IIS and ModSecurity

# Notes & References

The following list of IIS status subcodes is taken from Microsoft, at <http://support.microsoft.com/kb/943891>, they apply to IIS 7.0, 7.5, and 8.0.

* 400 Bad Request
* 400.1 - Invalid Destination Header
* 400.2 - Invalid Depth Header
* 400.3 - Invalid If Header
* 400.4 - Invalid Overwrite Header
* 400.5 - Invalid Translate Header
* 400.6 - Invalid Request Body
* 400.7 - Invalid Content Length
* 400.8 - Invalid Timeout
* 400.9 - Invalid Lock Token
* 401 Unauthorized
* 401.1 - Logon failed
* 401.2 - Logon failed due to server configuration
* 401.3 - Unauthorized due to ACL on resource
* 401.4 - Authorization failed by filter
* 401.5 - Authorization failed by ISAPI/CGI application
* 403 Forbidden
* 403.1 - Execute access forbidden
* 403.2 - Read access forbidden
* 403.3 - Write access forbidden
* 403.4 - SSL required
* 403.5 - SSL 128 required
* 403.6 - IP address rejected
* 403.7 - Client certificate required
* 403.8 - Site access denied
* 403.9 - Forbidden: Too many clients are trying to connect to the web server
* 403.10 - Forbidden: web server is configured to deny Execute access
* 403.11 - Forbidden: Password has been changed
* 403.12 - Mapper denied access
* 403.13 - Client certificate revoked
* 403.14 - Directory listing denied
* 403.15 - Forbidden: Client access licenses have exceeded limits on the web server
* 403.16 - Client certificate is untrusted or invalid
* 403.17 - Client certificate has expired or is not yet valid
* 403.18 - Cannot execute requested URL in the current application pool
* 403.19 - Cannot execute CGI applications for the client in this application pool
* 403.20 - Forbidden: Passport logon failed
* 403.21 - Forbidden: Source access denied
* 403.22 - Forbidden: Infinite depth is denied
* 403.502 - Forbidden: Too many requests from the same client IP; Dynamic IP Restriction limit reached
* 404 Not Found
* 404.0 - Not found
* 404.1 - Site Not Found
* 404.2 - ISAPI or CGI restriction
* 404.3 - MIME type restriction
* 404.4 - No handler configured
* 404.5 - Denied by request filtering configuration
* 404.6 - Verb denied
* 404.7 - File extension denied
* 404.8 - Hidden namespace
* 404.9 - File attribute hidden
* 404.10 - Request header too long
* 404.11 - Request contains double escape sequence
* 404.12 - Request contains high-bit characters
* 404.13 - Content length too large
* 404.14 - Request URL too long
* 404.15 - Query string too long
* 404.16 - DAV request sent to the static file handler
* 404.17 - Dynamic content mapped to the static file handler via a wildcard MIME mapping
* 404.18 - Querystring sequence denied
* 404.19 - Denied by filtering rule
* 404.20 - Too Many URL Segments
* 500 Internal Server Error
* 500.0 - Module or ISAPI error occurred
* 500.11 - Application is shutting down on the web server
* 500.12 - Application is busy restarting on the web server
* 500.13 - Web server is too busy
* 500.15 - Direct requests for Global.asax are not allowed
* 500.19 - Configuration data is invalid
* 500.21 - Module not recognize
* 500.22 - An ASP.NET httpModules configuration does not apply in Managed Pipeline mode
* 500.23 - An ASP.NET httpHandlers configuration does not apply in Managed Pipeline mode
* 500.24 - An ASP.NET impersonation configuration does not apply in Managed Pipeline mode
* 500.50 - A rewrite error occurred during RQ\_BEGIN\_REQUEST notification handling. A configuration or inbound rule execution error occurred
* 500.51 - A rewrite error occurred during GL\_PRE\_BEGIN\_REQUEST notification handling. A global configuration or global rule execution error occurred
* 500.52 - A rewrite error occurred during RQ\_SEND\_RESPONSE notification handling. An outbound rule execution occurred
* 500.53 - A rewrite error occurred during RQ\_RELEASE\_REQUEST\_STATE notification handling. An outbound rule execution error occurred. The rule is configured to be executed before the output user cache gets updated
* 500.100 - Internal ASP error
* 502 Bad Gateway
* 502.1 - CGI application timeout
* 502.2 - Bad gateway: Premature Exit
* 502.3 - Bad Gateway: Forwarder Connection Error (ARR)
* 502.4 - Bad Gateway: No Server (ARR)
* 503 Service Unavailable
* 503.0 - Application pool unavailable
* 503.2 - Concurrent request limit exceeded
* 503.3 - ASP.NET queue full

Exercises

1. Determine the appcmd.exe syntax to add a new web site from the command line by running the command

C:\Windows\System32\inetsrv>appcmd.exe add site /?

Add a new web site with appcmd.exe.

1. Use OpenSSL on a Kali system to connect to a Windows server running the remote management service (TCP/8172 by default). What is the server's public certificate? How long is the server's private key? Can you communicate with the service? What happens if you visit that server in a browser?
2. Use the tool SSLyze to analyze the SSL configuration of an IIS server. The tool is available for download from <https://github.com/nabla-c0d3/sslyze>.
3. Consider an IIS installation with multiple web sites. Configure ModSecurity so that it only analyzes traffic to/from one web site. Hint: read the README file that comes with ModSecurity for IIS.
4. Add an FTP server to an existing IIS installation. Create an FTP site that allows for anonymous read (but not write) access. A reasonable location for the physical path is C:\inetpub\ftproot. Test the site.