Security Admin

The security database was introduced in tiki 1.8.5 and consists of a database that contains all md5 sums of all tiki php files. This shall help tiki admins to detect uploaded, old or changed scripts. In 1.8.5 the database was a plain file (serialized php array), now it is located in the db. For easyness i decided to use tiki-install.php to import the security db. So (after creating the tiki-secdb table with tiki_1.8to1.9.sql) you can import the md5 sums with tiki-install.php and select the *secdb* files in the update section.

After import you can check the files: go to tiki-admin_security.php and click "check all files". This walks though all *.php files and compares them to the security database. It can detect if a file is modified - since the secdb content is now some hours old, you'll find some changed files. I plan to generate secdb files for all tiki versions and mods so that admins then can find old and possible dangerous files. The db also contains a "severity" column to mark dangerous old script files (to be implemented). admin_security also tells you if it thinks that a file does not contain to a tiki installation.

For release managers: the doc/devtools/tiki-create_md5.php is used to create a security database of a set of files.
Call it as
tiki-create_md5.php?tikiver=1.9&chkdir=../../
or better copy it to tiki-root (it will not md5 itself) and call it with
tiki-create_md5.php?tikiver=1.9
Then use mysqldump no-create-info tables tiki_secdb to generate a sql dump of this security database.
Probably it is better to sort the output before commit to avoid large commits:
mysqldump no-create-info tables tiki_secdb | sort > db/tiki-secdb_1.9_mysql.sql
(untested, check if mysqldump creates other lines than inserts)

You can scan other directories with (example)
tiki-create_md5.php?tikiver=1.8&chkdir=../../../tiki-1.8/