This is a design checklist – things you should keep in mind while developing websites.

## User inputs

| Check | Description |
|---|---|
| | User inputs are checked for type, length and content. |
| | User inputs with arithmetic operations are checked and validated for minimum and maximum values. |
| | All user inputs are validated on server side as well as on client side. |
| | Values stored in hidden form fields are validated properly. |

## Attack prevention

| Check | Description |
|---|---|
| **Cross-site scripting** | |
| | User inputs are escaped and validated. |
| | Content is encoded before it is rendered on a page. |
| | Strings from external sources are encoded using the HTMLHelper.HTMLEncode() method. |
| | URL parameters are sanitized using the QueryHelper.GetText() method. |
| | Values from external sources rendered as part of JavaScript code are encoded using CMS.Base.Web.UI.ScriptHelper.GetString(). |
| | Cookies are configured as http-only. |
| **SQL injection** | |
| | SQL parameters are used for dynamic parts of SELECT, INSERT, UPDATE and DELETE queries. |
| | The exec() function is not used in SQL code. |
| **Cross-site request forgery** | |
| | Actions are performed using POST requests, not GET. |
| | View state mac validation is enabled globally in the web.config file.<br>`<pages enableViewStateMac="true" />` |
| **LDAP injection** | |
| | User inputs for LDAP queries are sanitized before execution. |
| **Unvalidated redirects and forwards** | |
| | Any custom redirects to URLs obtained from untrusted inputs are performed using the URLHelper.LocalRedirect method, or are validated using the URLHelper.IsLocalUrl method. |

## Other issues

| Check | Description |
|---|---|
| | User accounts are secured against all types of attacks. |
| | Error messages in the UI are configured so that they show only basic information and the whole information is logged only into the Event log. |
| **File upload** | |
| | Name, length, type and content of files is checked upon file upload. |
| **Logging** | |
| | All critical activities in the website are logged. |
| | The website does not allow unhandled exceptions to occur. |