The Road to Olympus

Experiences

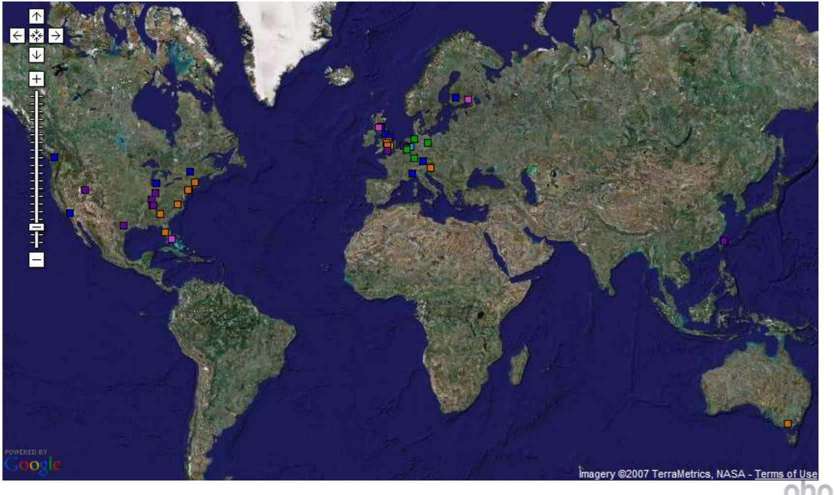
Henry “Kellanved” Sudhof

December 2007

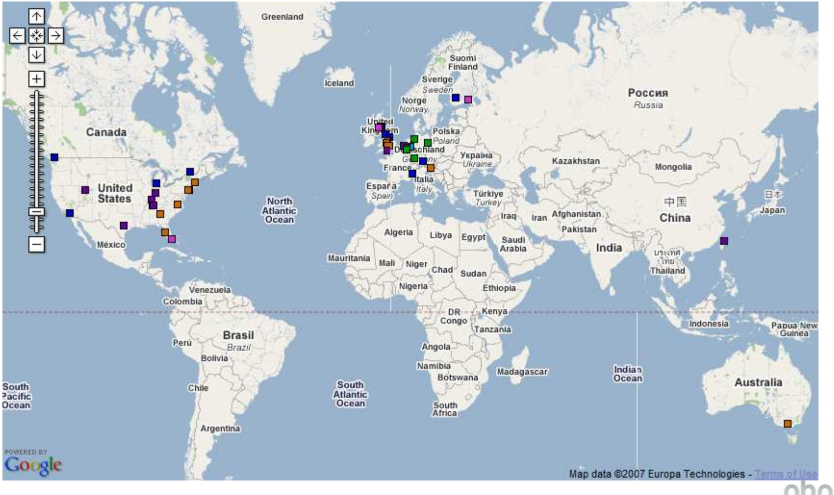
A full plate

1. The Story so far
2. phpBB3 Olympus
3. Lessons learned
4. Mean Tricks

the phpBB group



the phpBB group



phpBB

- Started as a one-man project in 2000
- James "theFinn" Atkinson
- simple UBB–like forum
- PHP3 / MySQL
- hardcoded language
- product of the PHP hype

phpBB 2

- Started 2001
- Released **2002**
- PHP 3,4
- Paul "PSOTFX" Owen
- groundbreaking
- webby nominated
- Database abstraction
- template system
- i18n

phpBB 2 - what went wrong?

Santy

- 2004
- A worm exploiting outdated phpBB 2 installations
- major media attention
- Ruined reputation
- incidentally, vulnerable code was from the PHP docs

Development slowed

- phpBB 3 was IIRC earmarked for a 2004/2005 release
- three years late
- almost complete team turnover

phpBB 2 - what went wrong?

Santy

- 2004
- A worm exploiting outdated phpBB 2 installations
- major media attention
- Ruined reputation
- incidentally, vulnerable code was from the PHP docs

Development slowed

- phpBB 3 was IIRC earmarked for a 2004/2005 release
- three years late
- almost complete team turnover

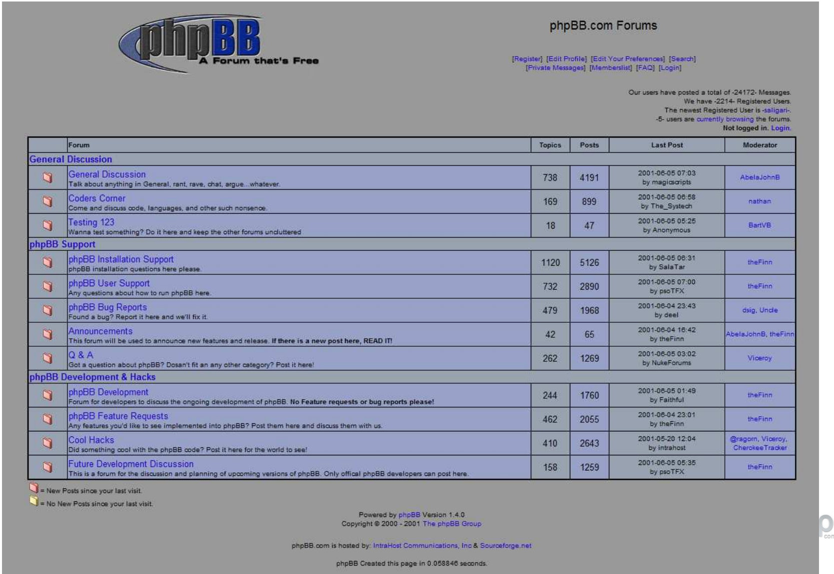
phpBB 2 - how bad is it really

- written 2001
- PHP 3
- 22 versions in six years
- statistically neither more nor worse exploits than in competition
- however, still latest stable release
- no vulnerability reports in more than a year
- Installed on several million servers
- included in most distributions
- Extremely frequently forked
- Ongoing – sometimes questionable – reporting
- Prime subject for heise/slashdot Trolls

phpBB 2 - how bad is it really

- written 2001
- PHP 3
- 22 versions in six years
- statistically neither more nor worse exploits than in competition
- however, still latest stable release
- no vulnerability reports in more than a year
- Installed on several million servers
- included in most distributions
- Extremely frequently forked
- Ongoing – sometimes questionable – reporting
- Prime subject for heise/slashdot Trolls

Generations



phpBB.com Forums

[Register] [Edit Profile] [Edit Your Preferences] [Search]
[Private Messages] [Memberslist] [FAQ] [Login]

Our users have posted a total of -24172- Messages.
We have -2214- Registered Users.
The newest Registered User is -saligari-.
-5- users are currently browsing the forums.
Not logged in. Login.

	Forum	Topics	Posts	Last Post	Moderator
General Discussion					
🟥	General Discussion Talk about anything in General, rant, rave, chat, argue...whatever.	738	4191	2001-06-05 07:03 by magicscripts	AbelaJohnB
🟥	Coders Corner Come and discuss code, languages, and other such nonsence.	169	899	2001-06-05 06:58 by The_Systech	nathan
🟥	Testing 123 Wanna test something? Do it here and keep the other forums uncluttered	18	47	2001-06-05 05:25 by Anonymous	BartVB
phpBB Support					
🟥	phpBB Installation Support phpBB installation questions here please.	1120	5126	2001-06-05 06:31 by SalaTar	theFinn
🟥	phpBB User Support Any questions about how to run phpBB here.	732	2890	2001-06-05 07:00 by psoTFX	theFinn
🟥	phpBB Bug Reports Found a bug? Report it here and we'll fix it.	479	1968	2001-06-04 23:43 by deel	dsig, Uncle
🟥	Announcements This forum will be used to announce new features and release. **If there is a new post here, READ IT!**	42	65	2001-06-04 16:42 by theFinn	AbelaJohnB, theFinn
🟥	Q & A Got a question about phpBB? Dosan't fit an any other category? Post it here!	262	1269	2001-06-05 03:02 by NukeForums	Viceroy
phpBB Development & Hacks					
🟥	phpBB Development Forum for developers to discuss the ongoing development of phpBB. **No Feature requests or bug reports please!**	244	1760	2001-06-05 01:49 by Faithful	theFinn
🟥	phpBB Feature Requests Any features you'd like to see implemented into phpBB? Post them here and discuss them with us.	462	2055	2001-06-04 23:01 by theFinn	theFinn
🟥	Cool Hacks Did something cool with the phpBB code? Post it here for the world to see!	410	2643	2001-05-20 12:04 by intrahost	@ragorn, Viceroy, CherokeeTracker
🟥	Future Development Discussion This is a forum for the discussion and planning of upcoming versions of phpBB. Only offical phpBB developers can post here.	158	1259	2001-06-05 05:35 by psoTFX	theFinn

🟥 = New Posts since your last visit.

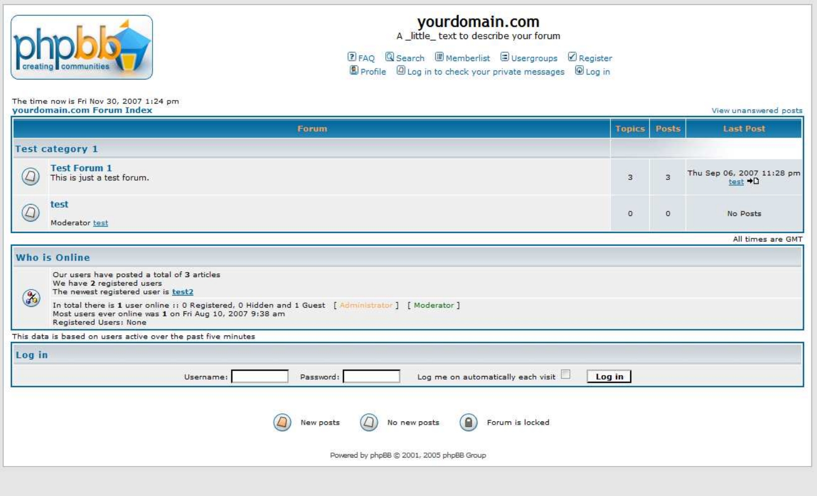
🟨 = No New Posts since your last visit.

Powered by phpBB Version 1.4.0
Copyright © 2000 - 2001 The phpBB Group

phpBB.com is hosted by: IntraHost Communications, Inc & Sourceforge.net

phpBB Created this page in 0.058846 seconds.

Generations



yourdomain.com

A _little_ text to describe your forum

FAQ Search Memberlist Usergroups Register
Profile Log in to check your private messages Log in

The time now is Fri Nov 30, 2007 1:24 pm
yourdomain.com Forum Index

View unanswered posts

Forum	Topics	Posts	Last Post
Test category 1			
Test Forum 1 This is just a test forum.	3	3	Thu Sep 06, 2007 11:28 pm test
test Moderator test	0	0	No Posts

All times are GMT

Who is Online

Our users have posted a total of **3** articles
We have **2** registered users
The newest registered user is **test2**

In total there is **1** user online :: 0 Registered, 0 Hidden and 1 Guest [Administrator] [Moderator]
Most users ever online was **1** on Fri Aug 10, 2007 9:38 am
Registered Users: None

This data is based on users active over the past five minutes

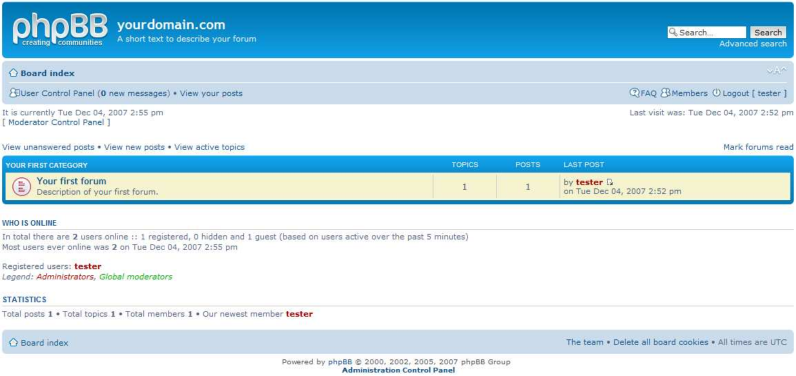
Log in

Username: ____ Password: ____ Log me on automatically each visit □ **Log in**

New posts No new posts Forum is locked

Powered by phpBB © 2001, 2005 phpBB Group

Generations



yourdomain.com
A short text to describe your forum

Board index

User Control Panel (**0** new messages) • View your posts

FAQ Members Logout [tester]

It is currently Tue Dec 04, 2007 2:55 pm
[Moderator Control Panel]

Last visit was: Tue Dec 04, 2007 2:52 pm

View unanswered posts • View new posts • View active topics

Mark forums read

YOUR FIRST CATEGORY	TOPICS	POSTS	LAST POST
Your first forum Description of your first forum.	1	1	by **tester** on Tue Dec 04, 2007 2:52 pm

WHO IS ONLINE

In total there are **2** users online :: 1 registered, 0 hidden and 1 guest (based on users active over the past 5 minutes)
Most users ever online was **2** on Tue Dec 04, 2007 2:55 pm

Registered users: **tester**
Legend: Administrators, Global moderators

STATISTICS

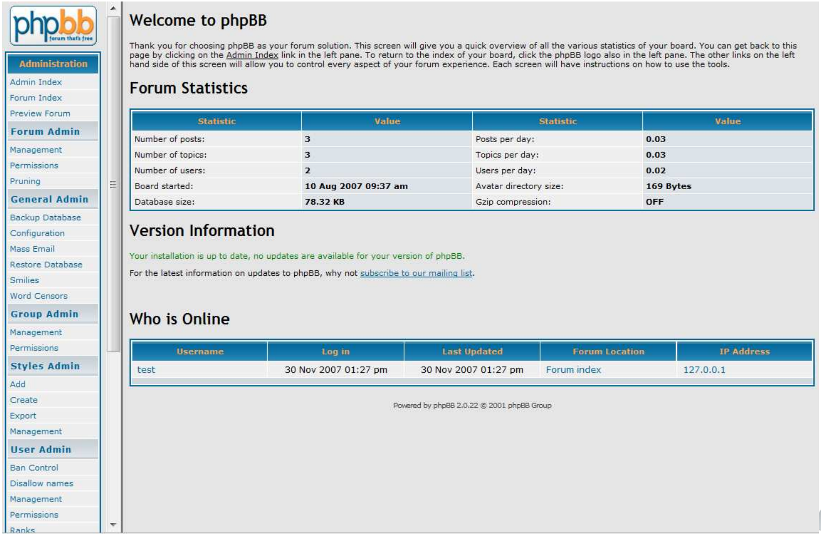
Total posts **1** • Total topics **1** • Total members **1** • Our newest member **tester**

Board index

The team • Delete all board cookies • All times are UTC

Powered by phpBB © 2000, 2002, 2005, 2007 phpBB Group
Administration Control Panel

Generations



Welcome to phpBB

Thank you for choosing phpBB as your forum solution. This screen will give you a quick overview of all the various statistics of your board. You can get back to this page by clicking on the Admin Index link in the left pane. To return to the index of your board, click the phpBB logo also in the left pane. The other links on the left hand side of this screen will allow you to control every aspect of your forum experience. Each screen will have instructions on how to use the tools.

Forum Statistics

Statistic	Value	Statistic	Value
Number of posts:	**3**	Posts per day:	**0.03**
Number of topics:	**3**	Topics per day:	**0.03**
Number of users:	**2**	Users per day:	**0.02**
Board started:	**10 Aug 2007 09:37 am**	Avatar directory size:	**169 Bytes**
Database size:	**78.32 KB**	Gzip compression:	**OFF**

Version Information

Your installation is up to date, no updates are available for your version of phpBB.

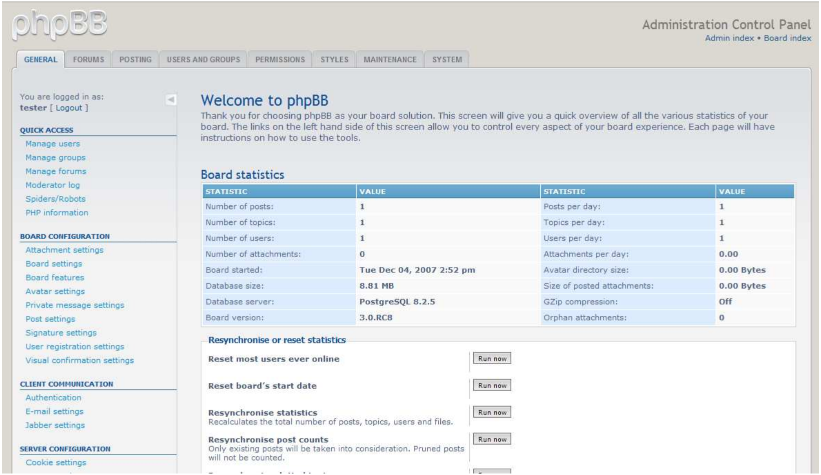
For the latest information on updates to phpBB, why not subscribe to our mailing list.

Who is Online

Username	Log in	Last Updated	Forum Location	IP Address
test	30 Nov 2007 01:27 pm	30 Nov 2007 01:27 pm	Forum index	127.0.0.1

Powered by phpBB 2.0.22 © 2001 phpBB Group

Generations



Welcome to phpBB

Thank you for choosing phpBB as your board solution. This screen will give you a quick overview of all the various statistics of your board. The links on the left hand side of this screen allow you to control every aspect of your board experience. Each page will have instructions on how to use the tools.

Board statistics

STATISTIC	VALUE	STATISTIC	VALUE
Number of posts:	1	Posts per day:	1
Number of topics:	1	Topics per day:	1
Number of users:	1	Users per day:	1
Number of attachments:	0	Attachments per day:	0.00
Board started:	Tue Dec 04, 2007 2:52 pm	Avatar directory size:	0.00 Bytes
Database size:	8.81 MB	Size of posted attachments:	0.00 Bytes
Database server:	PostgreSQL 8.2.5	GZip compression:	Off
Board version:	3.0.RC8	Orphan attachments:	0

Resynchronise or reset statistics

Reset most users ever online

Reset board's start date

Resynchronise statistics
Recalculates the total number of posts, topics, users and files.

Resynchronise post counts
Only existing posts will be taken into consideration. Pruned posts will not be counted.

Audience

- new communities
- Open Source users
- Teens/twens
- Clubs and non-profits
- startup commercial communities
- Hardware : usually shared server, MySQL, PHP4, memory limit 8-20 MB
- sometimes several high-powered servers

The Good

- GPL
- powerful DBAL (MySQL, postgres, SQL Server, Oracle, SQLite, firebird, ...)
- Caching
- plugins for authentication, caching, search, ...
- wrapable
- UTF-8
- 61 languages and counting, BiDi support
- highly optimized
- Modules
- ACL
- XHTML strict compliant
- a ton of new features (try it!)
- Yes, it scales
- Joomla! on board

No Light without Shadow

The Bad

- Usability-wise not up to commercial packages (no Ajax)
- bbcode parser can be suboptimal
- no easy extension outside the modules (yet)
- limited API

And the Ugly

- about 300 KLOC
- designed in 2001
- PHP4
- Some functions in the 1000 LOC ballpark
- 2 – 3 years overdue

No Light without Shadow

The Bad

- Usability-wise not up to commercial packages (no Ajax)
- bbcode parser can be suboptimal
- no easy extension outside the modules (yet)
- limited API

And the Ugly

- about 300 KLOC
- designed in 2001
- PHP4
- Some functions in the 1000 LOC ballpark
- 2 – 3 years overdue

Why are things better?

- Threat-aware design
- layered defense
- I/O API
- six active developers lead by Meik “Acyd Burn” Sievertsen
- established Incident Response Team
- dedicated security tracker
- Paid audit by Stefan Esser

type-aware Parameter Sanitation

- All input via request_var function
- `function request_var($var_name, $default, $multibyte = false)`
- `...?foo=<evil>` + `$foobar = request_var('foo', 'bar')` ⟹ `&lt;evil&gt;`
- `...?foo='%20UNION...` + `$foobar = request_var('foo', 0)` ⟹ 0
- works for multidimensional arrays as well
- principle: never have any variable holding unsanitized data

type-aware Query Builder

- automagically escape query parameters
- powerful DB abstraction

Build Query

```
$sql = $db->sql_build_query('SELECT', array(
  'SELECT' => 'a.forum_id, ug.user_id',

  'FROM'    => array(
    ACL_OPTIONS_TABLE   => 'o',
    USER_GROUP_TABLE    => 'ug',
    ACL_GROUPS_TABLE    => 'a'
  ),

  'LEFT_JOIN' => array(
    array(
      'FROM'    => array(ACL_ROLES_DATA_TABLE => 'r'),
      'ON'      => 'a.auth_role_id = r.role_id'
    ),
  ),
));
```

Stateful Randomizer

- normal rand/mtrand gives attackers a 1 in 20 chance
- lethal for passwords, UIDs, CAPTCHAs
- phpBB's rand is not just seeded by time
- re-generated on each use
- used for one-time passwords
- used for bbcode UIDs
- used for strong hashes

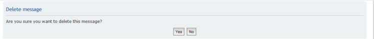
CSRF

Form Tokens

- Timed
- form-specific
- user-specific
- no queries needed

Confirm Boxes

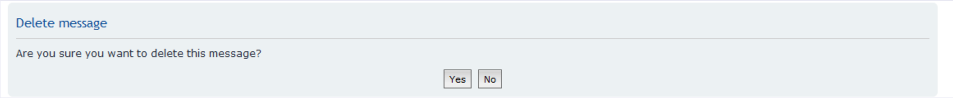
- "Do you really want" boxes



Delete message

Are you sure you want to delete this message?

CSRF



Delete message

Are you sure you want to delete this message?

The usual suspects

IE: Just a nice little png

- Defense
- never allow direct access
- always use C-D: attachment
- hide physical locations
- for IE 6: disallow caching
- [a]

[a] This seems to be fixed in IE7 since 11/07 – still works for BMP

IE: Encoding

- Waiter, I believe there's a quote in my query string
- IE won't encode double quotes
- Solution: just like any other _SERVER variable: don't trust it

The usual suspects

IE: Just a nice little png

- Defense
- never allow direct access
- always use C-D: attachment
- hide physical locations
- for IE 6: disallow caching
- [a]

[a] This seems to be fixed in IE7 since 11/07 – still works for BMP

IE: Encoding

- Waiter, I believe there's a quote in my query string
- IE won't encode double quotes
- Solution: just like any other _SERVER variable: don't trust it

The usual suspects

IE: Just a nice little png

- Defense
- never allow direct access
- always use C-D: attachment
- hide physical locations
- for IE 6: disallow caching
- [a]

[a] This seems to be fixed in IE7 since 11/07 – still works for BMP

IE: Encoding

- Waiter, I believe there's a quote in my query string
- IE won't encode double quotes
- Solution: just like any other _SERVER variable: don't trust it

Unexpected surprises

base64

- `data:text/html;base64,PHNjcmlwdD5hbGVydCgnbXVoYWhhaGEnKTwvc2NyaXB0Pgo=`
- survives `htmlspecialchars` just fine
- javascript:, vbscript: similar

"<script>"? That's a weird IP address.

- users can write anything into X_FORWARDED_FOR
- don't trust it. Don't ever use it unsanitized

Unexpected surprises

base64

- data:text/html;base64,PHNjcmlwdD5hbGVydCgnbXVoYWhhaGEnKTwvc2NyaXB0Pgo=
- survives htmlspecialchars just fine
- javascript:, vbscript: similar

"<script>"? That's a weird IP address.

- users can write anything into X_FORWARDED_FOR
- don't trust it. Don't ever use it unsanitized

Does it pay off?

- We don't know
- but are optimistic

Stefan Esser wrote

> *Due to the usage of helper functions to create parts of the SQL queries and due to the strict usage of the request_var() function on all identifier variables it seems the code that interfaces with the database was very well written.*

SektionEins

Does it pay off?

- We don't know
- but are optimistic

Stefan Esser wrote

> *Due to the usage of helper functions to create parts of the SQL queries and due to the strict usage of the request_var() function on all identifier variables it seems the code that interfaces with the database was very well written.*

SektionEins

Thankies

Time to wake up!

`http://www.phpbb.com`

Assorted Live Demos