OPE, JOIN, DET, ENCRYPTED, HOM

PhpBB annotations

Princ types .. 🡪 2 annotations

**in acl\_groups:**

predicate groupaccess: CREATE FUNC..

- groupid has access to formed if groupaccess(optioned, roleid)

🡪 4 annotations

**in forums**

- forumname, forumposts, forumlastpostsubject, forumimage, forumlastpostername enc for forumid

forumtopics

🡪 1 unique, 5 repeated

**in posts**

forumid equals forums.forumid

postsubject, post\_text, , post\_attachment, post\_edit\_reason, post\_edit\_user, post\_edit\_count, postime, encfor forumid

🡪 1 unique ; 7 repeated

**privmsgs**

encfor msgid: messagesubject, messagetext, to\_address, bcc\_address, message attachment, message time, message edit reason, message edit user, message edit time, message reported, message edit count, pm\_new

* 1 unique enc for
* 12 repeated

pm\_unread

**privmsgsto**

msgid equals privmsgs.msgid

authorid has access to msgid

userid has access to msgid

authorid equals users.userid

userid equals users.userid

**🡪 2 has access**

**usergroup**

groupid equals

userid equals , hasaccess to groupid

-> 1 has access

**users**

userid equals

username\_clean givespsswd

🡪 1 has access

Storage overhead:

In forum: 2048 for forum topics

🡪 stores >2870 bytes per row, overhead: 256 bytes

In privmessages: 2048 for pm\_unread hom, 64 ope, (128+1024)\*2 for access (2 for sender, receiver) tables

🡪 assume email 500 chars

🡪 stores: 1333bytes, overhead 552

In posts: 64 bits for ope, 64 bits for ope,

🡪 assume posts are 500 chars

🡪 stores > 1592bytes, 16 bytes overhead + 144 from group, user

Group, user: 1024bits + 128 bits for access tables

Most sensitive fields are: forum name, post text, post subject, message subject, message text, message attachment

HOTCRP:

PRINC TYPES EXTERNAL

PRINC TYPES

Anns: 2

Contact info:

Physicalcontacta has access to contact

anns: 1

NoConflict predicate 3 lines

Anns: 2

PaperReview:

PCMember.contactId has access to paperId

reviewerId, commentsToPC, technical merit, likely presenetaion, papersummary, comentstoAuthor, commentstoAddress, weaknesses of paper, strengths of paepr, enc for paperId IF..

++ (ope, review needs submit)

(HOM review score is summed up)

anns: 2/10

PaperReviewArchive

PCMember.contactId has access to papered

reviewerId, commentsToPC,

anns: 2/3

Paper

Title, authorinfo, abstract, collaborators, pcPaper, timesubmitted, pcPaper, leadcontactid, shephercontactid, Encfor papered

++ (OPE time submitted)

SEARCH on authorinformation

(DET title)

Papered has access to paperstorage

2/10

Paperstorage

1/1

Paper encfor paperstorageid

For different adversaries, most sensitive fields are: all except review needs submit, pcPaper, timesubmitted, shepherdcontactid

All are at HIGH because paper title is most likely unique and not joined

Grad-apply – onion levels generated by query traces

PRINC TYPES user, ctluser;

EXTERNAL

-> 2 annot

Appsusers:

Id has access to password

-> 1 anot

Ctlusers:

Id has access to name

Has access to appusers.id

Has access to letter id 1, letter id2, letter id3

* 5 annot

Forderid

17 scores, 61 grades, enc for, 6 ref name and email each is enc for letter id

name last, first – at ope

name last, first at SEARCH (there are more searches, but not among these sensitive fields)

4/84

6 dets: referee name and email

letters

10 fields enc for id

1/10

reviews:

7 fields (Score, teach\_exp, res\_exp, comments) encfor id

🡪they are all point updates so not DET

total fields: 17+61+6+2+10+7=103

2 + 1 + 5 + (4/86) + (1/10) + (1/7) = 13 /111

103 fields secured, 6 dets, 2 ope, 0 hom

ILIKE on:

Most sensitive are scores(17), grades(61), the contents of the letters in letters table(9 – answers to questions by the reviewers), all from reviews(7)