Rebellion UI Production

Apache Hardening

Contents

1. Document Control

1.1 Document Preparation

Date	Version	Author	Role	Comment
06/24/2015	0.1	Cloud Security Engineering	Cloud Security	1st Draft

1.2 Document Review Members

A series of workshop and review meetings held between x/x/x and x/x/x with the following people contributing to the reviewing and approval process.

Date	Version	Reviewer	Role	Status
		Arjun Shah	Delivery lead	

1.3 Informed participants

Date	Version	Resource	Role	Status

1.4 Document Approval/Signoff

Date	Version	Reviewer	Role	Status

2. Overview

This document covers the standard configurations for apache web servers in Rebellion environment.

3. Application Hardening Standards

3.1 Operating System Security

Oracle Enterprise Linux is the standard operating system used for all instances in Rebellion per EIT standards. As a Red Hat Enterprise Linux derivative, Oracle Linux provides full compatibility for applications designed to be run in RHEL environments, with the significant advantage that Oracle freely distributes Oracle Linux without the need for licencing, leading to significant cost savings over Red Hat's per-server licensing. Oracle Linux is preferable to CentOS, another freely available RHEL derivative, because Oracle Linux is backed by Oracle, with notable enhancements and the option of receiving official Oracle support. Configuration standards for Operating system are covered

separately under Operating system hardening standards documentation.

3.2 Application Security

3.2.1 Apache

The Apache HTTP server is utilized across all AWS Rebellion systems and environments. The version of Apache used is v2.2. These standards are derived from industry best practices and references from Center for Internet Security (CIS) Benchmark guides for Apache.

3.2.1.1 Standard Configuration

Ref. No	Description	Reference	Settings
1.1.1	The /tmp directory is a world-writable directory used for temporary storage by all users and some applications.	The /tmp reside on a separate mount point created based on Operating system hardening standards	/tmp directory created
1.2.1	Enable only necessary Authentication and Authorization Modules - 'Loaded auth._* modules'	/usr/sbin/httpd -M | /usr/bin/egrep 'auth._' /usr/sbin/httpd -M | /usr/bin/egrep 'ldap	Modules are disabled by commenting out or removing the LoadModule directive from the Apache configuration files httpd.conf #LoadModule auth_basic_module modules/mod_auth_basic.so #LoadModule auth_digest_module modules/mod_auth_digest.so #LoadModule authn_file_module modules/mod_authn_file.so #LoadModule authn_alias_module modules/mod_authn_alias.so #LoadModule authn_anon_module modules/mod_authn_anon.so #LoadModule authn_dbm_module modules/mod_authn_dbm.so #LoadModule authn_default_module modules/mod_authn_default.so #LoadModule authz_host_module modules/mod_authz_host.so #LoadModule authz_user_module modules/mod_authz_user.so #LoadModule authz_owner_module modules/mod_authz_owner.so #LoadModule authz_groupfile_module modules/mod_authz_groupfile.so #LoadModule authz_dbm_module modules/mod_authz_dbm.so #LoadModule authz_default_module modules/mod_authz_default.so

			#LoadModule ldap_module modules/mod_ldap.so #LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
1.2.2	Enable the Log Config Module - 'log_config_module is loaded'"	'/usr/sbin/httpd -M | /bin/grep log_config	Enabled the Log Config Module LoadModule log_config_module modules/mod_log_config.so
1.2.3	Disable WebDAV modules - 'dav_*module is not loaded'"	'/usr/sbin/httpd -M | /usr/bin/egrep -v '^([Ll]oaded|[Ss]yntax)' | /usr/bin/egrep 'dav[^\s]+module' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	Disabled load module by commenting out or removing the LoadModule directive from the Apache configuration files httpd.conf #LoadModule status_module modules/mod_status.so
1.2.4	Disable Status module - 'status_module is not loaded	/usr/sbin/httpd -M | /usr/bin/egrep -v '^([Ll]oaded|[Ss]yntax)' | /usr/bin/egrep 'status_module' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	Disabled the LoadModule directive from the Apache configuration files httpd.conf #LoadModule status_module modules/mod_status.so
1.2.5	Disable Autoindex module - 'autoindex_module is not loaded	'/usr/sbin/httpd -M | /usr/bin/egrep -v '^([Ll]oaded|[Ss]yntax)' | /usr/bin/egrep 'autoindex_module' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	autoindex_module is enabled but have set Options = None as per the recommendation.
1.2.6	Disable Proxy Modules - 'proxy_* is not loaded	'/usr/sbin/httpd -M | /usr/bin/egrep -v '^([Ll]oaded|[Ss]yntax)' | /usr/bin/egrep 'proxy_' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	Disabled the LoadModule directive from the Apache configuration files httpd.conf #LoadModule proxy_module modules/mod_proxy.so
1.2.7	Disable User Directories Modules - 'userdir_* is not loaded	/usr/sbin/httpd -M | /usr/bin/egrep -v '^([Ll]oaded|[Ss]yntax)' | /usr/bin/egrep 'userdir_' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	Disabled the LoadModule directive from the Apache configuration files httpd.conf #LoadModule userdir_module modules/mod_userdir.so
1.2.8	Disable Info module - 'info_module is not loaded	/usr/sbin/httpd -M | /usr/bin/egrep -v '^([Ll]oaded|[Ss]yntax)' | /usr/bin/egrep 'info_module' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	Disabled the LoadModule directive from the Apache configuration files httpd.conf #LoadModule info_module modules/mod_info.so
1.3.1	Run the Apache Web Server as a non-root user - 'httpd.conf User = apache	/etc/httpd/conf/httpd.conf /usr/bin/id apache' /bin/ps axu | /bin/grep httpd | /usr/bin/egrep -v '(^root|grep\s+httpd)' | /usr/bin/egrep -v '^apache' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	Applications runs as apache user and apache group
1.3.2	Give the Apache User Account an Invalid Shell - 'apache user shell is /sbin/nologin	/bin/grep apache /etc/passwd | /usr/bin/egrep -v '\/sbin\/nologin\s*$' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	Set to /sbin/nologin shell.
1.3.3	Lock the Apache User Account - 'apache user password	/usr/bin/passwd -S apache	passwd -l apache
1.3.4	Apache Directory and File Ownership - '$APACHE_PREFIX owned by root:root	Update APACHE_PREFIX with the proper value for the local environment	change apache path /usr/local/apache2 to /etc/httpd/conf- Owned by root

1.3.5	Apache Directory and File Permissions - '$APACHE_PREFIX mode 755'	Update /etc/httpd/conf to 755	Apache Directories are set to 755
1.3.5	Apache Directory and File Permissions - '$APACHE_PREFIX/bin mode 751	Update /etc/httpd/conf with 755 and files to 644	All apache directory has permission 755 and files 644
1.3.6	The CoreDumpDirectory directive can be used to specify a directory which Apache attempts to switch before dumping core for debugging	Change CORE_DUMP_DIR with the appropriate value for the local environment	Added CoreDumpDirectory /var/log/httpd in httpd.conf file
1.3.8	The PidFile directive sets the file path to the process ID file to which the server records the process ID of the server Pid File Security - 'PidFile is configured'	/etc/httpd/conf/httpd.conf	PID file is configured
1.3.8	The PidFile directive sets the file path to the process ID file to which the server records the process ID of the server, which is usefulfor sending a signal to the server process or for checking on the health of the process. If the PidFile is placed in a writable directory, other accounts could create a denial of service attack and prevent the server from starting by creating a pid file with the same name.	Validate Pid File Security - 'PidFile permissions	/var/run/httpd - drwx--x--- 2 root apache – httpd
1.3.9	The ScoreBoardFile directive sets a file path which the server will use for inter-process communication (IPC) among the Apache processes	ScoreBoard File Security - 'ScoreBoardFile is configured /etc/httpd/conf/httpd.conf" does not contain "^[\s\t]*[Ss]core[Bb]oard[Ff]ile\s+	Changes updated

1.4.1	Deny Access to OS Root Directory - 'httpd.conf Order = Deny,Allow Deny Access to OS Root Directory - 'httpd.conf Deny = from all' Deny Access to OS Root Directory - 'httpd.conf no Allow directives exist	/bin/sed -n '/<Directory \/>/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Oo]rder\s+ '/bin/sed -n '/<Directory \/>/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Dd]eny\s+'' /bin/sed -n '/<Directory \/>/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Aa]llow\s+' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	perl -ne 'print if /^ *<Directory *\//i .. /<\/Directory/i' /etc/httpd/conf/httpd.conf <Directory /> Order deny,allow Deny from all Options None AllowOverride None </Directory>
1.4.2	Allow Appropriate Access to Web Content - 'httpd.conf Order = Deny,Allow Allow Appropriate Access to Web Content - 'httpd.conf Deny is configured Allow Appropriate Access to Web Content - 'httpd.conf Allow is configured	/bin/sed -n '/<Directory "/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Oo]rder\s+' | /usr/bin/egrep -v '^\s*[Oo]rder\s+[Dd][Ee][Nn][Yy],\s*[Aa][Ll][Ll][Oo][Ww]' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}'' /bin/sed -n '/<Directory "\\/var\\/www\\/html"/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Dd]eny\s+'' /bin/sed -n '/<Directory "\\/var\\/www\\/html"/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Aa]llow\s+''	Apply configuration as per recommendation in all directory. <Directory /> Order deny,allow Deny from all </Directory>
1.4.3	The Apache OverRide directive allows for .htaccess files to be used to override much of the configuration, including authentication,handling of document types, auto generated indexes, access control, and options. When the server finds an .htaccess file (as specified by AccessFileName) it needs to know which directives declared in that file can override earlier access information. When this directive is set to None, then .htaccess files are completely ignored. In this case, the server will not even attempt to read .htaccess files in the filesystem. When this directive is set to All,	/bin/sed -n '/<Directory \/>/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Aa]llow[Oo]verride\s+'	<Directory> . . . AllowOverride None . . . </Directory>

	then any directive which has the .htaccess. Context is allowed in .htaccess files.Restrict OverRide for the OS Root Directory - 'httpd.conf AllowOverride = None		
1.4.4	Restrict OverRide for All Directories - 'httpd.conf AllowOverride = None	/bin/sed -n '/<Directory "/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Aa]llow[Oo]verride\s+' | /usr/bin/egrep -v '^\s*[Aa]llow[Oo]verride\s+[Nn]one' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	<Directory> . . . AllowOverride None . . . </Directory>
1.5.1	Restrict Options for the OS Root Directory - 'httpd.conf Options = None	'/bin/sed -n '/<Directory \/>/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Oo]ptions\s+''	<Directory> . . . Options None . . . </Directory>
1.5.2	Restrict Options for the Web Root Directory - 'httpd.conf Options = None or Multiviews	'/bin/sed -n '/<Directory "/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Oo]ptions\s+' | /usr/bin/egrep -v '^\s*[Aa]llow[Oo]verride\s+([Nn]one|[Mm]ulti[Vv]iews)' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	<Directory> . . . Options None . . . </Directory>
1.5.3	Minimize Options for Other Directories - 'httpd.conf Options does not have Includes	'/bin/sed -n '/<Directory "/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Oo]ptions\s+' | /usr/bin/egrep -v '\s*[Ii]ncludes[N]o[Ee]xec' | /usr/bin/egrep '\s*[Ii]ncludes' | /usr/bin/awk '{print} END {if (NR == 0) print "none"}''	Includes option not used.
1.5.4	Remove Default HTML Content - 'httpd-manual is not installed	"/etc/httpd/conf/httpd.conf" does not contain "^[\s\t]*<Location /server-status>\s*"	Content has been removed
1.5.4	Remove Default HTML Content - 'Server Status handler does not exist	"/etc/httpd/conf/httpd.conf" does not contain "^[\s\t]*<Location /server-status>\s*"	Content has been removed
1.5.4	Remove Default HTML Content - 'Server Information handler does not exist	"/etc/httpd/conf/httpd.conf" does not contain "^[\s\t]*<Location /server-info>\s*"	Content has been removed
1.5.4	Remove Default HTML Content - 'perl-status handler does not exist	"/etc/httpd/conf/httpd.conf" does not contain "^[\s\t]*<Location /perl-status>\s*"	Content has been removed
1.5.5	Remove Default CGI Content printenv - 'printenv does not exist'	/var/www/cgi-bin/printenv	Content has been removed

1.5.6	Remove Default CGI Content test-cgi - 'test-cgi does not exist	/var/www/cgi-bin/test-cgi	Content has been removed
1.5.7	Limit HTTP Request Methods - 'httpd.conf Document Root Order = Allow, Deny	'/bin/sed -n '/<Directory "\\\/var\\/www\\/html"/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Oo]rder\s+''	<LimitExcept GET POST OPTIONS> deny from all </LimitExcept>
1.5.7	Limit HTTP Request Methods - 'httpd.conf Document Root LimitExcept = GET,POST or OPTIONS only'	The command '/bin/sed -n '/<Directory "\\\/var\\/www\\/html"/,/<\/Directory>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*<[Ll]imit[Ee]xcept\s+''	Configure <LimitExcept GET POST OPTIONS> deny from all </LimitExcept> for all directories.
1.5.8	Disable HTTP TRACE Method - 'httpd.conf TraceEnable = off'	/etc/httpd/conf/httpd.conf	Trace is OFF
1.5.9	Restrict HTTP Protocol Versions - 'httpd.conf RewriteEngine = on Restrict HTTP Protocol Versions - 'httpd.conf RewriteCond = %{THE_REQUEST} !HTTP/1.1$' Restrict HTTP Protocol Versions - 'httpd.conf RewriteRule = .* - [F] Restrict HTTP Protocol Versions - 'httpd.conf <VirtualHost> RewriteEngine = on Restrict HTTP Protocol Versions - 'httpd.conf <VirtualHost> RewriteOptions = inherit	'/bin/egrep '^[\s\t]*[Rr]ewrite[Ee]ngine\s*' /etc/httpd/conf/httpd.conf | /usr/bin/egrep -v '^[\s\t]*[Rr]ewrite[Ee]ngine\s+[Oo][Nn]\s*$' \| /usr/bin/awk '{print} END {if (NR == 0) print "none"}'' '/bin/egrep '^[\s\t]*[Rr]ewrite[Cc]ond\s*' /etc/httpd/conf/httpd.conf \| /usr/bin/egrep -v '^[\s\t]*[Rr]ewrite[Cc]ond\s+%{THE_REQUEST}\s+!HTTP/1\\.1\$' \| /usr/bin/awk '{print} END {if (NR == 0) print "none"}'' '/bin/sed -n '/### Section 3: Virtual Hosts/,$p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '(<VirtualHost|[Rr]ewrite[Ee]ngine)'' '/bin/sed -n '/### Section 3: Virtual Hosts/,$p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '(<VirtualHost|[Rr]ewrite[Oo]ptions)''	Add this in httpd.conf file RewriteEngine On RewriteOptions Inherit RewriteCond %{THE_REQUEST} !HTTP/1\.1$ RewriteRule .* - [F]
1.5.10	Restrict Access to .ht* files - 'httpd.conf Order = allow,deny Restrict Access to .ht* files - 'httpd.conf Deny = from all Restrict Access to .ht* files - 'httpd.conf Satisfy = all	'/bin/sed -n '/<FilesMatch "\^\\\.ht"/,/<\/FilesMatch>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Oo]rder\s+'' '/bin/sed -n '/<FilesMatch "\^\\\.ht"/,/<\/FilesMatch>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Dd]eny\s+'' '/bin/sed -n '/<FilesMatch "\^\\\.ht"/,/<\/FilesMatch>/p'	<FilesMatch "^\.ht"> Order allow,deny Deny from all Satisfy All </FilesMatch>

		/etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Ss]atisfy\s+''	
1.6.1	Configure the Error Log - 'httpd.conf LogLevel = notice info or debug	'/bin/sed -n '/<FilesMatch "\^\\\.ht"/,/<\/FilesMatch>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Ss]atisfy\s+''	LogLevel notice
1.6.1	Configure the Error Log - 'httpd.conf ErrorLog is configured	'/bin/sed -n '1,/### Section 3: Virtual Hosts/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^[\s\t]*[Ee]rror[Ll]og\s*''	LogLevel notice; ErrorLog "logs/error_log"
1.6.1	Configure the Error Log - 'httpd.conf <VirtualHost> ErrorLog is configured	'/bin/sed -n '/### Section 3: Virtual Hosts/,$p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '(<VirtualHost|[Ee]rror[Ll]og)''	VirtualHost config not used and disabled
1.6.2	Configure the Access Log - 'httpd.conf LogFormat is configured	Update LOG_FORMAT to the appropriate value for the local environment.	LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"" CustomLog log/access_log combined
1.6.2	Configure the Access Log - 'httpd.conf CustomLog is configured	/bin/sed -n '1,/### Section 3: Virtual Hosts/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^[\s\t]*[Cc]ustom[Ll]og\s*''	set CustomLog logs/access_log combined
1.6.2	Configure the Access Log - 'httpd.conf <VirtualHost> ErrorLog is configured	'/bin/sed -n '/### Section 3: Virtual Hosts/,$p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '(<VirtualHost|[Cc]ustom[Ll]og)''	VirtualHost config not used and disabled
1.6.4	Log Storage and Rotation - '/etc/logrotate.conf rotate log files = weekly'	Script awslogs.conf is already avaiable at /var/awslogs/etc and used for transfer logs to another location.	Script awslogs.conf is already available at /var/awslogs/etc and used for transfer logs to another location.
1.6.4	Log Storage and Rotation - '/etc/logrotate.conf rotate > 52	Script awslogs.conf is already avaiable at /var/awslogs/etc and used for transfer logs to another location.	Script awslogs.conf is already avaiable at /var/awslogs/etc and used for transfer logs to another location.
1.7.1	Install SSL, NSS modules	Mod_ssl loaded	Modules Loaded
1.7.2	Install a valid trusted certificate	Load T-Mobile Root, Intermediate and Issuing Certs	T-mobile certs used for SSL/TLS CA Root certs loaded to the server config in ssl.conf.

1.7.3	Protect the Servers Private Key - 'httpd.conf SSLCertificateFile is a private key'	Store the private key in clear text so that a passphrase is not required.	Private key to owned by root:root with permission 0400.
1.7.4	Restrict weak SSL Protocols and Ciphers - 'httpd.conf SSLProtocol	Restrict weak SSL Protocols and Ciphers. Only TLS versions should be allowed	cat /etc/httpd/conf.d/ssl.conf | grep SSLProtocol SSLProtocol all -SSLv2 -SSLv3 - Added in ssl.conf
1.7.4	Restrict weak SSL Protocols and Ciphers - 'httpd.conf SSLHonorCipherOrder = On'	Restrict weak SSL Protocols and Ciphers - 'httpd.conf SSLHonorCipherOrder = On'	SSLHonorCipherOrder on in ssl.conf
1.7.4	Restrict weak SSL Protocols and Ciphers - 'httpd.conf VirtualHost SSLHonorCipherOrder = On	Restrict weak SSL Protocols and Ciphers - 'httpd.conf VirtualHost SSLHonorCipherOrder = On	SSLHonorCipherOrder On SSLCipherSuite ALL:!EXP:!NULL:!ADH:!LOW:!SSLv2:!SSLv3:!MD5:!RC4
1.7.5	Restrict Insecure SSL Renegotiation - 'httpd.conf SSLInsecureRenegotiation = off	/etc/httpd/conf/httpd.conf SSLInsecureRenegotiation = off	SSLInsecureRenegotiation = off
1.8.1	Limit Information in the Server Token - 'httpd.conf ServerTokens = Prod or ProductOnly	/etc/httpd/conf/httpd.conf ServerSignature Off ServerTokens Prod	ServerSignature Off ServerTokens Prod
1.8.2	Limit Information in the Server Signature - 'httpd.conf ServerSignature = Off	/etc/httpd/conf/httpd.conf ServerSignature Off	ServerSignature Off
1.9.1	Denial of Service Mitigation - 'httpd.conf Timeout < 10	Denial of Service Mitigation - 'httpd.conf Timeout < 10	Timeout 10
1.9.1	Denial of Service Mitigation - 'httpd.conf KeepAlive = On	Denial of Service Mitigation - 'httpd.conf KeepAlive = On	KeepAlive = On
1.9.1	Denial of Service Mitigation - 'httpd.conf MaxKeepAliveRequests > 100	Denial of Service Mitigation - 'httpd.conf MaxKeepAliveRequests > 100	MaxKeepAliveRequests > 100
1.9.1	Denial of Service Mitigation - 'httpd.conf KeepAliveTimeout < 15	Denial of Service Mitigation - 'httpd.conf KeepAliveTimeout < 15	KeepAliveTimeout < 15

1.5.11	Restrict File Extensions - 'httpd.conf <FilesMatch ''^.*$''> Order = allow,deny	R '/bin/sed -n '/<FilesMatch "\^\.*\$"/,/<\/FilesMatch>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Oo]rder\s+''	httpd.conf <FilesMatch ''^.*$''> Order = allow,deny (Got 443 forbidden error, if we applied this config)
1.5.11	Restrict File Extensions - 'httpd.conf <FilesMatch ''^.*$''> Deny from All exists	'/bin/sed -n '/<FilesMatch "\^\.*\$"/,/<\/FilesMatch>/p' /etc/httpd/conf/httpd.conf | /usr/bin/egrep '^\s*[Dd]eny\s+''	For all three 1.5.11 applied below config
1.5.11	Restrict File Extensions - 'httpd.conf approved extention <FilesMatch> directive exists	/etc/httpd/conf/httpd.conf	<FilesMatch "^.*\.(css|html?|js|pdf|txt|xml|xsl|gif|ico|jpe?g|png)$"> Order Deny,Allow Allow from all </FilesMatch>
1.8.3	Information Leakage via Default Apache Content - 'httpd.conf Include conf/extra/httpd-autoindex.conf does not exists	"/etc/httpd/conf/httpd.conf" "^[\s\t]*[Ii]nclude\s+conf\/extra\/httpd-autoindex\.conf\s*"	httpd.conf Include conf/extra/httpd-autoindex.conf has been removed
1.8.3	Information Leakage via Default Apache Content - 'httpd.conf Alias /icons/ ''/var/www/icons/''	httpd.conf Alias /icons/ ''/var/www/icons/''	Icon directive has been commented/disabled
1.8.3	Information Leakage via Default Apache Content - 'httpd.conf Directory ''/var/www/icons/'' does not exists	Information Leakage via Default Apache Content - 'httpd.conf Directory ''/var/www/icons/	Default Icon directive has been commented/disabled
1.9.2	Buffer Overflow Mitigation - 'httpd.conf LimitRequestline < 512	"/etc/httpd/conf/httpd.conf" LimitRequestline < 512	LimitRequestLine 512
1.9.2	Buffer Overflow Mitigation - 'httpd.conf LimitRequestFields < 100'	"/etc/httpd/conf/httpd.conf" LimitRequestFields < 100'	LimitRequestFields < 100'
1.9.2	Buffer Overflow Mitigation - 'httpd.conf LimitRequestFieldsize < 1024	"/etc/httpd/conf/httpd.conf" LimitRequestFieldsize 1024	LimitRequestFieldsize 1024
1.9.2	Buffer Overflow Mitigation - 'httpd.conf LimitRequestBody < 102400	"/etc/httpd/conf/httpd.conf" LimitRequestBody 102400	LimitRequestBody 102400
1.9.3	Restrict Listen Directive - 'httpd.conf Listen	Restrict listen 0.0.0.0:80	Directive - 'httpd.conf Listen 0.0.0.0:80 does not exists

	0.0.0.0:80 does not exists		
1.9.4	Restrict Browser Frame Options - 'httpd.conf X-Frame-Options SAMEORIGIN	Restrict Browser Frame Options - 'httpd.conf X-Frame-Options SAMEORIGIN	Header always append X-Frame-Options SAMEORIGIN

4. Reference

https://benchmarks.cisecurity.org/tools2/apache/CIS_Apache_HTTP_Server_Benchmark_v3.0.0.pdf