

Re: generate 2 random numbers in rapid sequence

Re: generate 2 random numbers in rapid sequence

Source: <http://coding.derkeiler.com/Archive/PHP/comp.lang.php/2006-04/msg01436.html>

- *From:* "Jim Michaels" <NOSPAMFORjimichae3@xxxxxxxxxx>
 - *Date:* Sat, 22 Apr 2006 23:43:21 -0700
-

"Gordon Burditt" <gordonb.cg3n5@xxxxxxxxxxxxxx> wrote in message
news:124luplqscmpm9f@xxxxxxxxxxxxxxxxxxxxxxxxxx

I need to generate 2 random numbers in rapid sequence from either PHP or mysql.

Same page hit or different page hits? I cannot explain why you would get the same number in rapid sequence from several calls on the same hit.

same page hit on the webserver to a .html file, which has 2 elements.
on a multiprocessor webserver, this may be occurring simultaneously.

I have not been able to do either. I get the same number back several times
from PHP's mt_rand() and from mysql's RAND().
any ideas?

When PHP starts up, the seed gets initialized to <SOMETHING>, possibly based on microtime(), but I really don't care. Apache/PHP don't get restarted very often. With a good host, it could easily be less than once a month. However, once PHP starts, it's fixed.

It is likely that if Apache fork(s) for a given hit, the seed stays initialized to <SOMETHING> unless you explicitly set it. Any changes to that by more calls to get pseudo-random numbers are discarded when that instance of Apache exits. To get different values, you need to explicitly set the seed to a function of something other than just microtime().

Re: generate 2 random numbers in rapid sequence

which makes sense. if all set to microtime, you would still get the same images.

Things to use for a seed (jumble them all together, as in concatenate, then take md5 of result, then convert some of md5 result to integer):
microtime()
getmypid()

believe it or not, on these 2 I get the same pictures. frustrating.

`$_SERVER['UNIQUE_ID']` (Apache only, and may need a module turned on)

Don't think I have that option. sure sounds good though.

`$_SERVER['REMOTE_ADDR']`
`$_SERVER['REMOTE_PORT']`

these two won't make it unique, because both images are going to be all on the same page.

```
mt_srand(make_seed()+getmypid()+$_SERVER['UNIQUE_ID']);
```

```
$n=mt_rand(1,$row['a']);
```

tried this, but still doesn't do it. I don't even get an error on

`$_SERVER['UNIQUE_ID']`. I think it's NULL. is `$_SERVER['UNIQUE_ID']` a string I should hash, or an integer?

Actually, using just the first two should be sufficient, as the pair (microtime(), getmypid()) should be unique. However, to get more entropy, throw in some of the others.

If you are using pseudo-random numbers to select one of 100 images, expect the same image twice in a row about 1% of the time, unless you have code to deal with this. My suggestion is to not attempt to avoid this.

I get a different image on next page refresh, possibly due to the time involved. but the same images all over the page, possibly due to the time involved.

Re: generate 2 random numbers in rapid sequence

Re: generate 2 random numbers in rapid sequence

I suppose I could use the current random number as the seed for the next random number. but would that really work?

It's a very BAD idea to seed a pseudo-random number generator multiple times in the same run. Using the output of the random number generator as a new seed is also not a good idea. It's very easy to cripple a good pseudo-random number generator with a poor method of choosing a seed. The problem you're having with `microtime()`

I understand that. I was trying to avoid it. but nothing seems to work short of having semaphore'd access to a file or database as the seed and just incrementing it like a counter. And then I'm circumventing the web server's whole concept of parallelism. :-/

demonstrates this. Seed once. Use a good source of (pseudo-)randomness. `microtime()` alone doesn't qualify if you require rapid-fire results.

tell me about it. :-/

Gordon L. Burditt

.