# TikiInSharedHosting

FutureQuest (FQ) has established that their hardware and network are physically capable of accomodating tikiwiki.org. Next step is to determine if Tikiwiki would work well in shared hosting environments, their core business. By sponsoring Tiki, they will be effectively endorsing the product.

- How server friendly is Tikiwiki ?
    - tiki is very friendly when well. I host tikiwiki.org on my personnal server, with a lot of other services, but with low traffic, so it's not easy to estimate. But some page can help to get a view :
    - http://tikiwiki.org/webalizer/ stats from apache logs
    - http://tikiwiki.org/tiki-stats.php numbers about content of tw.o
    - http://feu.org/sys/ the id card of the server. notice the uptime : it's the same as the one of tikiwiki project (offset by 2 days)

- Could our clients easily use this on a Community Server, or would it cause problems for the server ?
    - Of course they could. Like a yahoo groups service. But it's some backend work, though. I simulated such environment, and run about 10 tikiwikis in the same place, using one file tree and one db per account. So virtuality management is on db, and almost all the stored data is in separated places. But higher volumes would require some fine tuning.

- If all of TikiWiki's features were used by a client, how many (full running) Tikiwiki instances could run on a Community Server before it's resource consumption will be noticed...
    - No idea. You'll have to benchmark it on a dedicated box. Or maybe some of tiki experts can set it up for you.
    - You can't activate all features in a shared environment. More even, your package has to take in account a meduim use of tikiwiki. Rare are those that run all features. You should put limitation on some that are resource consuming : webchat, live support, phpopentracker, webmail ..

- I would like to see a full manifest documenting all security holes that have been found and fixed... I am mostly interested in seeing how long a security hole is left open before a patch is released...
    - it depends who is motivated to do the patch. Usually, it's the one that suffer from the hole, obviously. Welcome in the community But if it's a responsiveness issue, and if you need 10 geeks work 24h a day, it's possible, if you find, with each of them or with that subgroup, a way to interest them, with money or individual free services or any private or group agreement on the fly : we can never predict who will be avalaible before it comes.

- Something as complex as Tikiwiki usually carries a high risk of exploitable flaws, and with Tikiwiki running via our PHP Secure_Mode™ setup* - the risk greatly intensifies**... This is because the PHP scripts run as your user and group id, instead of the more generic permissions of the Apache server, and any exploits found and used - will have full access to that site owners account... Our Secure_Mode™ offers a tremendous amount of power and flexibility (no safe_mode), but with that also carries the same risk as what CGI scripts have...

> * Secure_Mode™ is an underlying nomenclature for our proprietary high speed low overhead mechanisms that allow Apache to elevate the privileges of an embedded PHP engine from an:

==>request> unprivileged ==> privileged ==>results> unprivileged

for that particular PHP execution phase... It by no means suggests sandboxing, chrooting, or any other type of security measure other than helping to solidify privacy...

**PHP scripts are notoriously more lax when it comes to secure programming, mostly because the web author assumes that it will not be running with the full user and group privileges of the site owner, but rather with unprivileged/generic rights...

FQ: The above listed items must be weighed very carefully, because a side-effect of sponsoring the hosting of this, we are in effect endorsing Tikiwiki and putting forth an implied message that it is OK for site owners to run this on our servers... It would be terribly embarrassing if it was later found that Tikiwiki is simply too heavy for clients to run on a Community Server and we had to place the application on our Community Server watchlist or blacklist...