

EGA

e-Government Agency

Electronic Government Agency (Public Organization)
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

Apache Harden



APACHE
HTTP SERVER



APACHE
HTTP SERVER

Apache HTTP Server 2.4 Benchmark

Apache httpd 2.4.16 Released
2015-07-15



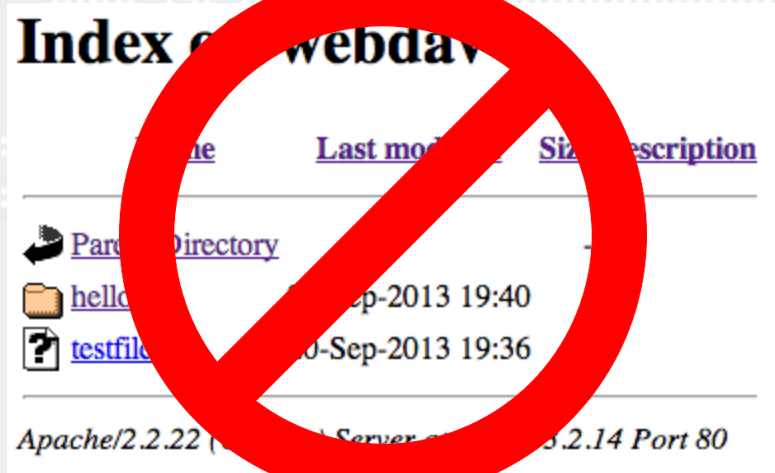
APACHE
HTTP SERVER

Enable the Log Config Module

```
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Cache-Control' => 'no-cache' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Connection' => 'keep-alive' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Pragma' => 'no-cache' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Accept' => 'application/json, text/javascript, */*; q=0.01' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Accept-Encoding' => 'gzip, deflate' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Accept-Language' => 'en-gb,en;q=0.5' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Host' => 'vx-garcia.wcn.co.uk' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Referer' => 'http://vx-garcia.wcn.co.uk/vx/lang-en-GB/config-jail/channel-1/system-51/brand-2/user-1/xf-cbf4d27dad84/wid-4/ats/recruiter/profile/edit' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'User-Agent' => 'Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/17.0 Firefox/17.0' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Content-Length' => '134' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Content-Type' => 'application/x-www-form-urlencoded; charset=UTF-8' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'Cookie' => 'utma=1.893613000.1353586388.1356003545.1356012074.105; utmc=1.1353586388.1.1.utmcsrc=(direct)
[utmccn=(direct)|utmcmd=(none); utma=164338489.1362821095.1354014424.1354641679.1355835790.3; utmc=164338489.1355835790.3.3.utmcsrc=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20p
rovided); wcn_session=000097a096228f7b2bdfa454194513879815e69871128c680440ee76ee108d9d39d6c44ddd261d1d4f1a; utmc=1; su_user=0; utmb=1.89.9.1356016597942; wcn_session=00007fc8285376
9ec1126766805e5e2137f801ea5d9ad42d9f35dclf31f70a566bb922e61ace6f080f6' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 158] 'X-Requested-With' => 'XMLHttpRequest' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 4] [WCN.Role.PathMunge 173] In parse_url() - user requested access to 'vx-garcia.wcn.co.uk', 'lang-en-GB/config-jail/channel-1/system-51/brand-2/user-1/xf-cbf4d27dad84/wid-4/ats/recruiter/profile/map_update/1'
[Thu Dec 20 15:41:01 2012] [notice] Apache/2.2.16 (Debian) mod_perl/2.0.4 Perl/v5.10.1 configured -- resuming normal operations
[INFO] [47152f7f] [2012/12/20 15:41:01 48] [WCN.Role.PathMunge 747] c->set_system: 51 (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.DBIC 388] Going to set system database to system '51', jail '1'
[INFO] [47152f7f] [2012/12/20 15:41:01 36] [WCN.Role.PathMunge 718] Setting brand to be '2'
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PathMunge 791] Set current language to 'en-GB'
[DEBUG] [47152f7f] [2012/12/20 15:41:01 2] [WCN.Role.PathMunge 319] Cookie for 'recruiter' => '97a096228f7b2bdfa454194513879815e6987112
[DEBUG] [47152f7f] [2012/12/20 15:41:01 6] [WCN.Role.PerformanceLogger 175] *** Request Params (4) ***
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 189] 'vxXSRF Token' => '4ddc5de6bed3d3760b59c430cbeae48a6f0c8e95' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 189] 'code version' => '1355995679' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 189] 'submitted via ajax' => 'true' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 189] 'datafield_53274_1_1[]' => '1798' (1)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 193] *** Uploads (0) ***
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 215] PERFORMANCE: prepare took 0.115999937057495 secs
[DEBUG] [47152f7f] [2012/12/20 15:41:01 1] [WCN.Role.Session 142] User's session id is '97a096228f7b2bdfa454194513879815e6987112', on server '0'
[DEBUG] [47152f7f] [2012/12/20 15:41:01 17] [WCN.AccessControl 233] Going to _cache_role_profile_rules for recruiter '1', role profile '20'
[DEBUG] [47152f7f] [2012/12/20 15:41:01 16] [WCN.Controller.Root 64] ** Enter root auto
[INFO] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Controller.Root 65] ** User requested access to 'ats/recruiter/profile/map_update/1' from '192.168.146.46'
[DEBUG] [47152f7f] [2012/12/20 15:41:01 10] [WCN.Role.Session 347] Loading session flash
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Controller.Root 219] ** About to return 1 from root auto
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Controller.ATS 61] ** Enter ATS auto
[DEBUG] [47152f7f] [2012/12/20 15:41:01 1] [WCN.Controller.ATS 145] User 'WCN::DBIC::Recruiter=HASH(0x7f9b16810610)' (id: 1) logged in
[DEBUG] [47152f7f] [2012/12/20 15:41:01 1] [WCN.Controller.ATS 950] Validate ATS access rights for recruiter '1' to path 'ats/recruiter/profile/map_update/1' in system '51'
[WARN] [47152f7f] [2012/12/20 15:41:01 37] [WCN.Controller.ATS 988] User '' does not have access to path 'ats/recruiter/profile/map_update - ACCESS DENIED'
[ERROR] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.Controller.BadRequest 104] 403 FORBIDDEN
[DEBUG] [47152f7f] [2012/12/20 15:41:01 1] [WCN.Controller.Root 324] **** enter root controller's end() method
[INFO] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Controller.Root 339] Have already set status (403) and set a body, so will not render any templates
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Controller.Root 376] Set Content-Length header => '1' bytes
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 231] PERFORMANCE: dispatch finished at 0.209099595489502 secs (took: 0.0930960178375244 secs)
[DEBUG] [47152f7f] [2012/12/20 15:41:01 4] [WCN.Role.PerformanceLogger 249] PERFORMANCE: finalize finished at 0.213540077209473 secs (took: 0.0044412231445312 secs) for url 'ats/recruiter/profile/map_update/1'
[DEBUG] [47152f7f] [2012/12/20 15:41:01 0] [WCN.Role.PerformanceLogger 266] PERFORMANCE: SQL query count: 'SELECT' => 15, 'SET' => 4
[DEBUG] [47152f7f] [2012/12/20 15:41:01 2] [WCN.Role.PerformanceLogger 274] PERFORMANCE: SAN calls: '0' total: '0' avg: '0'
```



Disable WebDAV Modules











↓
httpd.conf


↓
##LoadModule dav_module modules/mod_dav.so
##LoadModule dav_fs_module modules/mod_dav_fs.so



Disable Status Module

 apr.apache.org	29572	_	53	GET /docs/apr-util/trunk/apr__strmatch_8h.html HTTP/1.0
archive.apache.org	1845	_	61	GET /dist/tomcat/tomcat-3/archive/v3.2.1/bin/win32/i386/?C=D;O=
	20257	W	366	GET /dist/xml/batik/batik-1.5beta3.zip HTTP/1.0
	5643	K	2	GET / HTTP/1.1
	5643	_	95	GET /dist/james/server/binaries/james-2.3.0.zip HTTP/1.1
	29572	C	0	GET /dist/tomcat/tomcat-4/archive/v4.0.1/bin/linux/i386/?C=M;O=
	1845	W	39	GET /dist/james/server/binaries/james-2.3.0.zip HTTP/1.1
	1845	_	38	GET /gnats/6760 HTTP/1.0
 bugs.apache.org	29572	_	10	GET /robots.txt HTTP/1.0
cocoon.apache.org	5643	K	2	GET /skin/images/page.gif HTTP/1.1
	1845	W	0	GET /mirror.cgi?Preferred=http://www.axint.net/apache HTTP/1.1
	29572	_	45	GET /2.1/apidocs/org/apache/cocoon/woody/acting/package-tree.ht
	1845	K	2	GET /skin/images/chapter.gif HTTP/1.1
	1845	_	22	GET /2.1/changes.rss HTTP/1.1
	29572	_	34	GET /2.1/apidocs/org/apache/cocoon/components/language/markup/L
 excalibur.apache.org	1845	K	0	GET /robots.txt HTTP/1.1
 forrest.apache.org	5643	_	107	GET /docs_0_80/build.html HTTP/1.1
geronimo.apache.org	29572	_	66	GET /images/menu_bgstretch_1x22.gif HTTP/1.1
	1845	_	43	GET /maven/server/maven-plugins/car-maven-plugin/issue-tracking
 harmony.apache.org	29572	_	74	GET /site.css HTTP/1.1

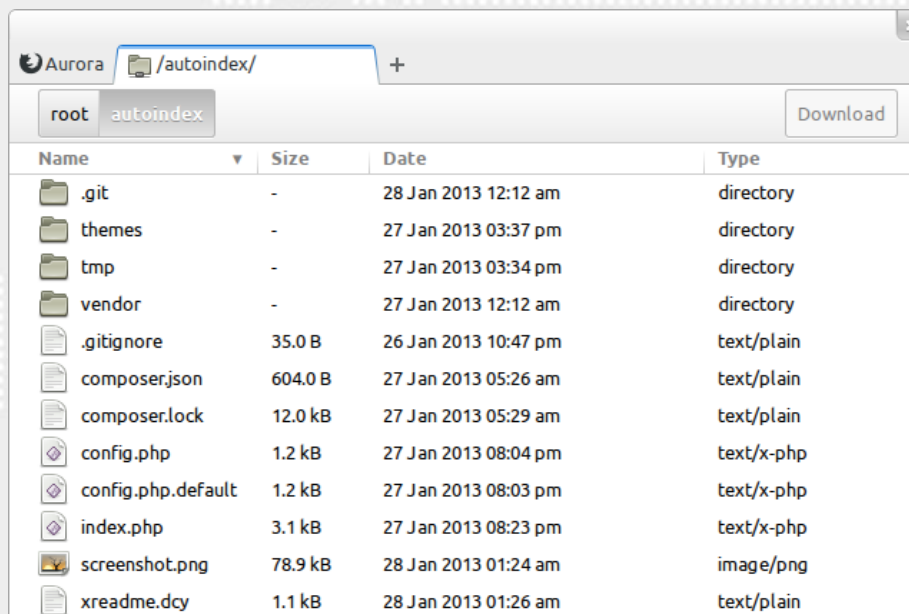
httpd.conf

 `##LoadModule status_module modules/mod_status.so`

http://httpd.apache.org/docs/2.4/mod/mod_status.html



Disable Autoindex Module



Name	Size	Date	Type
.git	-	28 Jan 2013 12:12 am	directory
themes	-	27 Jan 2013 03:37 pm	directory
tmp	-	27 Jan 2013 03:34 pm	directory
vendor	-	27 Jan 2013 12:12 am	directory
.gitignore	35.0 B	26 Jan 2013 10:47 pm	text/plain
composer.json	604.0 B	27 Jan 2013 05:26 am	text/plain
composer.lock	12.0 kB	27 Jan 2013 05:29 am	text/plain
config.php	1.2 kB	27 Jan 2013 08:04 pm	text/x-php
config.php.default	1.2 kB	27 Jan 2013 08:03 pm	text/x-php
index.php	3.1 kB	27 Jan 2013 08:23 pm	text/x-php
screenshot.png	78.9 kB	28 Jan 2013 01:24 am	image/png
xreadme.dcy	1.1 kB	28 Jan 2013 01:26 am	text/plain

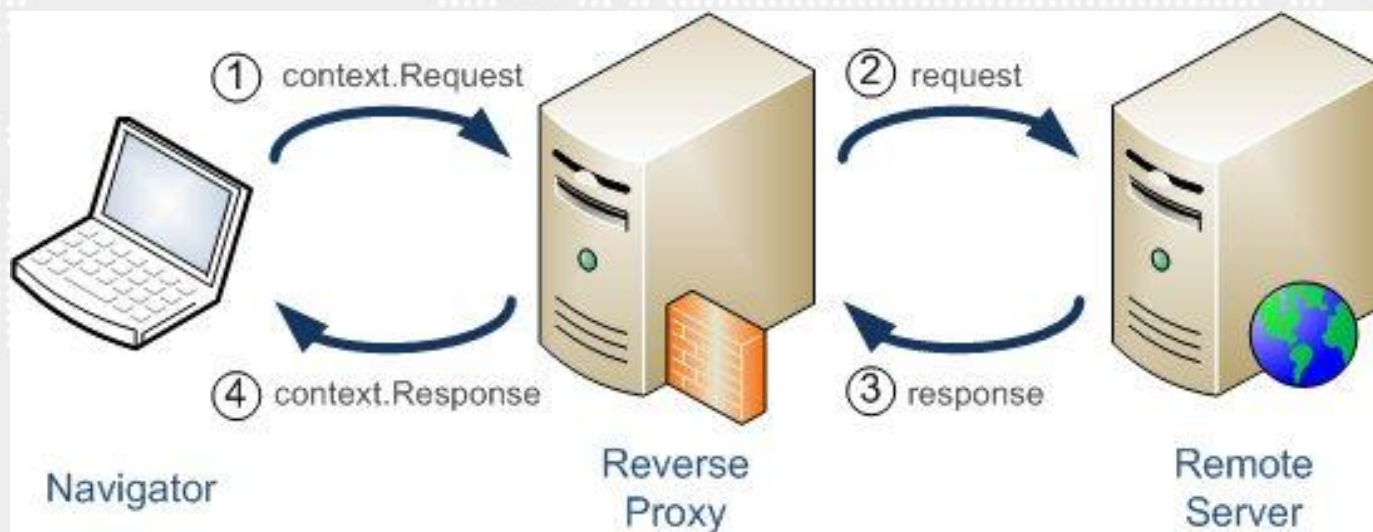
httpd.conf

↳ `## LoadModule autoindex_module modules/mod_autoindex.so`

http://httpd.apache.org/docs/2.4/mod/mod_autoindex.html



Disable Proxy Modules



httpd.conf

```
↳ ##LoadModule proxy_module modules/mod_proxy.so  
##LoadModule proxy_connect_module modules/mod_proxy_connect.so  
##LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
```

http://httpd.apache.org/docs/2.4/mod/mod_autoindex.html




Disable User Directories Modules(~)

`http://example.com/~ralph/` might access a `public_html` sub-directory of ralph user's home directory.

The directive `UserDir ./` might map `/~root` to the root directory (`/`).

`httpd.conf`

 `##LoadModule userdir_module modules/mod_userdir.so`



Disable Info Module

<http://your.host.example.com/server-info>

```
Apache Server Information

Subpages:
Configuration Files, Server Settings, Module List, Active Hooks

Sections:
Server Settings, Startup Hooks, Request Hooks

Loaded Modules:
mod\_ssl.c, mod\_python.c, mod\_proxy\_ajp.c, mod\_php5.c, mod\_perl.c, mod\_fcgid.c,
mod\_version.c, mod\_cgi.c, mod\_mem\_cache.c, mod\_file\_cache.c, mod\_disk\_cache.c,
mod\_suexec.c, mod\_cache.c, mod\_proxy\_connect.c, mod\_proxy\_http.c, mod\_proxy\_ftp.c,
mod\_proxy\_balancer.c, mod\_proxy.c, mod\_rewrite.c, mod\_alias.c, mod\_userdir.c,
mod\_speling.c, mod\_actions.c, mod\_dir.c, mod\_negotiation.c, mod\_vhost\_alias.c,
mod\_dav\_fs.c, mod\_info.c, mod\_autoindex.c, mod\_status.c, mod\_dav.c, mod\_mime.c,
mod\_setenvif.c, mod\_usertrack.c, mod\_headers.c, mod\_deflate.c, mod\_expires.c,
mod\_mime\_magic.c, mod\_ext\_filter.c, mod\_env.c, mod\_logio.c, mod\_log\_config.c,
mod\_include.c, mod\_authnz\_ldap.c, util\_ldap.c, mod\_authz\_default.c,
mod\_authz\_dbm.c, mod\_authz\_groupfile.c, mod\_authz\_owner.c, mod\_authz\_user.c,
mod\_authz\_host.c, mod\_authn\_default.c, mod\_authn\_dbm.c, mod\_authn\_anon.c,
mod\_authn\_alias.c, mod\_authn\_file.c, mod\_auth\_digest.c, mod\_auth\_basic.c, mod\_soc.c,
http\_core.c, prefork.c, core.c

Server Settings

Server Version: Apache/2.2.19 (Unix) DAV/2 mod_fcgid/2.3.6
mod_python/3.2.8 Python/2.4.3 mod_ssl/2.2.19 OpenSSL/0.9.8f
mod_perl/2.0.4 Perl/v5.8.8
Server Built: Jul 20 2011 10:24:27
Server loaded APR Version: 1.2.7
Compiled with APR Version: 1.2.7
Server loaded APU Version: 1.2.7
Compiled with APU Version: 1.2.7
Module Magic Number: 20051115:28
Hostname/port: www.landhelp.com
Timeouts: connection: 120 keep-alive: 15
MPM Name: Prefork
MPM Information: Max Daemons: 256 Threaded: no Forked: yes
Server Architecture: 64-bit
Server Root: /etc/httpd
```

httpd.conf

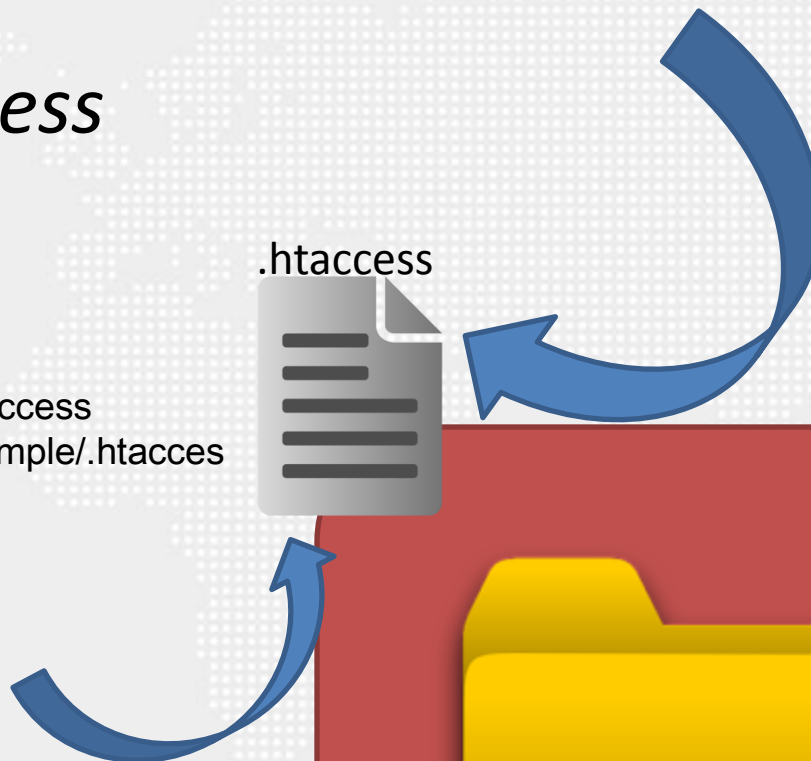
↳ `##LoadModule info_module modules/mod_info.so`

http://httpd.apache.org/docs/2.4/mod/mod_info.html



.htaccess

```
/.htaccess  
/www/.htaccess  
/www/htdocs/.htaccess  
/www/htdocs/example/.htaccess
```



Custom Directory Index Files
Custom Error Pages
Control access at files & directory level

•
••
•••

Secret Directory



10 Best Practices To Secure and Harden Your Apache Web Server

1. Disable Trace HTTP Request
2. Run as separate User & Group
3. Disable Signature
4. Disable Banner
5. Restrict Access to a Specific Network or IP
6. Use only TLS, Disable SSLv2, SSLv3
7. Disable Directory Listing
8. Remove unnecessary DSO Modules
9. Disable Null and Weak Ciphers
10. Stay Current

Thank You

Electronic Government Agency (Public Organization)

website : www.ega.or.th
e-mail : helpdesk@ega.or.th
Tel. : (+66) 0 2612 6000
Hotline : (+66) 0 2612 6060

