewall to secure the Poison Oak web application and its users.

Figure 2-1 The Poison Oak Insurance home page



If you have access to the Poison Oak sample application, you will be able to follow the steps described in this guide closely. However, you can also follow these steps with your own application or using an application that, like the Poison Oak Sample application, is intended to demonstrate web vulnerabilities, several of which are available on the web.