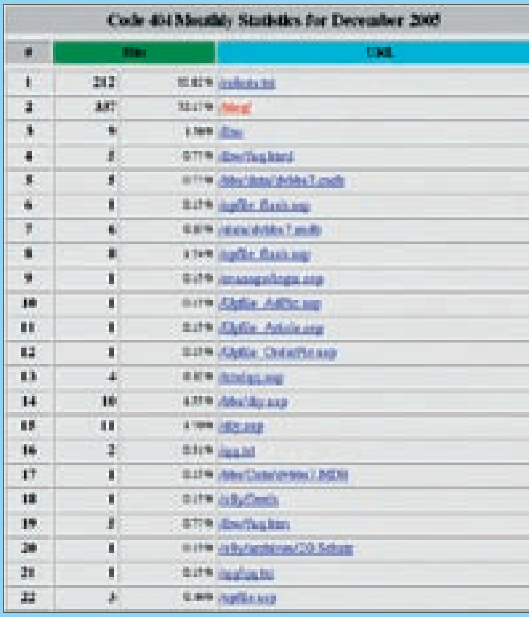
The Sysadmin's Daily Grind: Webalizer Xtended

WRONG NUMBER!

Webalizer is a tool for analyzing web server logfiles. A new patch lets admins see what isn't there. **BY CHARLY KÜHNAST**



Code 404 Monthly Statistics for December 2005

#	Hits		URL
1	212	[illegible]	[illegible]
2	487	[illegible]	[illegible]
3	9	[illegible]	[illegible]
4	2	[illegible]	[illegible]
5	2	[illegible]	[illegible]
6	1	[illegible]	[illegible]
7	6	[illegible]	[illegible]
8	8	[illegible]	[illegible]
9	1	[illegible]	[illegible]
10	1	[illegible]	[illegible]
11	1	[illegible]	[illegible]
12	1	[illegible]	[illegible]
13	4	[illegible]	[illegible]
14	10	[illegible]	[illegible]
15	11	[illegible]	[illegible]
16	2	[illegible]	[illegible]
17	1	[illegible]	[illegible]
18	1	[illegible]	[illegible]
19	2	[illegible]	[illegible]
20	1	[illegible]	[illegible]
21	1	[illegible]	[illegible]
22	3	[illegible]	[illegible]

Figure 1: Webalizer Xtended showing the wrong-number statistics for December 6.

From time to time, I browse my web server logfiles, although this isn't something I like to do too often. After all, I get to see enough of the pesky things at work. When I do check my own logs, it typically has to do with debugging, but I also tend to find "wrong number" type entries. Sometimes you get strange entries like:

```
tharis.xxxxx.at - - ➘
[03/Dec/2005:08:24:43
 +0100] „GET /LOST HTTP/1.1“ ➘
404 1025 „-“
 „Mozilla/4.0“
```

Although this message looks pretty offensive, it is actually quite harmless. On other occasions, I find people attempting to navigate to URLs belonging to applications that have been featured in recent security advisories. In the past few weeks, for example, I have read advisories concerning PhpMyAdmin and PhpBB. Attempts to access files with suffixes such as *.mdb* and *.asp*, are telltale signs of unfriendly fire. Listing 1 shows an excerpt.

It is good to know exactly which queries against your server have drawn blanks. In fact, this is a way of discovering attack patterns that might cause other servers some headaches.

Detecting 404 Patterns

Enter Webalizer, the admin's friend. Patrick Frei has written a patch for Webalizer that gives admins additional statistics concerning requests that triggered a *404 - File not found* response from the server. Figure 1 shows these statistics for my web server from December 6, 2005. You can see at a glance that the entries I discovered are not just isolated cases. You can also see a couple of dead links I will need to remove.

The Webalizer source code (including the applied patch) is available from [1]. Just do the following to build and install:

```
./configure
make
make install
```

You will need the Zlib, Libpng, and GD packages, along with the matching devel packages. A patch that converts the original Webalizer source code to "Webalizer Xtended" is available at [1]. To apply the patch, change to the Webalizer source code directory and give the following command:

```
patch -Np1 -i /Pfad
/webalizer-2.01-10-RB06-patch
```

Listing 1: Web Server Access

```
01 cncln.online.ln.cn - - [05/
   Dec/2005:22:09:04 +0100] „GET
   /bbs/upload.asp?action=upfile
   HTTP/1.1“ 404 1025 „-“
   „InetURL:/1.0“
02 58.241.228.180 - - [06/
   Dec/2005:03:32:54 +0100] „GET
   /bbs/diy.asp HTTP/1.1“ 404
   1025 „-“ „Mozilla/4.0“
03 222.62.228.179 - - [06/
   Dec/2005:07:19:49 +0100] „GET
   /bbs/diy.asp HTTP/1.1“ 404
   1025 „-“ „InetURL:/1.0“
04 220.191.42.203 - - [13/
   Oct/2005:10:12:23 +0200] „GET
   /data/dvbbs6.mdb HTTP/1.1“ 404
   1025 „-“ „InetURL:/1.0“
05 220.191.42.203 - - [13/
   Oct/2005:10:12:24 +0200] „GET
   /data/dvbbs7.mdb HTTP/1.1“ 404
   1025 „-“ „InetURL:/1.0“
```

Then go on to build Webalizer as described previously. The whole thing is even easier for Gentoo users, as a ready-to-run Ebuild is available. Happy wrong numbers! ■

INFO

[1] Webalizer Xtended: *http://www.webalizer.go.to*

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data-center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).