Checking your server & Tiki settings

The information on this page is incomplete and/or outdated. For related info see Tiki Check and System Configuration.

On tiki-admin_security.php, you can check for less secure server or Tiki settings.

PHP settings			
PHP variable	Setting	Risk Factor	Explanation
allow_url_fopen		safe	
register_globals		safe	
session.use_trans_sid	0	safe	
upload_tmp_dir		unknown	cannot check if the upload_tmp_dir is accessible via web browser. To be sure you should check your webserver config.
xbithack		safe	

Tikiwiki settings			
Tiki variable	Setting	Risk Factor	Explanation
gal_use_dir	imagegals/	unsafe	The Path to store files in the imagegallery should be outside the tiki root directory

Check your files (secdb)

File check (at tiki-admin_security.php) will detect any PHP files (and .tpl files in recent versions of Tiki), but not images (.jpg, .gif, .png) which have been altered compared to the default, clean install of Tiki.

Check all tiki files
Note, that this can take a very long time. You should check your max_execution_time setting in php.ini.
Note: You have to import security data via installation process (**tiki-install.php**).
Import the *secdb* update files in your database.

File checks	
Filename	State
./tiki-install.php	This file is from another Tikiwiki version: 1.9
./db/local.php	This is not a Tikiwiki file. Check if this file was uploaded and if it is dangerous.

This is the result of checking all PHP files in my local install compared to the default/clean Tiki install.

It is normal that local.php be modified. If you check the file:

```
<?php
$db_tiki='mysql';
$dbversion_tiki='1.9';
$host_tiki='localhost';
$user_tiki='my_database_user_name';
$pass_tiki='my_database_secret_password';
$dbs_tiki='my_database_name';
?>
```

db/local.php should look like this

It is also normal that tiki-install.php be modified (as you probably clicked to de-activate it). All other modified files should have been by you.

Please note that if you update your site via SVN, it's normal that some files are reported because the secDB database is typically only updated at release time.

On more recent versions of Tiki, it's also normal that language files are flagged because they are compressed after the security check is done. This is solved starting in Tiki 9.2

Also, starting in Tiki 9.2, Tiki not only checks .php files but also .tpl, .css, .sql and .js

Robots Exclusion (Banning Search engines)

For some uses you may wish to prevent search engines from crawling, indexing or archiving your site. See: Robots Exclusion Protocol and Meta Elements

User/Content Security

see: Groups

Securing your webserver

If you are using Apache webserver, you can also secure it (and therefore, secure tiki) by means on enabling "**mod_security**".

See ModSecurity for more information.

related

More info:
http://tiki.org/AdminSecurity

Alias names for this page

SecDB | SecurityAdmin | Security