SearchSecurity.com
Security School

Developer's active content delivery checklist

By Michael Cobb

Make sure your Web developers follow these rules when creating dynamic content for your IIS server.

- **Specify a character set at the start of each page.**

- **Filter and encode all form data.**

Developers should read the CERT advisory on malicious HTML tags at http://www.cert.org/advisories/CA-2000-02.html, and then review the following Microsoft Knowledge Base articles:

  - Q252985 How to prevent cross-site scripting security issues
  - Q253119 How to review ASP code for CSSI vulnerability

- **Filter and encode all cookie data.**

Values read from cookies should be treated as untrusted input data, and filtered and encoded as in step two. Never store sensitive data in persistent cookies.

- **Use SSL for sending and receiving any sensitive data.**

Passwords, credit card details and any personally-identifiable information should be transmitted only over an SSL connection.

- **Disable IE's Autocomplete feature for password fields.**

Add the AUTOCOMPLETE=OFF attribute to either the <FORM> or <INPUT> tag of any forms that are used for requesting passwords. For example:

```
<INPUT TYPE=password NAME=Password SIZE=16 MAXLENGTH= 16
AUTOCOMPLETE=OFF>
```

- **Disconnect sessions when inactive for five minutes.**

By default, the Connection Timeout value for IIS is set to 900 seconds. Change this value to 300 seconds using the Internet Services Manager. Alternatively, if users have logged onto your site, add the following code to the top of each page:

```
<SCRIPT Language="JavaScript">
<!--
window.setTimeout("window.navigate('Logoff.asp')", 300000);
//--></SCRIPT>
```

Users will be sent to the Logoff.asp page after five minutes if they just sit on a page.

- **Remove all comments from code.**

Good developers provide well-commented code, but comments should be removed on pages that are loaded on the production server because they can provide possible clues to an attacker in the event of a security breach.

- **Use a COM+ component to store database connection information.**

Many developers store database connection information in the global.asa file. This information contains the server name, database name, database login and password, so it must be protected. Read Architecting the solution at msdn.microsoft.com for further information on how to use a COM+ component.

- **Use stored procedures to access a database.**

Stored procedures provide better access control over data and a performance advantage over SQL statements.