IIS 8 SERVER HARDENING HANDBOOK

Table of Contents

1. Executive Summary

1.1 Introduction

This document is a security hardening guide for the Microsoft IIS 8 Server. It summarizes a checklist of the configuration settings that constitute a secure server to safeguard against potential hackers and crackers. It provides contextual descriptions of each checklist item along with details of what the setting means and possible values followed by recommended mitigating strategies. The recommendations are intended to provide helpful information to administrators attempting to evaluate or improve the security of their systems. Proper use of the recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” solutions for securing server’s operating system. For server specific recommendations a Vulnerability Assessment on the server is required.

Recognition

The following resources were referred during the development of this guide.

1. Security Configuration Benchmark for CIS Microsoft IIS 8 Benchmark, released by The Centre for Internet Security (CIS)

2. Basic Configurationx

Title	2.1 Disable IIS Default Web Site
Description	The Default virtual directories and default permissions exist on the Default Web Site.
Risk Rating	High

Impact: The case for keeping the Default Web site is that a time might arise when you need the online documentation.The best way to avoid this potential security hole is to place all your content in a new \wwwroot folder outside \inetpub (and off the system drive).

Solution: It is recommended to implement the below setting:

1. Open IIS Manager
2. In the Connections pane expand the Sites node and select Default Web Site
3. In the Actions pane click stop in Manage Website
4. Then click Application Pool list and select the "DefaultAppPool"
5. In the Actions pane click stop in Application Pool Tasks
6. Restart IIS.

X

Title	2.2Disable Web Content and Script directories access
Description	Web resource published through IIS are mapped, via Virtual Directories, to physical locations or disk.
Risk Rating	High

Impact: Excessive permission for the anonymous web user account contributes to the compromise of a web server.

Solution: It is recommended to implement the below setting:

1. Browse to web content in C:\inetpub\wwwroot\
2. Copy or cut content onto a dedicated and restricted web folder on a non-system drive such as D:\webroot\

3. Change mappings for any applications or Virtual Directories to reflect the new location

X

Title	2.3Host Headers
Description	Host Headers provide the ability to host multiple websites on the same IP address and port. It is recommended that host headers be configured for all sites.
Risk Rating	High

Impact: DNS rebinding attacks can compromising or abusing site data or functionality.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager
2. In the Connections pane expand the Sites node and select Default Web Site
3. In the Actions pane click Bindings
4. In the Site Bindings dialog box, select the binding for which host headers are going to be configured, Port 80 in this example
5. Click Edit
6. Under host name, enter the sites FQDN, such as *<www.examplesite.com>*
7. Click OK, then Close

Note: Requiring a host header may impair site functionality for HTTP/1.0 clients.

Title	2.4Directory Browsing
Description	Directory browsing allows the contents of a directory to be displayed upon request from a web client.
Risk Rating	High

Impact: An attacker can exploit Directory Browsing feature to access unauthorized files through directory traversal.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager

2. In the Connections pane expand the Sites node and select Web Site
3. Click Directory Browsing icon in IIS (Feature View)
4. In the Actions pane click Disable to disable Directory Browsing

Title	2.5Application Pool Identity
Description	Application Pool Identities are the actual users/authorities that will run the worker process.
Risk Rating	High

Impact: Creating a custom identity for each application pool will better track issues occurring within each web-sites.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager
2. In the Connections pane, expand the Server node and Click Application Pools
3. Highlight an Application Pool to review and in the Connection pane click Advanced Setting
4. Scroll down to the Process Model section and set the value for Identity to ApplicationPoolIdentity, Network Service or a custom identity with rights and privileges equal to or less than the built-in-security principal.
5. Restart IIS.

Title	2.6Application Pools
Description	Application pools isolate sites and applications to address reliability, availability, and security issues. Sites and applications may be grouped according to configurations, although each site will be associated with a unique application pool.
Risk Rating	High

Impact: Assigning resource-intensive applications to their own application pools improves server and application performance.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager
2. Open the Sites node underneath the machine node
3. Select the Site to be changed
4. In the Actions pane, select Advanced Settings
5. Click the Select… box next to the Application Pool text box
6. Select the desired Application Pool
7. Once selected, click OK

Title	2.7Ensure Application Pools Run Under Unique Identities
Description	Application Pool Identities are the actual users/authorities that will run the worker process - w3wp.exe.Assigning the correct user authority will help ensure that applications can function properly, while not giving overly permissive permissions on the system.
Risk Rating	High

Impact: Setting Application Pools to use unique identities reduces the potential harm the identity could cause should the application become compromised.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager
2. Open the Application Pools node underneath the machine node
3. Create new and then select Application Pool that have been created
4. Right click the Application Pool and select Advanced Settings…
5. Under the Process Model section, locate the Identity option and ensure that ApplicationPoolIdentity is set

Note: Setting the Application Pools to run under the ApplicationPoolIdentity will ensure that each pool runs under a unique authority.

Title	2.8Anonymous User Identity
Description	IIS can be configured to automatically use the application pool identity if no anonymous user account is configured for a Web site.
Risk Rating	High

Impact: Configuring the anonymous user identity to use the application pool identity will help site isolation.

Solution: It is recommended to implement the below setting:

1. Open the IIS Manager GUI and navigate to the desired server, site, or application
2. In Features View, find and double-click the Authentication icon
3. Select the Anonymous Authentication option and in the Actions pane select Edit
4. Choose Application pool identity in the modal window and then press the OK button

X

Title	2.9Webserver TLS Version
Description	IIS can be configured to automatically use the application pool identity if no anonymous user account is configured for a Web site.
Risk Rating	High

Impact: An attacker can intercepted clear text sensitive information over the network.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager
2. Open the Sites node underneath the machine node
3. Double click the SSL icon
4. Click the Require SSL and Require SSL 128-Bit check boxes.

Enable the TLS 1.2 protocol on R2, ensure the following key is set to 0.

HKLM/System/CurrentControlSet/Control\SecurityProviders\SCHANNEL\Protocols\TLS1.2\Server\DisabledByDefault

Title	2.10Enable IP Address and Domain Restrictions
Description	The concept of Dynamic IP Address Restrictions which can be used to thwart DDos attacks.
Risk Rating	High

Impact:IP address and Domain Restriction filtering allows administrators to configure the server to block admin access and allow register IPs only.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager
2. Open the IP Address and Domain Restrictions feature
3. Open Feature or Double clickIP Address and Domain Restriction Setting
4. Click Edit and Feature settings in Action Pane
5. Select Deny in Access for unspecified clients so No one can access the admin panel
6. Then click Add Allow entry for allowing access for the following IP address or IP address Range (Internal or External Users)

Title	2.11Remove unwanted entries from Default Document
Description	The default document of that the site or application will return to a client browser when the site receives a request to the root directory.
Risk Rating	High

Impact: If there isn't a default document in the directory, the client will receive a "file not found" or "directory browsing denied" error. Also if we use one default document or use the first document in the list, this speeds up the request time.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager
2. Open the Sites node underneath the machine node
3. In Features View, find and double-click the Default Document
4. Click the document that you want to remove, and then click Remove in Action Pane

5. Click Add in Action pane and type the name of Default Document in the box that you want to add
6. Then Click OK

Note: Don't give common names (such as Default.aspx, index.htmletc.) to site default/home page

X

Title	2.12Encrypt DB Connection String
Description	ASP.NET stores all the configuration information in plain text files called web.config and machine.config files. We store all vital information including database connection strings, user names, passwords for the databases.
Risk Rating	High

Impact: Storing all sensitive information in vulnerable plain text files or DB connection string which is nothing but security compromise.

Solution: It is recommended to encrypt connection string in web.config file.

Alternative Solution:

1. Open Command Prompt with Administrator privileges
2. At the Command Prompt, enter:
3. The aspnet_regiis.exe tool is located in the %systemroot%\Microsoft.NET\Framework\versionNumberfolder.
4. In case your web config is located in "/SampleApplication/" directory path, then enter the following to encrypt the ConnectionString. Use Aspnet_regiis.exe tool with the

   -pef option and specify the application path as shown below.

   Note: The -app option, passing it the name of your application.

   aspnet_regiis -pef "connectionStrings" -app "/SampleApplication/Web.config"

   Note: The parameter "connectionStrings" is case sensitive.

Decrypting the Connection String

5. Simply perform the following command to decrypt the connectionStrings element in the Web.config file.

   aspnet_regiis -pdf "connectionStrings" -app "/SampleApplication/Web.config"

   Note: The parameter "connectionStrings" is case sensitive.

Authentication Configuration

Title	2.13 SSL Forms Authentication
Description	Forms-based authentication can pass credentials across the network in clear text.
Risk Rating	High

Impact: Implementing SSL for Forms Authentication will protect the confidentiality of credentials during the login process, helping mitigate the risk of stolen user information.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager and navigate to the appropriate tier
2. In Features View, double-click Authentication
3. On the Authentication page, select Forms Authentication
4. In the Actions pane, click Edit
5. Check the Requires SSL checkbox in the cookie settings section, click OK

Title	2.14Forms Authentication
Description	Forms Authentication can be configured to maintain the site visitor's session identifier in either a URI or cookie.
Risk Rating	High

Impact: An attacker can hi-jack a user's session to gain unauthorized access to the application.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager and navigate to the level where Forms Authentication is enabled
2. In Features View, double-click Authentication

3. On the Authentication page, select Forms Authentication
4. In the Actions pane, click Edit
5. In the Cookie settings section, select Use cookies from the Mode dropdown

Title	2.15 Cookie Protection Mode
Description	Cookie protection mode always encrypt and validate Forms Authentication cookies.
Risk Rating	High

Impact: An attacker can hi-jack cookie to gain unauthorized access to the application.

Solution: It is recommended to implement the below setting:

1. Open IIS Manager and navigate to the level where Forms Authentication is enabled
2. In Features View, double-click Authentication
3. On the Authentication page, select Forms Authentication
4. In the Actions pane, click Edit
5. In the Cookie settings section, verify the drop-down for Protection mode is set for Encryption and validation

X

Title	2.16Ensure passwordFormat Credentials Element Not Set To Clear
Description	PasswordFormat attribute specifies the encryption format for storing passwords.
Risk Rating	High

Impact: An attacker can intercept Authentication credentials transmitted in clear text.

Solution: It is recommended to implement the below setting:

1. Locate and open the configuration file where the credentials are stored
2. Find the <credentials> element
3. If present, ensure passwordFormat is not set to Clear
4. Change passwordFormat to SHA1 or MD5

X

Title	2.17Configure SSL for Basic Authentication
Description	Basic Authentication can pass credentials across the network in clear text. It is therefore imperative that the traffic between client and server be encrypted using SSL.
Risk Rating	High

Impact: Credentials sent in clear text can be easily intercepted by malicious code or persons. Enforcing the use of Secure Sockets Layer will help mitigate the chances of hijacked credentials.

Solution: To Use Basic Authentication with SSL:

1. Open IIS Manager
2. In the Connections pane on the left, select the server to be configured
3. In the Connections pane, expand the server, then expand Sites and select the site to be configured
4. In the Actions pane, click Bindings; the Site Bindings dialog appears
5. If an HTTPS binding is available, click Close and see below "To require SSL"
6. If no HTTPS binding is visible, perform the following steps

   To add an HTTPS binding:
   1. In the Site Bindings dialog, click Add; the Add Site Binding dialog appears
   2. Under Type, select https
   3. Under SSL certificate, select an SSL certificate
   4. Click OK, then close

7. Change passwordFormat to SHA1 or MD5

X

Title	2.18 Enable Advanced IIS Logging
Description	IIS Advanced Logging is a module which provides flexibility in logging requests and client data.
Risk Rating	Medium

Impact: Correlation of logs and establishment of timeline for any malicious activity detected cannot be accurately performed.

Solution: It is recommended to implement the below setting:

1. Open Internet Information Services (IIS) Manager
2. Click the server in the Connections pane
3. Double-click the Advanced Logging icon on the Home page
4. Click Enable Advanced Logging in the Actions pane

Note: The following fields should be logged:

a. date
b. time
c. s-ip
d. cs-method
e. cs-uri-stem
f. cs-uri-query
g. s-port
h. c-ip
i. cs(User-Agent)
j. cs(Referer)
k. sc-status
l. sc-bytes

3 ASP.NET Configuration Recommendations

#	Policy	Description	Suggested Setting
1	Set Deployment Method to Retail	The <deployment retail> switch is intended for use by production IIS Servers. This switch is used to help applications run with the best possible performance	It is recommended to implement the below settings: Open the machine.config file located in:%windir%\Microsoft.NET\Framework\<framework_version>\CONFIG Add the line <deployment retail=”true”/> within the <system.web> section If the systems are 64-bit, do the same for the machine.config located in: %windir%\Microsoft.NET\Framework64\<framework_version>\CONFIG
2	Remote authors or content providers will only use secure encrypted logons and connection to upload files to the Document Root directory	Logging in to a web server via a telnet session or using HTTP or FTP in order to upload documents to the web site is a risk if proper encryption is not utilized to protect the data being transmitted. A secure shell service or HTTPS need to be installed and in use for these purposes.	User only secure encrypted logons and connections for uploading files to the web site.
3	Access to the web content and script directories must be restricted	Excessive permission for the anonymous web user account is a common fault contributing to the compromise of a web server. If the account is able to upload and execute files on the web server, the organization or owner of the server will no longer have control of the asset.	It is recommended to implement the below setting: 1. Open IIS Manager. 2. Click and expand the Sites name under review. 3. In the Actions pane select Edit

			Permissions. 4. Select the Security Tab. 5. Set the permissions for the accounts IUSR and Everyone to read.
4	The application pool identity must be defined for each web site.	Creating a custom identity for each application pool will better track issues occurring within each web-site. When a custom identity is used, the rights and privileges must not exceed those associated with the Network Service security principal.	1. Open IIS Manager. 2. Click the Application Pools. 3. Highlight an Application Pool to review and click Advanced Settings in the Actions Pane. 4. Scroll down to the Process Model section and set the value for Identity to ApplicationPoolIdentity, Network Service or a custom identity with rights and privileges equal to or less than the built-in security principle.
5	Web server/site administration must be performed over a secure path	Logging into a web server via telnet session or using HTTP or FTP to perform updates and maintenance carries risk because userIDs and passwords are passed in the plain text. A secure shell service or HTTPS should be used for these purposes. Another alternative is to administer the web server /site from the local console.	1. Develop documentation listing those individuals who are authorized to perform remote administration. 2. Right-click the Computer icon, select Properties. 3. Click Remote Settings. 4. Select Allow connections only from computers running remote desktop with Network Level Authentication. 5. Click Select Users and add the users to the list the SA has documented as authorized to access the system remotely.

6	Turn Debug Off	Setting compilation debug to false ensures detailed error information does not inadvertently display during live application usage, mitigating the risk of application information being display to users.	1. Open IIS Manager. 2. Click the site name under review. 3. Double-click .NET Compilation 4. Scroll down to the Behavior section and set the value for Debug to False.
7	Ensure Custom Error Messages are not Off	When an ASP.NET application fails and causes an HTTP/1.x 500 Internal Server Error, or a feature configuration (such as Request Filtering) prevents a page from being displayed, an error message will be generated. This error messages enumerates the backend technology used to the attacker.	It is recommended to implement the below setting: 1. Open the IIS Manager GUI and navigate to the site to be configured 2. In Features View, find and double-click .NET Error Pages icon. 3. In the Actions Pane, click Edit Feature Settings. 4. In modal dialog, choose On or Remote Only for Mode settings. 5. Click OK.
8	ASP.NET stack tracing is Not Enabled	The trace element configures the ASP.NET code tracing service that controls how trace results are gathered, stored, and displayed.	It is recommended to disable trace attribute in web.config file by configuring the below value Trace=”true”
9	Configure Use Cookies Mode for Session State	A session cookie associates session information with client information for that session, which can be the duration of a user’s connection to a site.	It is recommended to configure sessionState tag is set to use cookies: 1. Open the IIS Manager GUI and navigate desired server, site, or application. 2. In Features View, find and double-click the Session State icon.

			3. In the Cookie Setting section, choose Use Cookies from the Mode dropdown. 4. In the Actions Pane, click Apply.
10	Ensure Cookies Are Set With HttpOnly Attribute	The HttpOnly flag indicates to the user agent that the cookie must not be accessible by client-side script	It is recommended that the httpOnlyCookies attribute be set to true. 1. Locate and open the application's web.config file 2. Add the <httpCookieshttpOnlyCookies="true" /> tag within <system.web>:
11	Hide IIS HTTP Detailed Errors from Displaying Remotely	A Web site's error pages are often set to show detailed error information for troubleshooting purposes during testing or initial deployment.	It is recommended to remove detail error pages by configuring the below settings 1. Open IIS Manager with Administrative privileges. 2. In the Connections pane on the left, expand the server, then expand the Sites folder. 3. Select the Web site or application to be configured. 4. In Features View, select Error Pages, in the Action pane, select Open Feature. 5. In the Actions Pane, select Edit Feature Settings. 6. In the Edit Error Pages Setting dialog, under Error Responses, select either Custom error pages or

			Detailederrorsfor local requests and custom error pages for remote requests. 7. Click OK and exit the Edit Error Pages Settings dialog.
12	Configure maxURL Request Filter	Limiting maxURL helps to ensure availability of web services and may also help mitigate the risk of buffer overflow type attacks.	It is recommended to limit maxURL request by entering the below command: 1. Open IIS Manager. 2. In the Connections pane, click on the connection, site, application, or directory to be configured. 3. In the Home pane, double-click Request Filtering. 4. In the Actions Pane, Click Edit Feature Settings. 5. Under the Request Limits section, key the maximum URL length in bytes that has been tested with web applications.
13	Configure MaxQueryString Request Filter	Configuring limits on web requests, helps to ensure availability of web services and may also help mitigate the risk of buffer overflow type attacks.	It is recommended to implement the below settings: 1. Open the IIS Manager. 2. Click the site name under review. 3. Double-click the Request Filtering icon. 4. In the Actions Pane, Click Edit Feature Settings. 5. Set the Maximum Query String value

			to 2048.
14	Disallow non-ASCII Characters in URLs	Configuring limits on web requests, it ensures availability of web services and mitigates the risk of buffer overflow type attacks. The allow high-bit characters Request Filter enables rejection of requests containing non-ASCII characters.	It is recommended to implement the below settings: 1. Open the IIS Manager. 2. Click the site name under review. 3. Double-click the Request Filtering icon. 4. In the Actions Pane, Click Edit Feature Settings 5. Uncheck the allow high-bit characters checkbox.
15	Ensure Double-Encoded Request will be Rejected	Request filtering enables administrators to create a more granular rule set with which to allow or reject inbound web content. It ensures availability of web services and mitigates the risk of buffer overflow type attacks.	It is recommended to implement the below settings: 1. Open IIS Manager. 2. In the Connections pane, select the site, application, or directory to be configured. 3. In the Home pane, double-click Request Filtering. 4. In the Actions Pane, Click Edit Feature Settings. 5. Under the General Section, uncheck Allow double escaping.
16	Disallow Unlisted File Extensions	Unlisted property of the File Extensions Request Filter enables rejection of requests containing specific file extensions not defined in the File Extensions filter.	It is recommended to implement the below settings: 1. Open IIS Manager. 2. In the Connections pane, select the

			server. 3. In the Home pane, double-click Request Filtering. 4. In the Actions Pane, Click Edit Feature Settings. 5. Under the General Section, uncheck Allow unlisted file name extensions.
17	Ensure Handler is not granted Write and Script/Execute	Allowing both Execute/Script and Write permissions, a handler can run malicious code on the target server.	It is recommended to implement the below settings: 1. Open theApplicationHost.config file in %windir%\system32\inetsrv\config 2. Edit the <handlers> section accessPolicy attribute so that write is not present when Script or Execute are present.
18	Disable HTTP Trace Method	The HTTP TRACE method returns the contents of client HTTP requests in the entity-body of the TRACE response. Attackers could leverages this behavior to access sensitive information, such as authentication data or cookies, contained in the HTTP headers of the request.	It is recommended to implement the below settings: 1. Open IIS Manager. 2. In the Connections pane, select the site, application, or directory to be configured. 3. In the Home pane, double-click Request Filtering. 4. In the Request Filtering pane, click the HTTP verbs Tab, and then click Deny Verb… in the Actions Pane. 5. In the Deny Verb dialog box, enter the TRACE, and then click OK.

4 Application Root Folder Permission at IIS Server

#	Application Type	Permissions
1.	ASP	The application 'root' folder should be given 'READ' and 'SCRIPT ONLY' at the web server level
2.	ASPX	The application 'root' folder should be given 'READ' and 'SCRIPT EXECUTE' at the web server level
File Upload Permission		
3. Application files saved in the database, no permission required.		
4. Files saved in file system then 'File Name' folder should be given 'READ' and 'WRITE' permission		

…End of Document…