IBM HTTP Web server Hardening Document

Revision Number: 1.10
Revision Date: 31 March, 2019

Table of Contents

Version Control History:

Review History

Version No	Author	Reviewed By	Date of Review	Remarks
1.0	Devraj Ardu / Ankit Jain / Jitendra Chavan	Rakesh Mashruwala	02 Aug 2010	Initial Draft
1.1	IPAT, WebAdmin team	Rakesh Mashruwala	30 Aug 2010	Revised based on admin comments
1.2	IPAT, WebAdmin team	IAG / ISG	16 June2011	Annual Revision
1.3	Jitendra Chavan	BTO Web Admin team\ISG	31 March 2012	Annual Revision
1.4	Harshad Mahajan	ISG, TIG and BTG	15 May 2013	Annual Revision
1.5	Uday Solanke and Sachin Pandhare	ISG, TIG and BTG	20th Jan 2014	Annual Revision
1.6	Harshad Mahajan	ISG-IPAT	8 December 2015	Risk classification
1.7	Amol Shukla	ISG-IPAT / BTO APP TEAM	9 January 2016	Annual Revision
1.8	Troy Lewis	ISG-IPAT	11th August 2017	Annual Revision
1.9	Harshad Mahajan / Roopesh Sarupuru	ISGIPAT / BTOApp Team	30th March, 2018	Annual Revision
1.10	Amit Rane/Pratish Sawant	ISGIPAT/BTOApp Team	31st March 2019	Annual Revision

1. Introduction

Purpose

The purpose of this document is to highlight the key security considerations to be put in place before offering any service on the Internet / Intranet. These security practices will assist ICICI Bank in:

- Establishing a sound and robust technology risk management process
- Strengthening system availability, security and recovery capability

Scope

All systems implemented on ICICI Bank network will need to comply with the guidelines mentioned in this document.

Any exceptions to the guidelines should be brought to the notice of management for their sign off before implementing the system in production.

These hardening parameters do not replace hardening documents relating to the OS, database and application.

2. Guidelines

1.	Business Approval Procedures should be in place, to ensure that all information posted to the Internet or Intranet is reviewed and approved by the respective department head and information owner.	Internet Facing	Intranet Facing
2.	Harden the Operating System before configuring the Http Web Server component and apply all the latest patches	High	High
3.	For configuring Web server, user “sysadmin” should be used for unix and “netadmin” for windows. Patches recommended by IBM must be implemented during configuration	High	High
4.	It’s important to separate the binaries /bin, docs (/htdocs), and logs (/logs) into separate partitions on the system.	Low	Low
5.	Create a distinct group for all the users who will have permission to change the configuration, start, and stop the web server i.e webserv.	Low	Low
6.	Disable SSL v2 and Low strength ciphers. Configure SSLv3 for securing all communication between Application server, Webserver and Database and Browser	Low	Low
7.	Disable by default web servers return information about the product and version they are running in the Server variable of the HTTP header.	High	Medium
8.	Remove default IBM HTTP server files, It’s important to remove default files such as .html, cgi files etc.	High	Medium
9.	Set AddServerHeader off to prevent IBM HTTP Server from adding the Server header to outgoing responses.	High	Medium

10.	Preventing information leaks Remove the web server information from the error pages by changing the value of the ServerSignature directive (in httpd.conf): 1. ServerSignature - Off 2. ServerTokens - Prod	High	Medium
11.	Set following directory and file permissions for the server: Following directory permission should be set • bin – to be set to 755. Ownership will be with btowebadmin ID • conf– to be set to 740. Ownership will be with btowebadmin ID • logs - to be set to 755 It should be readable only by the btowebadmin ID. • Htdoc s – to be set to 740. Ownership will be with btowebadmin ID	Medium	Medium
12.	Separation of web content and web system files The web document directory should be in a separate directory from the web server's system files.	High	High
13.	Default listening port should be changed to a non trojan port other than 8008. For list of trojan ports that should not be used, refer http://10.16.168.211/InfoSecurity/Security_Alerts/Trojan%20Port%20List%20Ver_1.pdf	High	High
14.	Default home page should be removed or changed to other page	High	Medium
15.	Remove version information from banner	High	Medium
16.	Review all default users (other than 'nobody') created during installation and change the default passwords.	High	Medium
17.	The HTTP account must not be used as a regular login account, and should be assigned an invalid or nologin shell to ensure that the account cannot be used to login.	Medium	Medium
18.	The user account under which HTTP runs, should not have a valid password, but should be locked.	High	Medium

19.	Track,.Trace, Put, Delete, Options, Option, Propfind dangerous options should be disabled	High	Medium

20.	Cookie attribute should be set to HTTPOnly and secureflag	Medium	Medium
21.	An adversary should not be able to fingerprint the web server from the HTTP responses	Medium	Medium
22.	Disable directory browsing	High	Medium
23.	Necessary security patches should be applied based on criticality and its potential impact as per patch management policy before and after going live.	High	High
24.	Installing the server in DMZ An Open (public) web server is to be isolated in a DMZ. Such a web server should be behind the perimeter router and firewall and also separated from Internal LANs by either a combination of a firewall, a switch or router, or both with necessary access controls	High	High
25.	Backup and recovery Proper procedures for backup & recovery of web server should be defined.	High	High
26.	Modules to disable Disable the following default modules for your production server: • info: gives out too much information about your web server to potential attackers. • status: gives out server stats via web pages. • autoindex: provides directory listings when no index.html file is present. • imap: provides server-side mapping of index files. • include: provides server-side includes (.shtml files) • userdir: translates URLs to user-specific directories • auth: you won't need it – you'll set up authentication against LDAP via mod_ldap For implementing the same, Log Level should be set to WARN	High	Medium

27.	Disable HTTP methods	High	Medium
28.	JMX MBeans are network accessible and ensure that they have proper authorization on their operations	Low	Low
29.	Cgi-bin directory should be disabled	High	Medium
30.	Following settings should be in place • Session Idle timeout – 600 • MaxClients – 6000 • Startserver – 16	Medium	Low
31.	The log_config module provides for flexible logging of client requests, and provides for the configuration of the information in each log.	Medium	Low
32.	The http mod_dav and mod_dav_fs modules support WebDAV ('Webbased Distributed Authoring and Versioning') functionality for Http. WebDAV is an extension to the HTTP protocol which allows clients to create, move, and delete files and resources on the web server.	Medium	Medium
33.	The Http proxy module allow the server to act as a proxy (either forward or reverse proxy) of http and other protocols with additional proxy modules loaded. If the http installation is not intended to proxy requests to or from another network then the proxy module should not be loaded.	Medium	Medium
34.	Although Http typically is started with root privileges in order to listen on port 80 and 443, it can and should run as another non-root user in order to perform the web services. The Http User and Group directives are used to designate the user and group to be used	Low	Low
35.	Most Web Servers include Http installations have default content which is not needed or appropriate for production use. The primary function for these sample content is to provide a default web site, provide user manuals or to demonstrate special features of the web server. All content that is not needed should be removed.	Medium	Medium
36.	Restrict access to any files beginning with .ht using the FileMatch directive.	Low	Low

37.	The Http Listen directive specifies the IP addresses and port numbers the Http web server will listen for requests. Rather than be unrestricted to listen on all IP addresses available to the system, the specific IP address or addresses intended should be explicitly specified. Specifically a Listen directive with no IP address specified, or with an IP address of zero's should not be used.	High	Medium
38.	Corporate anti virus software should be installed on the server and it should be updated.	Medium	Medium
39.	Disable unused ports.	High	Medium
40.	Enable port filtering .	Medium	Low
41.	Cookie path attribute should be set	Medium	Low
42.	All Security headers should be set.	Medium	Low
43.	Minimize the Server Footprint It is not recommended to operate multiple services like mail, FTP, LDAP etc. on the same server, unless absolutely necessary	Medium	Low
44.	TLS 1.2 should be enable.	Medium	Low
45.	Click checking should to be implemented on server.	Medium	Low
46.	TCP sequence number approximation based-denial of service	Medium	Low
47.	SNMP service should be disable.(Its leads to enumeration)	Medium	Low
48.	Disable Etag header	Medium	Low
49.	Ensure mod_headers.so is enabled in httpd.conf. and Header X-Frame-Options set to SAMEORIGIN	Medium	Low
50.	Set Header X-XSS-Protection "1; mode=block" to prevent cross site scripting	Medium	Low
51.	LTPAToken2 expiration is 120 Minutes	Medium	Low
52.	Enable Security Integration	Medium	Low

53.	Enable modern ciphers and key exchange using TLS v1.2 in httpd.conf as below SSLProtocolDisable SSLv2 SSLv3 TLSv10 TLSv11 SSLCipherSpec ALL NONE SSLCipherSpec TLSv12 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 SSLCipherSpec TLSv12 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 SSLCipherSpec TLSv12 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 SSLCipherSpec TLSv12 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 SSLCipherSpec ALL TLS_RSA_WITH_AES_128_GCM_SHA256 SSLCipherSpec ALL TLS_RSA_WITH_AES_256_GCM_SHA384 SSLCipherSpec ALL TLS_RSA_WITH_AES_128_CBC_SHA256 SSLCipherSpec ALL TLS_RSA_WITH_AES_256_CBC_SHA256 SSLCipherSpec ALL TLS_RSA_WITH_AES_128_CBC_SHA SSLCipherSpec ALL TLS_RSA_WITH_AES_256_CBC_SHA SSLCipherSpec ALL SSL_RSA_WITH_3DES_EDE_CBC_SHA SSLEnable	High	Medium
54.	Auditing of Success/Failure events for critical content directories On a windows Setup : The following events should be logged for Application Content directories : Create files / write data Create folders / append Data Delete subfolders and files Delete Change permission and take ownership Permissions on such log files should be restricted to Administrators o changes to, or attempts to change, system security settings and controls o log on attempts (successful or unsuccessful) o account changes (e.g., account creation and deletion, account privilege assignment) o successful/failed use of privileged accounts o successful and failed application authentication attempts o application account changes (e.g., account creation and deletion, account privilege assignment)	Medium	Medium

	o use of application privileges o application startup and shutdown o application failures o major application configuration changes		

3. Exception

The Information Security policy and procedure document at ICICI Bank requires all the above security parameters should be implemented. In case it is not possible to implement any/all parameters, for whatsoever reason the Admin should ensure that the business head should sign an appropriate exception form highlighting the security parameters not implemented together with the reasons for non- compliance.