### 

* Open **IIS Manager**
* Click your **server name**
* Go to **“Modules”**
* **Remove anything not used**, such as:  
  + WebDAV Publishing
  + CGI (if you're not running CGI scripts)
  + Request Filtering (if not used)
  + FTP Publishing if not serving FTP

* Select your website → **Directory Browsing**
* **Disable** (right-hand panel)

**Turn off debug mode** + enable custom error pages.

Web.config:

<configuration>

<system.web>

<customErrors mode="RemoteOnly" />

<compilation debug="false" />

</system.web>

</configuration>

# **6) Web.config Exposure**

If misconfigured, IIS may serve web.config as plain text → **critical leak**.

### **Fix**

This is normally protected by default. Never change handler mappings for .config.  
 If using reverse proxies, ensure:

web.config

appsettings.json

.env

are **deny-access** in the reverse proxy config too.

Set Application Pool Identity to:

ApplicationPoolIdentity

instead of:

LocalSystem or Administrator (DANGEROUS)

Check:  
 **IIS Manager → Application Pools → Right click pool → Advanced Settings → Identity**

# **9) Outdated IIS + Windows Updates**

Many IIS compromises come from unpatched servers.

### **Fix**

Enable:

Windows Update → Automatic → Security-Only

Also check:

Server Manager → Dashboard → Notifcations → Critical Updates