4/13/18

Apache Http Server Sniffing Problem Resolved

Problem: A program or script coming in every often with different IP addresses crawling through all dir stupidly looking for */scripts/setup.php. Below is an example from Apache access log file.

188.166.91.145 - - [10/Apr/2018:17:46:52 -0400] "GET /muieblackcat HTTP/1.1" 302 213
188.166.91.145 - - [10/Apr/2018:17:46:52 -0400] "GET //phpMyAdmin/scripts/setup.php HTTP/1.1" 302 229
188.166.91.145 - - [10/Apr/2018:17:46:52 -0400] "GET //phpmyadmin/scripts/setup.php HTTP/1.1" 302 229
188.166.91.145 - - [10/Apr/2018:17:46:53 -0400] "GET //pma/scripts/setup.php HTTP/1.1" 302 222
188.166.91.145 - - [10/Apr/2018:17:46:53 -0400] "GET //pMa/scripts/setup.php HTTP/1.1" 302 222
188.166.91.145 - - [10/Apr/2018:17:46:53 -0400] "GET //PMA/scripts/setup.php HTTP/1.1" 302 222
188.166.91.145 - - [10/Apr/2018:17:46:53 -0400] "GET //PMA2009/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:53 -0400] "GET //PMA2010/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:54 -0400] "GET //PMA2011/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:54 -0400] "GET //PMA2013/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:54 -0400] "GET //PMA2014/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:54 -0400] "GET //PMA2015/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:54 -0400] "GET //myadmin/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:55 -0400] "GET //MyAdmin/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:55 -0400] "GET //scripts/setup.php HTTP/1.1" 302 218
188.166.91.145 - - [10/Apr/2018:17:46:55 -0400] "GET //admin/scripts/setup.php HTTP/1.1" 302 224
188.166.91.145 - - [10/Apr/2018:17:46:55 -0400] "GET //admin/pma/scripts/setup.php HTTP/1.1" 302 228
188.166.91.145 - - [10/Apr/2018:17:46:56 -0400] "GET //admin/phpmyadmin/scripts/setup.php HTTP/1.1" 302 235
188.166.91.145 - - [10/Apr/2018:17:46:56 -0400] "GET //db/scripts/setup.php HTTP/1.1" 302 221
188.166.91.145 - - [10/Apr/2018:17:46:56 -0400] "GET //dbadmin/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:56 -0400] "GET //myadmin/scripts/setup.php HTTP/1.1" 302 226
188.166.91.145 - - [10/Apr/2018:17:46:56 -0400] "GET //mysql/scripts/setup.php HTTP/1.1" 302 224
188.166.91.145 - - [10/Apr/2018:17:46:57 -0400] "GET //mysqladmin/scripts/setup.php HTTP/1.1" 302 229
188.166.91.145 - - [10/Apr/2018:17:46:57 -0400] "GET //typo3/phpmyadmin/scripts/setup.php HTTP/1.1" 302 235
188.166.91.145 - - [10/Apr/2018:17:46:57 -0400] "GET //web/scripts/setup.php HTTP/1.1" 302 222
188.166.91.145 - - [10/Apr/2018:17:46:57 -0400] "GET //websql/scripts/setup.php HTTP/1.1" 302 225
188.166.91.145 - - [10/Apr/2018:17:46:57 -0400] "GET / HTTP/1.1" 302 201

76.74.178.171 - - [11/Apr/2018:23:03:05 -0400] "GET /w00tw00t.at.blackhats.romanian.anti-sec:) HTTP/1.1" 302 242
76.74.178.171 - - [11/Apr/2018:23:03:06 -0400] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 302 229
76.74.178.171 - - [11/Apr/2018:23:03:06 -0400] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 302 229
76.74.178.171 - - [11/Apr/2018:23:03:06 -0400] "GET /pma/scripts/setup.php HTTP/1.1" 302 222
76.74.178.171 - - [11/Apr/2018:23:03:06 -0400] "GET /myadmin/scripts/setup.php HTTP/1.1" 302 226
76.74.178.171 - - [11/Apr/2018:23:03:06 -0400] "GET /MyAdmin/scripts/setup.php HTTP/1.1" 302 226
76.74.178.171 - - [11/Apr/2018:23:03:06 -0400] "GET /scripts/setup.php HTTP/1.1" 302 218
76.74.178.171 - - [11/Apr/2018:23:03:07 -0400] "GET /admin/scripts/setup.php HTTP/1.1" 302 224
76.74.178.171 - - [11/Apr/2018:23:03:07 -0400] "GET /admin/pma/scripts/setup.php HTTP/1.1" 302 228
76.74.178.171 - - [11/Apr/2018:23:03:07 -0400] "GET /admin/phpmyadmin/scripts/setup.php HTTP/1.1" 302 235
76.74.178.171 - - [11/Apr/2018:23:03:07 -0400] "GET /db/scripts/setup.php HTTP/1.1" 302 221
76.74.178.171 - - [11/Apr/2018:23:03:07 -0400] "GET /dbadmin/scripts/setup.php HTTP/1.1" 302 226
76.74.178.171 - - [11/Apr/2018:23:03:08 -0400] "GET /myadmin/scripts/setup.php HTTP/1.1" 302 226
76.74.178.171 - - [11/Apr/2018:23:03:08 -0400] "GET /mysql/scripts/setup.php HTTP/1.1" 302 224
76.74.178.171 - - [11/Apr/2018:23:03:08 -0400] "GET /mysqladmin/scripts/setup.php HTTP/1.1" 302 229
76.74.178.171 - - [11/Apr/2018:23:03:08 -0400] "GET /typo3/phpmyadmin/scripts/setup.php HTTP/1.1" 302 235
76.74.178.171 - - [11/Apr/2018:23:03:08 -0400] "GET /phpadmin/scripts/setup.php HTTP/1.1" 302 227
76.74.178.171 - - [11/Apr/2018:23:03:08 -0400] "GET /pma/scripts/setup.php HTTP/1.1" 302 222
76.74.178.171 - - [11/Apr/2018:23:03:09 -0400] "GET /web/phpMyAdmin/scripts/setup.php HTTP/1.1" 302 233
76.74.178.171 - - [11/Apr/2018:23:03:09 -0400] "GET /xampp/phpmyadmin/scripts/setup.php HTTP/1.1" 302 235
76.74.178.171 - - [11/Apr/2018:23:03:09 -0400] "GET /web/scripts/setup.php HTTP/1.1" 302 222
76.74.178.171 - - [11/Apr/2018:23:03:09 -0400] "GET /php-my-admin/scripts/setup.php HTTP/1.1" 302 231
76.74.178.171 - - [11/Apr/2018:23:03:09 -0400] "GET /websql/scripts/setup.php HTTP/1.1" 302 225
76.74.178.171 - - [11/Apr/2018:23:03:10 -0400] "GET /phpMyAdmin-2/scripts/setup.php HTTP/1.1" 302 231
76.74.178.171 - - [11/Apr/2018:23:03:10 -0400] "GET /_phpmyadmin/scripts/setup.php HTTP/1.1" 302 230
76.74.178.171 - - [11/Apr/2018:23:03:10 -0400] "GET /php/phpmyadmin/scripts/setup.php HTTP/1.1" 302 233

76.74.178.171 - - [11/Apr/2018:23:03:10 -0400] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 302 229
76.74.178.171 - - [11/Apr/2018:23:03:10 -0400] "GET /phpMyAdmin3/scripts/setup.php HTTP/1.1" 302 230

Solution: Go download mod_security-2.9.2-win64-VC15.zip
from http://www.apachelounge.com/download/. Install with instructions in the package and no one will be able to iterate through your web server anymore.

How do we test whether some program or a script can iterate through our web sites?

Visit any web site URL with "http://www.xxxx.com/?abc=../../"

Just replace www.xxxx.com with real URL. If anything comes up, like a home page or anything, then that website security isn't good.

After securing with Mod Security, you should get:

Forbidden

You don't have permission to access / on this server.

When you try that sniffing dir method above.

Mod security is a very recent Apache security module, 20 July 2017. I am amaze its other capabilities, such as help with wordpress, cpanel, oscommerce, and etc many popular web solution packages's vulnerabilities could be all addressed with it.

-Christopher McGrath