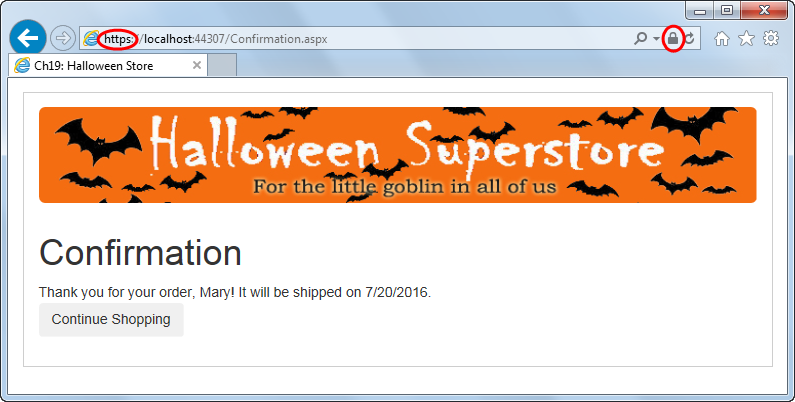
Extra 19-1 Add security to the Halloween Store application

In this exercise, you’ll add the security to the Halloween Store application that’s presented in the book.



Open and test the web application

1. Open the XEx19HalloweenStore web application in your exercises\_extra directory.
2. Test the application to see how it works. Be sure to test all of the buttons on each page that go to another page.

Secure the web application

1. Enable SSL for the web application, and then note the URLs that can be used to access the web application using both a secure and an unsecure connection.
2. Add two add elements to the appSettings element of the Web.config file. The first one should have a key of “SecurePath” and a value of the secure URL. The second one should have a key of “UnsecurePath” and a value of the unsecure URL. (See Slide 11)
3. Modify the Order page so it doesn’t post back to the CheckOut1 page when the Check Out button is clicked.   
     
   Then, add a using directive to the code-behind file for the page for the SystemConfiguration namespace.   
     
   Finally, code an event handler for the Click event of the Check Out button that displays the CheckOut1 page with a secure connection. Do the same for the Cart page. (See Slide 12)
4. Modify the event handlers for the Click event of the Cancel Order buttons on the CheckOut1 and CheckOut2 pages so they display the Order page with an unsecure connection. (See Slide 13)
5. Modify the Continue Shopping buttons on the CheckOut1 and CheckOut2 pages so they don’t post back to the Order page. Then, code event handlers for the Click event of these buttons that display the Order page with an unsecure connection. Do the same for the Return to Order Page button on the Confirmation page. (See Slide 13)
6. Add code at the beginning of the Load event handler for the CheckOut1 page that checks if the page is secure. If the page isn’t secure, it should be redirected to a secure page. Do the same for the CheckOut2 page. (See Slide 15)
7. Test the application again. When it tries to enter a secure connection, it will display a page indicating that there’s a problem with the certificate. Click the “Continue to this website” link to display the secure page.

Note: If you’ve chosen to trust a self-signed certificate generated by IIS Express as described in figure 19-3, you won’t see this error page in Internet Explorer. In that case, the web application will function just as if it has a digital secure certificate issued by a certification authority (CA). However, you probably *will* still see an error page or some kind of warning in other browsers.

1. Continue through all of the pages to place an order, and notice which pages use a secure connection and which pages don’t.