

Forum:[Hack Forums](#)

Thread: [\[Team OpenFire\] IBM Research Blown.](#)

pwntoken - *January 11, 2012, 1:51 pm*

IBM Research Hacked

Coded32 was There !

Version: 5.0.67

User: root@localhost

Database: researcher_development

Datadir: /Applications/xampp/xamppfiles/var/mysql/

All databases:

Code information_schema

bluebase

cdcol

mysql

researcher_development

testTables from main database "researcher_development":

Code group_types

groups

locations

navbar_entries

publication_authors

publications

redirects

research_areas

researcher_group_entries

researcher_navbar_entries

researchersTables from "bluebase" database:

Code activity

auth_group

auth_group_permissions

auth_message

auth_permission

auth_user

auth_user_groups

auth_user_user_permissions

bluecomments_bluecomment

bluecomments_bluekarmascore

bluecomments_bluemoderatordeletion

bluecomments_blueuserflag

comments_comment

comments_freecomment

comments_karmascore

comments_moderatordeletion
comments_userflag
django_admin_log
django_content_type
django_session
django_site
projects_appacademy08
projects_application
projects_application_members
projects_application_moderators
projects_application_restrict
projects_appspeaker
projects_changelog
projects_document
projects_notespdb
projects_patent
projects_patent_authors
projects_person
projects_pic
projects_pic_chairs
projects_project
projects_project_application
projects_project_contacts
projects_project_docs
projects_project_linemangers
projects_project_members
projects_project_pics
projects_project_reviewers
projects_project_tags
projects_publication
projects_publication_authors
projects_pubstat
projects_restriction
projects_restriction_access_list
projects_tag
projects_useractivity
tag
tagged_item
votesAccounts from "auth_user" table:

Code er2008 : sha1\$9b957\$e6294a9dbf3f94c4e1ebbd010d2a3562d3f29a15 |
[color=#1E90FF]hash cracked:[/color] review
haixun : sha1\$b1367\$728086dd648468598b8d070b82f16136b011be1d | hash cracked: lapid
The account from "mysql.user":

Code root : *F9F9C3D7DD04044668ABBFA629CE289E02F7A918 | [color=#1E90FF]hash
cracked:[/color] godiva12

Here we can see the "/etc/passwd":

Quote: # User Database

#

Note that this file is consulted directly only when the system is running
in single-user mode. At other times this information is provided by
Open Directory.

```

#
# This file will not be consulted for authentication unless the BSD local node
# is enabled via /Applications/Utilities/Directory Utility.app
#
# See the DirectoryService(8) man page for additional information about
# Open Directory.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
_lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
_postfix:*:27:27:Postfix Mail Server:/var/spool/postfix:/usr/bin/false
_mcxalr:*:54:54:MCX AppLaunch:/var/empty:/usr/bin/false
_pcastagent:*:55:55:Podcast Producer Agent:/var/pcast/agent:/usr/bin/false
_pcastserver:*:56:56:Podcast Producer Server:/var/pcast/server:/usr/bin/false
_serialnumberd:*:58:58:Serial Number Daemon:/var/empty:/usr/bin/false
_devdocs:*:59:59:Developer Documentation:/var/empty:/usr/bin/false
_sandbox:*:60:60:Seatbelt:/var/empty:/usr/bin/false
_mdnsresponder:*:65:65:mDNSResponder:/var/empty:/usr/bin/false
_ard:*:67:67:Apple Remote Desktop:/var/empty:/usr/bin/false
_www:*:70:70:World Wide Web Server:/Library/WebServer:/usr/bin/false
_eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false
_cvs:*:72:72:CVS Server:/var/empty:/usr/bin/false
_svn:*:73:73:SVN Server:/var/empty:/usr/bin/false
_mysql:*:74:74:MySQL Server:/var/empty:/usr/bin/false
_sshd:*:75:75:sshd Privilege separation:/var/empty:/usr/bin/false
_qtss:*:76:76:QuickTime Streaming Server:/var/empty:/usr/bin/false
_cyrus:*:77:6:Cyrus Administrator:/var/imap:/usr/bin/false
_mailman:*:78:78:Mailman List Server:/var/empty:/usr/bin/false
_appserver:*:79:79:Application Server:/var/empty:/usr/bin/false
_clamav:*:82:82:ClamAV Daemon:/var/virusmails:/usr/bin/false
_amavisd:*:83:83:AMaViS Daemon:/var/virusmails:/usr/bin/false
_jabber:*:84:84:Jabber XMPP Server:/var/empty:/usr/bin/false
_xgridcontroller:*:85:85:Xgrid Controller:/var/xgrid/controller:/usr/bin/false
_xgridagent:*:86:86:Xgrid Agent:/var/xgrid/agent:/usr/bin/false
_appowner:*:87:87:Application Owner:/var/empty:/usr/bin/false
_windowserver:*:88:88:WindowServer:/var/empty:/usr/bin/false
_spotlight:*:89:89:Spotlight:/var/empty:/usr/bin/false
_tokend:*:91:91:Token Daemon:/var/empty:/usr/bin/false
_securityagent:*:92:92:SecurityAgent:/var/empty:/usr/bin/false
_calendar:*:93:93:Calendar:/var/empty:/usr/bin/false
_teamsserver:*:94:94:TeamsServer:/var/teamsserver:/usr/bin/false
_update_sharing:*:95:-2:Update Sharing:/var/empty:/usr/bin/false
_installer:*:96:-2:Installer:/var/empty:/usr/bin/false
_atsserver:*:97:97:ATS Server:/var/empty:/usr/bin/false
_unknown:*:99:99:Unknown User:/var/empty:/usr/bin/false

```

Proof:

Hooded Robin - January 11, 2012, 2:13 pm

Nice job there fellas - Keep up the good work!

stdape2011 - January 11, 2012, 2:16 pm

Very impressive, congratulations. :)

Maxitj - January 11, 2012, 4:24 pm

Nice job, anyway seems website is in beta phase so literally the expected it

The Ion - January 12, 2012, 1:47 am

very nice job shoutouts to all members of openfire keep up the good work coded32

New Darth Vader - January 12, 2012, 6:26 am

Inb4 IBM sues you for IP theft. Be a white hat.

rand0 - January 12, 2012, 8:44 am

Lol nice job. Keep up the good work, guise :)

Error667 - January 12, 2012, 10:40 am

Very nice, keep up this great work mate.

pwntoken - January 23, 2012, 12:45 pm

Thanks for the feedbacks.

Reported to IBM.

smiegles - January 23, 2012, 1:55 pm

copy paste : <https://lists.owasp.org/pipermail/owasp-delhi/2010-March/000874.html>

FAIL