This is a security deployment checklist – things to do before you deploy your site to a live environment.

Web.config:

Check	Description	Details
	The debug mode is turned off to prevent sensitive information leakage.	Web.config file settings
	Tracing is disabled to prevent sensitive information leakage.	Web.config file settings
	The error messages of websites and application-server default error messages are not displayed in details to users.	Designing secure error messages
	Sensitive sections of the web.config file are encrypted (mainly the connection string).	How To: Encrypt Configuration Sections in ASP.NET 2.0 Using DPAPI
	Access to sensitive directories is forbidden to protect the servers against the enumeration attack.	Enumeration
	Cookieless authentication is disabled to prevent session hijacking. This can be done by changing the cookieless attribute of the form element.	Session protection
	The *HttpOnlyCookies* flag is set so that the cookies are accessible only from the server-side code (this behavior is set by default in Kentico).	Web.config file settings

IIS:

Check	Description	Details
	Directory listing is disabled in the website and web servers.	Export/import package directory browsing
	All HTTP methods except GET and POST are disabled if they are not in use.	Securing the Staging and REST web services
	Scripts and 3rd party libraries are up-to-date. If external libraries (e.g. for database access, XML parsing) are used, always use the current versions.	
	Sensitive links which should not be indexed by search engines are listed within robots.txt files.	Managing robots.txt
	The execution of scripts is disabled on folders where it is undesirable.	Edit Feature Permissions for the Handler Mappings Feature (IIS 7)

Kentico:

Check	Description	Details
	All test user accounts are deleted or disabled.	
	All unnecessary modules and applications are disabled.	Disabling unnecessary modules and services and keeping the system up-to-date
	All unnecessary pages are deleted.	
	File types that can be uploaded to the system are restricted. You can specify which extensions are allowed for uploaded files in general, including forms in *Settings -> System -> Files* in the *Security* category.	

	UI personalization for specified roles is set correctly to prevent users from accessing unnecessary user interface. You can configure UI personalization in the *UI personalization* application.	UI Personalization
	Permissions for specified actions in Kentico modules are set correctly for all roles. You can configure permissions in the *Permissions* application.	Configuring permissions securely
	Users are allowed to use only strong and complex passwords. You can enable the Use password policy setting in *Settings -> Security & Membership -> Passwords*.	Password strength policy and its enforcement
	Passwords are stored in a strong and secure format. The recommended option is PBKDF2. You can set the password format in Settings -> Security & Membership -> Passwords -> Password format.	Setting the user password format
	The number of allowed invalid sign-in attempts is limited. You can set the limit in *Settings -> Security & Membership -> Protection* in the *Invalid sign-in attempts* category.	Invalid sign-in attempts
	You have consider if autocomplete function is needed. Autocomplete can be enabled in *Settings -> Security & Membership -> Protection* in the *General* category.	Autocomplete deactivation
	Forms are secured with CAPTCHA (spam protection control).	Spam protection (CAPTCHA)
	Encrypted Internet connection (HTTPS) is configured properly.	Configuring SSL