You should always try to hide the information about the server and operating system you are using. When the attackers are not able to determine this information, it is much more difficult for them to find flaws in the system and exploit them.

If attackers discover a flaw in a certain technology (IIS, ASP.NET, or Kentico), they could utilize this flaw to attack a large number of web servers with the same configuration.

Fingerprinting

Fingerprinting are techniques, that allow attackers to learn the exact version of web servers by querying the servers and analyzing their responses. Since the different versions of web servers have different implementations, they respond to special queries in different ways.

The same applies for content management systems. By analyzing the input code and the files located on the server, the attacker can figure out the type of CMS running on the server and its version.

The problem is, that you can never completely conceal the details about your system.

Server banners

The servers send greeting messages, called banners, with information about the server versions and used technologies. The servers send these messages in HTTP headers (in respond to fingerprinting queries) and you can also find them in page footers of directory listings.

Best practice is to hide as much information as you can. See the procedures in this article: Configuring HTTP Response Headers in IIS 7.

Information about Kentico

Unfortunately, it is not possible to completely hide the fact that the server uses ASP.NET framework and the application running on it is Kentico. All you can do at the moment is:

- Forbid access to the administration interface. You can set this by adding the *CMSDisableAdministrationInterface* key in the **<appSettings>** section of web.config file:

  ```
  <add key="CMSDisableAdministrationInterface" value="true"/>
  ```

- Not to display information that the website was built using Kentico in the page footers.