**Abstract**

This paper is designed to demonstrate the common IIS web server security specifications in the form of a checklist that aids web masters or penetration testers to implement a secure web server infrastructure swiftly. It is mandatory for a web application to be duly full proof from vicious attacks and for stopping damage which could be in any form. Security professionals and penetration testers are typically part of a web project to ensure the website is protected from various attacks by detecting loopholes which might be exploited later. But such a critical task is typically not followed in a proper manner, and web applications go live into the production environment with inherent vulnerabilities, or even without complying to security guidelines. It is so because developers and organizations are often in a hurry to launch the software into the production environment due to various unnamed pressures.

Unfortunately, there is no single tool available which can claim comprehensive security of an application, because attacks can come in any form, in fact the horizon is so extensive that it is beyond assumption. So such summarized checklist snapshots have proven to be truly a savior for hardening or to improve our deployment workstation security precipitously.

**Virtual Directory**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Ensure restriction is enabled to those directories that allow anonymous access | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS1.gif |
| Ensure IISAdmin, IISHelp, IISamples directory are removed | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS2.gif |
| Confirm PARENT PATH configuration is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS3.gif |
| Ensure unused Front pages extension is removed | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS4.gif |
| Ensure website directories are dislocated from the system partition drive | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS5.gif |
| Ensure directory traversing is disabled (uncheck write permission) | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS6.gif |
| Ensure other unused utilities such resource kit, SDK are detached | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS7.gif |

**Machine Configuration File**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Ensure DEBUG is turned off in WEB.CONFIG file | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS8.gif |
| Ensure TRACE is set to false or disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS9.gif |
| Ensure unnecessary HTTP Modules are removed | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS10.gif |

**Secure Communication**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Ensure HTTP requests are filtered or categorized | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS11.gif |
| Ensure HTTPS is enabled, in case your website deals with sensitive data | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS12.gif |
| Ensure Server Certificates are updated and issued by a trusted organization | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS13.gif |
| Ensure Certificates have not withdrawn | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS14.gif |
| In case of remote administration, ensure proper time-outs and encryption are configured | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS15.gif |
| Ensure communication happens through only port 80 or 443 | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS16.gif |
| Ensure that IPSec is formed in the network for secure communication | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS17.gif |

**Logging and Audit**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Ensure Failed Logon Attempts are regularly inspected | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS18.gif |
| Ensure Log files are properly maintained and audited | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS19.gif |
| Confirm W3C extended format is enabled for auditing | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS20.gif |

**IIS Metabase and Filters**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Ensure Banner grabbing is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS21.gif |
| Ensure File (%systemroot%\system32\inetsrv\metabase.bin) access is restricted | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS22.gif |
| Ensure unused extensions (.shtml, .hta, .htw, .stm) are removed | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS23.gif |
| Ensure unemployed ISAPI filters are disabled or removed. | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS24.gif |
| Ensure ‘Forbidden Handler’ is mapped to unemployed ASP.NET files extension | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS25.gif |

**Server Accounts**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Ensure anonymous logon is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS26.gif |
| Ensure unused IUSR\_MACHINE account is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS27.gif |
| Ensure a solitary administrator account only | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS28.gif |
| Ensure administrator account is properly hardened by strong password scheme | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS29.gif |
| Ensure GUEST account is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS30.gif |
| Ensure remote logon is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS31.gif |
| Ensure ASP.NET process account is configured to least access | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS32.gif |
| Ensure anyone couldn’t login locally except administrator | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS33.gif |

**Code Access Security**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Confirm CAS is enabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS34.gif |
| Confirm source code is obfuscated | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS35.gif |
| Confirm custom error page is installed on server | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS36.gif |
| Confirm permissions removed from Internet and Intranet zone | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS37.gif |

**System Configuration**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Confirm ASP .NET state service is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS38.gif |
| Confirm Remote Registry Administration is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS39.gif |
| Confirm WebDAW service is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS40.gif |
| Confirm FTP and SMTP services are disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS41.gif |
| Confirm SMB service is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS42.gif |
| Confirm All Redundant share’s (C$, D$,..) is removed | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS43.gif |
| Confirm Remote Administration by TELNET is disabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS44.gif |
| Confirm only essential System Services are given least privileges | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS45.gif |
| Confirm redundant system services are stopped | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS46.gif |
| Ensure IIS is not installed on domain controller | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS47.gif |
| Ensure IDS is installed in the network perimeter | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS48.gif |
| Ensure that IIS server is configured inside DMZ | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS49.gif |

**Server Updates**

|  |  |
| --- | --- |
| Security Specifications | Status |
| Ensure Windows Operating System is updated | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS50.gif |
| Ensure .NET Framework is Updated | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS51.gif |
| Ensure IIS web server is duly patched | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS52.gif |
| Ensure MBSA is configured and running regularly | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS53.gif |
| Ensure EMET is installed on server and enabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS54.gif |
| Ensure Microsoft Notification Service is Enabled | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS55.gif |
| Ensure effective Anti-virus is installed and running | http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/042714_1222_SecuringIIS56.gif |

**Final Note**

In this article, we have seen how to harden the IIS web server to protect ASP.NET websites. This article in fact didn’t explain various attacks and their countermeasure. Instead, it is pinpointing major security guidelines in the form of checklists which can be applied swiftly over a web server, so that a developer can ensure himself that a particular security mechanism is applied and it is enabled. Because some critical bugs go unnoticed and remain in the final version of the software, which could get the application into trouble. Hence, such a synopsis reference eases the undertaking of developers or security professionals in terms of not overlooking or forgetting critical security configurations on the web server.