

## access\_log\*

**What application do the logs come from?**

**What are the dates, which are represented by the logs?** Dec 8 - Dec 13, 2013

**How many unique IP addresses appear?** 192

**What was the largest file export logged? And does it look out of the ordinary?** 8444bytes. There are three occurrences, 2 on the 9th and one on the 10th.

216.244.85.11 - - [09/Dec/2013:23:34:00 +0000] "POST /?q=user HTTP/1.0" 200 8444 "http://clinical-security.com/?q=user" "Mozilla/5.0 (Windows NT 5.1; rv:14.0) Gecko/20100101 Firefox/14.0.1"

**What is the most common error found in the error logs?** There were 456 / 200 or Success Codes

**Do you see anything, which is out of the ordinary?**

109.163.229.59 - - [10/Dec/2013:12:04:28 +0000] "POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F"

The above could be a possible exploitation to run code from an arbitrary server. It occurs about 4-5 times if I recall correctly through out this particular log.

**Write a short synopsis of what you found.**

## access\_log-20131117

**What application do the logs come from?**

**What are the dates which are represented by the logs?** 10/Nov/2013 – 17/Nov/2013

**How many unique IP addresses appear?** There are 414 unique IP addresses

**What was the largest file export logged? and does it look out of the ordinary?** 8475bytes

**What is the most common error found in the error logs?** 1415 - 200 or Success Codes

## access\_log-20131124\*

**What application do the logs come from?**

**What are the dates which are represented by the logs?** The dates are 17/Nov/2013 - 24/Nov/2013

**How many unique IP addresses appear?** 393 Unique IP Addresses

**What was the largest file export logged? and does it look out of the ordinary?** 8475b

**What is the most common error found in the error logs?** 1243 - 200 or Success Codes

## access\_log-20131201

**What application do the logs come from?**

**What are the dates which are represented by the logs?** 24/Nov/2013 - 01/Dec/2013

**How many unique IP addresses appear?** 398 Unique IP Addresses

**What was the largest file export logged? and does it look out of the ordinary?** 8444b

**What is the most common error found in the error logs?** 1199 - 200 or Success Codes

## access\_log-20131208

**What application do the logs come from?**

**What are the dates which are represented by the logs?** 01/Dec/2013 - 08/Dec/2013

**How many unique IP addresses appear?** 382 Unique IP Addresses

**What was the largest file export logged? and does it look out of the ordinary?** 8444b

**What is the most common error found in the error logs?** 1241 - 200 or Success Codes

## error\_log

**What application do the logs come from?** Apache/2.2.15 (Unix) DAV/2 PHP/5.3.3 configured

**What are the dates which are represented by the logs?** Sun Dec 8, 2013 - Tue Dec 10, 2013

**How many unique IP addresses appear?** 16 Unique Ip Addresses

**What was the largest file export logged? and does it look out of the ordinary?** N/A

**What is the most common error found in the error logs** 20 File does not exist and 20 script not found or unable to stat

## error\_log-20131117

**What application do the logs come from?** Apache/2.2.15 (Unix) DAV/2 PHP/5.3.3 configured

**What are the dates which are represented by the logs?** Sun Nov 10, 2013 - Sun Nov 17, 2013

**How many unique IP addresses appear?** 31 Unique IP addresses

**What was the largest file export logged? and does it look out of the ordinary?** N/A

**What is the most common error found in the error logs?** 36 File Does not exist

## error\_log-20131124

**What application do the logs come from?** Apache/2.2.15 (Unix) DAV/2 PHP/5.3.3 configured

**What are the dates which are represented by the logs?** Sun Nov 17, 2013 - Sun Nov 24, 2013

**How many unique IP addresses appear?** 32 unique IP Addresses

**What was the largest file export logged? and does it look out of the ordinary?** N/A

**What is the most common error found in the error logs?** 164 File Does Not Exist

**Do you see anything which is out of the ordinary?** There appears to be some sort of memory management issue bug that is throwing a log of gib c, backtrace etc errors on top of the normal content of the logs.

## error\_log-20131201

**What application do the logs come from?** Apache/2.2.15 (Unix) DAV/2 PHP/5.3.3 configured

**What are the dates which are represented by the logs?** Sun Nov 24, 2013 - Sun Dec 1, 2013

**How many unique IP addresses appear?** 40 unique IP addresses

**What was the largest file export logged? and does it look out of the ordinary?** N/A

**What is the most common error found in the error logs?** 139 File does not exist

**Do you see anything which is out of the ordinary?** Yes, this again "[Sun Dec 01 03:29:13 2013] [notice] SIGHUP received. Attempting to restart which occurs when the connection is severed generally by the hanging up of the modem

## error\_log-20131208

**What application do the logs come from?** Apache/2.2.15 (Unix) DAV/2 PHP/5.3.3 configured

**What are the dates which are represented by the logs ?** Sun Dec 1, 2013 - Sun Dec 8, 2013

**How many unique IP addresses appear?** 32 unique IP addresses

**What was the largest file export logged? and does it look out of the ordinary?** N/A

**What is the most common error found in the error logs?** 235 File Does Not Exist

**Do you see anything which is out of the ordinary?** appears to be a Wordpress site

## Messages

**What application do the logs come from?** IMKLOG - origin software="rsyslogd" swVersion="4.6.2" x-pid="917" x-info="http://www.rsyslog.com"

**What are the dates which are represented by the logs?** Dec 8 - Dec 10

**How many unique IP addresses appear?** 241 unique IP addresses

**What was the largest file export logged? and does it look out of the ordinary?** n/a

**What is the most common error found in the error logs?** n/a

**Do you see anything which is out of the ordinary?** It's a kernel log

# Secure

**What application do the logs come from?**

**What are the dates which are represented by the logs?** Dec 8 - Dec 10

**How many unique IP addresses appear?** 20 unique IP addresses

**What was the largest file export logged? and does it look out of the ordinary?** n/a

**What is the most common error found in the error logs?** Failed passwords

**Do you see anything which is out of the ordinary?**

9 Sudo User: Super User Counts

628 Invalid users

2858 Failed Passwords

511 Break - In Attempts