



Hacking Mediawiki

By Arthur Richards
Software Engineer, Wikimedia Foundation

arichards@wikimedia.org

IRC: awjr

`[[User:awjrichards]]`

What is Mediawiki anyway?

- GPL server-based Wiki software
- PHP and MySQL
- Community developed and maintained
- Powers Wikipedia and other Wikimedia projects

Welcome to Wikimedia

Wikimedia is owned and operated by the Wikimedia Foundation, a non-profit foundation dedicated to bringing free content to the world. The various Wikimedia projects are listed below:



Ok, but what is a 'wiki'?!

“A wiki (/ˈwɪki/ WIK-ee) is a website that allows the creation and editing of any number of interlinked web pages via a web browser using a simplified markup language or a WYSIWYG text editor.”

- <http://en.wikipedia.org/wiki/Wiki>



Editing GUnify

From Wikipedia, the free encyclopedia

B *I* [Advanced](#) [Special characters](#) [Help](#)

[[File:Gnunity.png|thumb|alt=Gnunity Logo|Gnunity Logo]]

'''Gnunity''' is an annual gathering consisting of Workshops, Talks, Seminars and BOFs (Birds of a feather) held by the [[Pune Linux User Group]] [<http://plug.org.in/>] and the [[Symbiosis Institute of Computer Studies and Research (SICSR)|Symbiosis Institute of Computer Studies and Research]] in [[Pune]], [[India]]. It is an event held to help increase the awareness of [[FOSS]] in India especially in Pune.Its a forum to unite open minds.

Gnunity (a play on the words [[GNU]] and Unify) is generally held during the second week of February. Gnunity has featured eminent people like [[Richard Stallman]]<ref name='richard-stallman-gnunity'>[<http://gnu.gds.tuwien.ac.at/wwwin/events.html> FSF India's events page in 2003</ref>, [[Brian Behlendorf]], [[David Axmark]] <ref name="technetra-gnunity-2008">[<http://opensourcebuzz.technetra.com/2008/02/18/gnunity-2008-it-only-gets-better> Article in Feb 2008 on Technetra's Blog</ref>, [[Danese Cooper]] <ref name='danese-blog'>[http://danesecooper.blogs.com/divablog/2006/02/gnunity_2006.html Danese Cooper's Blog entry on Gnunity</ref>, [[Robert Adkins]], [[Alolita Sharma]], Prof. [[Tony Wasserman]], Prof. [[Louis Pott]], Niyam Bhushan, Sankarshan, Zahira Bohrat and Anant Narayanan.<ref name='technetra-gnunity-2009'>[<http://opensourcebuzz.technetra.com/2009/03/08/gnunity-2009-community-support-matters> Technetra's Blog Entry on Gnunity 2009</ref> This year Gnunity is going to be held in February on 11th and 12th with the name Gnunity'11.The meetings have already started and the students of SICSR are ready with their ideas.

Gnunity 2011 is scheduled on 11 & 12 February 2011.

== Gnunity 2011==

As stated above, Gnunity 2011 is scheduled to be held on the 11th and 12 of February, 2011.



Revision history of GNUunify

From Wikipedia, the free encyclopedia

[View logs for this page](#)

[View or restore 4 deleted edits?](#)

Browse history

From year (and earlier): From month (and earlier): Tag filter: Deleted only

For any version listed below, click on its date to view it. For more help, see [Help:Page history](#) and [Help:Edit summary](#).

External tools: [Revision history statistics](#) • [Contributors](#) • [Revision history search](#) • [Number of watchers](#) • [Page view statistics](#)

(cur) = difference from current version, (prev) = difference from preceding version, **m** = minor edit, → = section edit, ← = automatic edit summary

- [\(cur | prev\)](#) [08:27, 7 February 2011](#) [Giraffedata](#) ([talk](#) | [contribs](#)) (3,224 bytes) (*"comprising of"*) ([undo](#))
- [\(cur | prev\)](#) [20:14, 26 January 2011](#) [Birajdarpriyanka22](#) ([talk](#) | [contribs](#)) (3,224 bytes) ([undo](#))
- [\(cur | prev\)](#) [18:59, 22 January 2011](#) [122.169.12.183](#) ([talk](#)) (3,224 bytes) ([→Tracks](#)) ([undo](#))
- [\(cur | prev\)](#) [17:55, 21 January 2011](#) [AninditAdhikary](#) ([talk](#) | [contribs](#)) (2,984 bytes) ([undo](#))
- [\(cur | prev\)](#) [10:55, 14 January 2011](#) [202.71.143.2](#) ([talk](#)) (2,980 bytes) ([undo](#))
- [\(cur | prev\)](#) [13:27, 7 December 2010](#) [Tej10030142085](#) ([talk](#) | [contribs](#)) (2,314 bytes) ([→Tracks](#)) ([undo](#))
- [\(cur | prev\)](#) [13:26, 7 December 2010](#) [Tej10030142085](#) ([talk](#) | [contribs](#)) (2,367 bytes) ([undo](#))
- [\(cur | prev\)](#) [17:47, 25 August 2010](#) [Xezbeth](#) ([talk](#) | [contribs](#)) (2,367 bytes) (*cat*) ([undo](#))

GNUUnify

From Wikipedia, the free encyclopedia
 (Difference between revisions)

Revision as of 20:14, 26 January 2011 (edit)

[Birajdarpriyanka22](#) (talk | contribs)

(del/undel)

[← Previous edit](#)

Current revision as of 08:27, 7 February 2011 (edit) (undo)

[Giraffedata](#) (talk | contribs)

(*"comprising of"*) (del/undel)

Line 1:

[[File:Gnunity.png|thumb|alt=GNUUnify Logo|GNUUnify Logo]]

'''GNUUnify''' is an annual gathering **comprising** of Workshops, Talks, Seminars and BOFs (Birds of a feather) held by the [[Pune Linux User Group]] [http://plug.org.in/] and the [[Symbiosis Institute of Computer Studies and Research (SICSR)|Symbiosis Institute of Computer Studies and Research]] in [[Pune]], [[India]]. It is an event held to help increase the awareness of [[FOSS]] in India especially in Pune.Its a forum to unite open minds.

GNUUnify (a play on the words [[GNU]] and Unify) is generally held during the second week of February. GNUUnify has featured eminent people like [[Richard Stallman]]<ref name='richard-stallman-gnunity'>[http://gnu.gds.tuwien.ac.at/wwwin/events.html FSF India's events page in 2003</ref>, [[Brian Behlendorf]], [[David Axmark]] <ref name="technetra-gnunity-2008">[http://opensourcebuzz.technetra.com/2008/02/18/gnunity-2008-it-only-gets-better Article in Feb 2008 on Technetra's Blog</ref>,

Line 1:

[[File:Gnunity.png|thumb|alt=GNUUnify Logo|GNUUnify Logo]]

'''GNUUnify''' is an annual gathering **consisting** of Workshops, Talks, Seminars and BOFs (Birds of a feather) held by the [[Pune Linux User Group]] [http://plug.org.in/] and the [[Symbiosis Institute of Computer Studies and Research (SICSR)|Symbiosis Institute of Computer Studies and Research]] in [[Pune]], [[India]]. It is an event held to help increase the awareness of [[FOSS]] in India especially in Pune.Its a forum to unite open minds.

GNUUnify (a play on the words [[GNU]] and Unify) is generally held during the second week of February. GNUUnify has featured eminent people like [[Richard Stallman]]<ref name='richard-stallman-gnunity'>[http://gnu.gds.tuwien.ac.at/wwwin/events.html FSF India's events page in 2003</ref>, [[Brian Behlendorf]], [[David Axmark]] <ref name="technetra-gnunity-2008">[http://opensourcebuzz.technetra.com/2008/02/18/gnunity-2008-it-only-gets-better Article in Feb 2008 on Technetra's Blog</ref>,

Why should I hack Mediawiki?

- Because you can
- Fix a problem with the software
- 'Scratch an itch'
- Public work record
- Mentor and be mentored
- Put the 'ww' in 'www'
- Support an awesome vision

Hacking the Software: What to Hack

- Bug fixes (<http://bit.ly/geY1u0>)
- Core code (<http://bit.ly/geY1u0>)
- Parser hooks
- External tools with the API (<http://bit.ly/eBl0i>)
- SpecialPages (<http://bit.ly/323H1o>)







Diving in with VariablePage extension



<http://www.flickr.com/photos/aknacer/2588798719/>

VariablePage

```
$ svn co \  
http://svn.wikimedia.org/svnroot/mediawiki/  
trunk/extensions/VariablePage
```

- ▼  VariablePage_bzr
 - ▼  VariablePage_trunk
 -  VariablePage.alias.php
 -  VariablePage.body.php
 -  VariablePage.i18n.php
 -  VariablePage.php

Setup: ExtensionName.php

Goal:

To simplify and centralize installation and configuration

```
1 <?php
2 require_once( "$IP/extensions/ExtensionName/Ext
   extensionName.php" );
3 $wgExtNameFoo = true;
4 $wgExtNameBar = 'baz';
...

```

Setup... continued

- Possible to defer extension setup until after LocalSettings.php has been run

```
1 <?php
2 ...
3 ...
4 ...
5 $wgExtensionFunctions[] = 'efExtensionNameSetup';
6
7 function efExtensionNameSetup() {
8     # do post-setup stuff here
9 }
...

```

Setup: database tables

```
39 ...
40 # Schema updates for update.php
41 $wgHooks['LoadExtensionSchemaUpdates'][] = 'fnMyHook';
42 function fnMyHook() {
43     global $wgExtNewTables, $wgExtModifiedFields;
44     $wgExtNewTables[] = array(
45         'tablename',
46         dirname( __FILE__ ) . '/table.sql'
47     );
48     $wgExtModifiedFields[] = array(
49         'table',
50         'field_name',
51         dirname( __FILE__ ) .
52         '/table.patch.field_name.sql'
53     );
54     return true;
55 }
```

- <http://bit.ly/fk9uyf>

Execution: VariablePage.body.php

- 'VariablePage' is a 'SpecialPage' extension
- `function execute() {}`
- `http://path/to/mediawiki/Special:VariablePage`
- For details on how to set up other types of extensions, see: <http://bit.ly/eaDnLT>

Coding Best Practices

- Security
- Scalability/Performance
- Security
- Concurrency
- Security

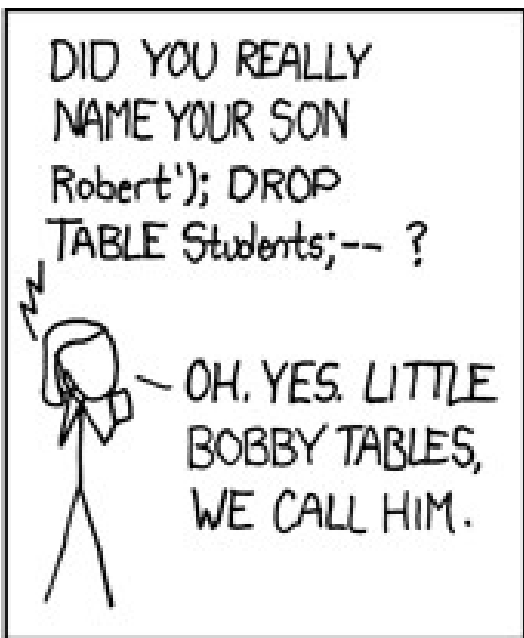
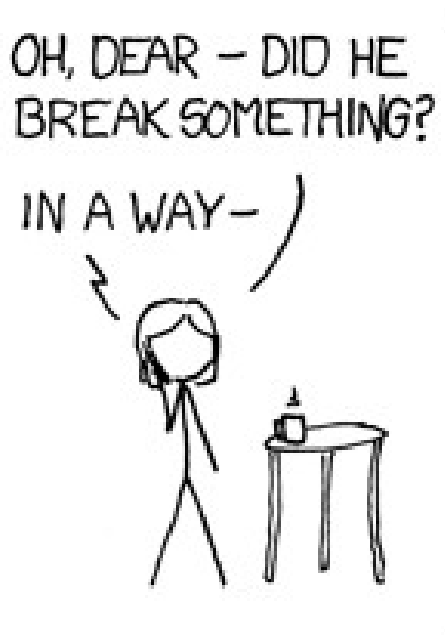
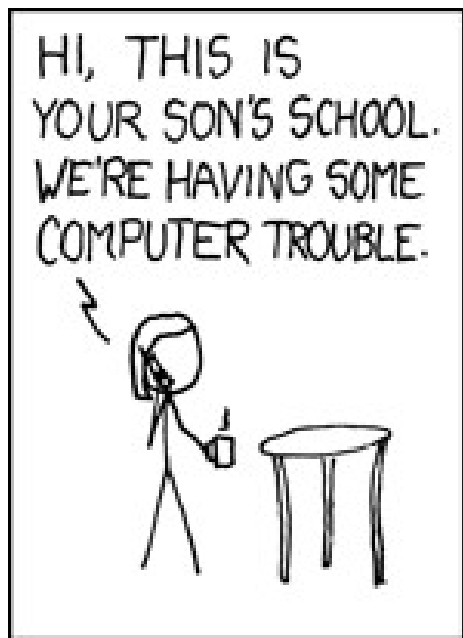
Security is Important. Really.

- Insecure extension in SVN = security risk for unwitting 3rd party admins and their users
- Insecure extension Wikipedia = potential security risk for hundreds of millions of users

Common Vulnerabilities to Avoid

- SQL Injection
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)

SQL Injection



SQL injection

Problem:

```
$sql = "INSERT INTO Students VALUES ($name, ... );";  
INSERT INTO Students VALUES ( 'Robert' ); DROP TABLE  
Students; --', ... );
```

SQL injection

Problem:

```
$sql = "INSERT INTO Students VALUES ($name, ... );";  
INSERT INTO Students VALUES ( 'Robert' ); DROP TABLE  
Students; --', ... );
```

Fix:

```
INSERT INTO Students VALUES ( 'Robert\'); DROP TABLE Students;  
-', ... );
```

Prevent SQL Injection with MW functions

BAD:

```
$dbr>query( "SELECT * FROM foo WHERE foo_id=' $id'" );
```

Acceptable:

```
$escID = $dbr>addQuotes( $id );
```

```
$dbr>query( "SELECT * FROM foo WHERE foo_id= $escID" );
```

Correct:

```
$dbr->select( 'foo', '*', array( 'foo_id' => $id ) );
```

XSS

Imagine:

```
40 $val = $wgRequest->getVal( 'input' );  
41 $wgOut->addHTML( "<input type=\"text\"  
value=\"$val\" />" );
```

XSS

Imagine:

```
40 $val = $wgRequest->getVal( 'input' );  
41 $wgOut->addHTML( "<input type=\"text\"  
value=\"\"$val\" />" );
```

User submits:

```
"/><script>do evil stuff</script>
```


XSS

Imagine:

```
40 $val = $wgRequest->getVal( 'input' );  
41 $wgOut->addHTML( "<input type=\"text\"  
value=\"\"$val\" />" );
```

User submits:

```
"/><script>do evil stuff</script>
```

EVIL STUFF GETS EXECUTED!!!

Preventing XSS

- ALWAYS escape inputs

```
39 ...
40 // better
41 $val = htmlspecialchars( $val );
42 $html = "<input type=\"text\"
name=\"foo\" value=\"$val\" />";
43
44 // best, using Mediawiki functions
45 $html = Html::input( 'foo', $val );
46 ...
```

EVIL STUFF DOESN'T GET EXECUTED :D

Cross Site Request Forgery (CSRF)

Insecure extension code:

```
40 ...
41 global $wgUser;
42 if ( $wgUser->isAllowed( 'delete' ) &&
isset( $_POST['delete'] ) ) {
43     $this->deleteItem( $_POST['delete'] );
44 }
45 ...
```

CSRF

Attack Vector:

'Bob' is logged in to Wikipedia. Mallory lures Bob to a website with the following HTML:

```
40 
```

CSRF

Attack Vector:

'Bob' is logged in to Wikipedia. Mallory lures Bob to a website with the following HTML:

```
40 
```

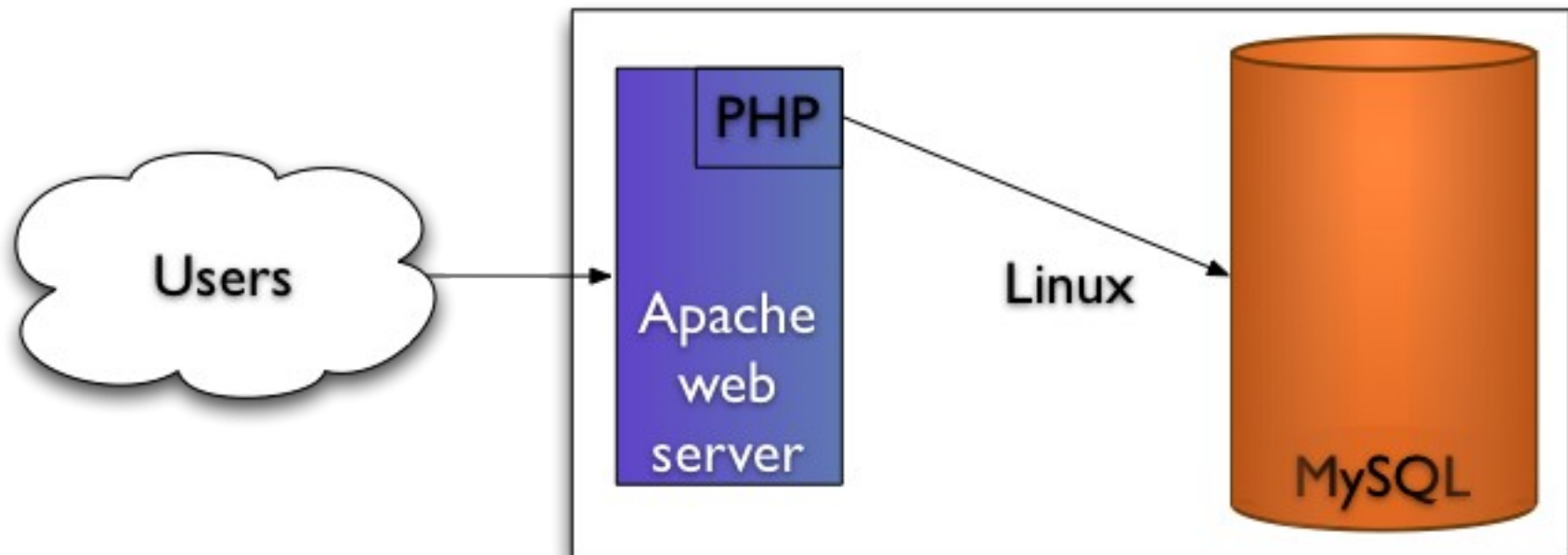
Article gets deleted by Bob,
but he doesn't know!!!

CSRF Prevention

```
40 ...
41 global $wgUser, $wgOut, $wgRequest;
42
43 $html .= Html::hidden( 'token',
    $wgUser->editToken() );
44 $wgOut->addHtml( $html );
45
46 ...
47 $token = $wgRequest->getText( 'token' )
48 if ( $wgUser->isAllowed( 'delete' )
49     && isset( $_POST['delete'] )
50     && $wgUser->matchEditToken( $token ) ) {
51     $this->deleteItem( $_POST['delete'] );
52 }
53 ...
```

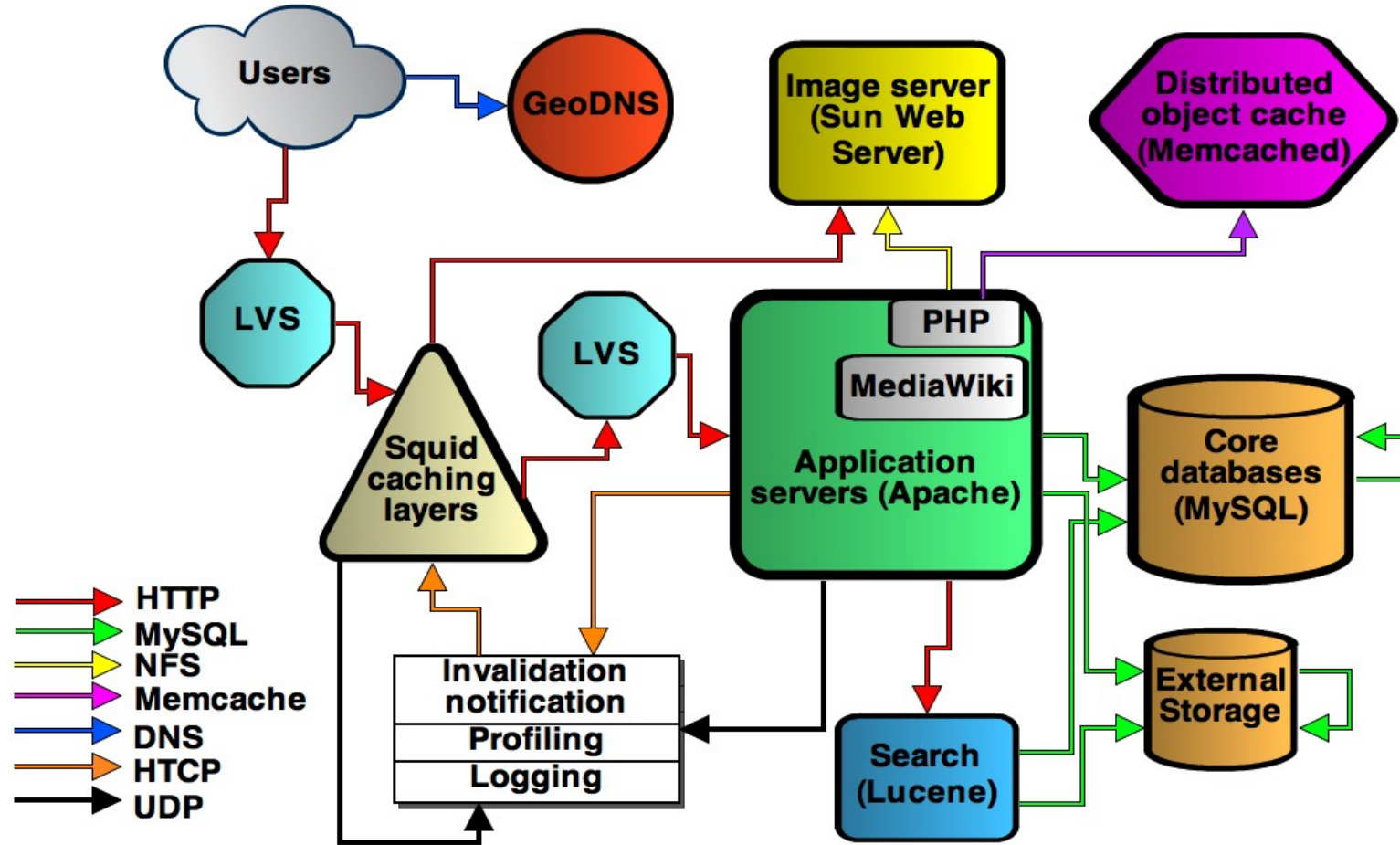
Scalability, Performance and Concurrency

Typical LAMP setup:



Scalability, Performance and Concurrency

On steroids:



Scalability, Performance and Concurrency

- Secure
- Performant
- Secure
- Scalable
- Secure
- Tolerant of concurrency
- Secure

I18n: VariablePage.i18n.php

- Translate performed by volunteers via translatewiki.net
- Putting the 'ww' in 'www'
- Even if you only know one language, your extension can be globally translingual
- Translations to your code happen automatically by SVN commits from translatewiki.net



translatewiki.net

MediaWiki:Viewdeleted_short/hi

Suggestions from translation memory

- ↓ देखें: {{बहुवचन: \$ 1 | एक संपादित नष्ट कर दिया | \$ 1 हटा}} संपादन | **Google**
- ↓ दृश्य {{बहुवचन:\$ 1|one हटा edit|\$ 1 हटाए गए संपादन}} | **Microsoft**
- ↓ {{PLURAL:\$1|एक हटाया हुआ|\$1 हटाये हुए}} बदलाव | **90.38% match •**

Information about message "Viewdeleted_short" (contribute)

Tab label for the undelete button when the user has permission to view the deleted history but not undelete.

Message definition (MediaWiki)

↓ View {{PLURAL:\$1|one deleted edit|\$1 deleted edits}}

Summary:

Save page (a) Save and open next (s) Skip to next (d)

MediaWiki	Current message text
↓ tog-nocache	!!FUZZY!!पन्ने कैश में ना रखें
↓ tog-externaleditor	!!FUZZY!!मूल रूप से बाह्य संपादन तंत्र का इस्तेमाल करें (केवल विशेषज्ञों के लिए, इसके लिए संगणक पर खास जमाव चाहिए होंगे)
↓ tog-externaldiff	!!FUZZY!!मूल रूप से अंतर देखने के लिए बाहरी तंत्र का इस्तेमाल करें (केवल विशेषज्ञों के लिए, इसके लिए संगणक पर खास जमाव करने होंगे)
↓ viewdeleted_short	View {{PLURAL:\$1 one deleted edit \$1 deleted edits}}
↓ pool-timeout	Timeout waiting for the lock
↓ pool-queuefull	Pool queue is full
↓ welcomecreation	स्वागत सृजन
↓ php-mail-error-unknown	Unknown error in PHP's mail() function

t and
ere!
nquiry

I18n Best Practices

- 'qqq'
- `wfmsg()` ;
- Only make message changes to 'en'
- Remove unused messages (only from 'en')

118n Best Practice Highlights

- Gender-specific, plurals, parameters all supported
- Avoid patchwork messages, but avoid message reuse
- Separate date and times in messages
- Do not include CSS/Javascript/HTML/etc
- Think about both LTR and RTL
- Avoid jargon/slang

I18n: not exactly intuitive

- Tough for new and veteran developers
- Thoroughly read the i18n guide for more:
<http://bit.ly/fjYtLX>
- TALK TO TRANSLATORS!
 - #mediawiki-i18n (irc.freenode.net)
 - <http://translatewiki.net/wiki/Support>

How to Engage the Community

- Discuss, Engage, Participate
- Mailing lists: (<http://bit.ly/77INC7>)
- IRC (#mediawiki on irc.freenode.net)
- Comment and document
- Commit your code (<http://bit.ly/hsTaIT>)

Community engagement best-practices

- Be patient...
- But don't expect patience
- RTFM
- Communicate changes
- Be concise
- Be HELPFUL
- Give credit where credit is due
- Return the favor
- CONTRIBUTE

IRC

#mediawiki

```
MediaWiki software support and dev: <http://www.mediawiki.org/> | Bugs: http://bit.ly/wmbugz | Read the FAQ <http://bit.ly/yr
10:57 < mw-bot2> http://www.mediawiki.org/wiki/Manual:$wgDifferenceEngine
11:02 < wikibugs> (NEW) I get redirected after rating a redirect page - https://bugzilla.wikimedia.org/27252 enhancement;
Normal; MediaWiki extensions: ReaderFeedback; (liangent)
11:02 -!- tomaszf [~tomaszf@216.219-78-194.adsl-static.isp.belgacom.be] has joined #mediawiki
11:03 -!- LauraHale [~laurahale@CPE-58-169-16-252.lns2.civ.bigpond.net.au] has quit [Quit: wiki wiki wiki wack!]
11:08 < wikibugs> (NEW) ref names should be anchor-decoded when displayed in error messages -
https://bugzilla.wikimedia.org/27253 enhancement; Normal; MediaWiki extensions: Cite; (liangent)
11:12 < Delta> !dump
11:12 < mw-bot2> For information on how to get dumps from Wikimedia Wikis, see http://meta.wikimedia.org/wiki/Data_dumps
11:12 < Delta> r!backupvision Log
11:12 < mw-bot2> See http://www.mediawiki.org/wiki/Manual:Backing_up_a_wiki for information about backing up your wiki. For
Revision 75285 - (strestoringyourwiki) see http://www.mediawiki.org/wiki/Manual:Moving_a_wiki#Import_the_database_backup
11:12 < codurr> hcatlin* (<http://www.mediawiki.org/wiki/Special:Code/MediaWiki/81714> /trunk/extensions/WikimediaMobile/
File size: 1950 bytes) (MobileRedirect.js user_agent_test.js):
11:12 < codurr> brion * <http://www.mediawiki.org/wiki/Special:Code/MediaWiki/81715> /trunk/phase3/skins/common/upload.js:
Don't throw JS error when AJAX license selection is on but there's no license selector because this is a
re-upload.
11:13 < codurr> brion * <http://www.mediawiki.org/wiki/Special:Code/MediaWiki/81716>
Special Page f /branches/wmf/1.17wmf1/skins/common/upload.js:
11:13 < codurr> MFT r81715
11:13 < codurr> Don't throw JS error when AJAX license selection is on but there's no license selector because this is a
re-upload.
11:13 < wikibugs> (FIXED) Regression: change to the redirection of the iPad users - https://bugzilla.wikimedia.org/27238
+comment (hcatlin)
11:13 -!- zaiphoooh [~zaiphoooh@194.19.110.196] has quit [Read error: Operation timed out]
11:14 < codurr> brion * <http://www.mediawiki.org/wiki/Special:Code/MediaWiki/81717>
/branches/REL1_17/phase3/skins/common/upload.js:
11:14 < codurr> MFT r81715
11:14 < codurr> Don't throw JS error when AJAX license selection is on but there's no license selector because this is a
re-upload.
11:14 < wikibugs> (FIXED) Android tablets that don't report themselves as "Mobile" should not redirect to mobile site -
https://bugzilla.wikimedia.org/27245 +comment (hcatlin)
11:15 |awjr(+i)| :9:#mediawiki(+cfjnt #wikimedia-overflow 5:10) |Act: 3 7 10
[#mediawiki]
```

Open Source Software Pro-tip

“The goal should be a solution to the problem – not simply inclusion of your code.”

- Jonathan Corbet (paraphrased from keynote address at FOSDEM 2011)

Absolutely Essential Reading

- Security for Developers: <http://bit.ly/1XFGPt>
- I18n guide: <http://bit.ly/esS0Bs>
- MW Coding conventions: <http://bit.ly/e9ASl9>
- How to become a Mediawiki Hacker:
<http://bit.ly/2rSaLX>

Key Resources

- [Http://www.mediawiki.org](http://www.mediawiki.org)
- [Http://wikitech.mediawiki.org](http://wikitech.mediawiki.org)
- <http://svn.wikimedia.org/doc/>
- <http://www.mediawiki.org/wiki/API>
- http://www.mediawiki.org/wiki/Security_for_developers
- http://www.mediawiki.org/wiki/How_to_become_a_MediaWiki_hacker
- IRC
 - #mediawiki
 - #mediawiki-dev

Any Questions?!

Special thanks to:

- Ryan Lane
- Roan Kattouw
- Tomasz Finc
- Danese Cooper
- Alolita Sharma
- Harshad, the rest of the staff and all of the awesomely energetic/enthusiastic students who helped put GNUunify on!
- SICSR

Presentation slides can be found at: <http://bit.ly/fJVTIN>



Self-introduction

- Name, where from, etc
- Time involved in FLOSS
- Time with the foundation
- What sort of stuff I work on
- Expertise (or lack of) in Mediawiki
- I'm a new Mediawiki Hacker!

What is Mediawiki anyway?

- GPL server-based Wiki software
- PHP and MySQL
- Community developed and maintained
- Powers Wikipedia and other Wikimedia projects

GPL

Software stack

Community developed/maintained

Powers Wikipedia, other projects

Runs on basic LAMP

Available for download/install by **ANYONE**

Welcome to Wikimedia

Wikimedia is owned and operated by the Wikimedia Foundation, a non-profit foundation dedicated to bringing free content to the world. The various Wikimedia projects are listed below:



a multilingual free
encyclopedia
Wiktionary
[ˈwɪkʃənəri] n.,
a wiki-based Open
Content dictionary
wɪkʃənəri [wɪkʃənəri]



Brief highlight of other projects

All powered by... Mediawiki!
Supported by the Foundation

Ok, but what is a 'wiki'?!

“A wiki (/ˈwiki/ WIK-ee) is a website that allows the creation and editing of any number of interlinked web pages via a web browser using a simplified markup language or a WYSIWYG text editor.”



- <http://en.wikipedia.org/wiki/Wiki>

- WikiWikiWeb by Ward Cunningham 1994
- So named b/c of Honolulu Airport employee saying 'take “wiki wiki shuttle”'
- Wiki literally means 'quick'
- Iwiki wiki sounds cooler than 'quick web'
- Intended for serious collaboration rather than just casual visitors
- Revision control – easy to CORRECT mistakes rather than making it difficult to MAKE them

Article Discussion Read Edit View history ☆ Search

Editing GNUUnify

From Wikipedia, the free encyclopedia

B *I*   [Advanced](#) [Special characters](#) [Help](#)

```

[[File:Gnunity.png|thumb|alt=GNUUnify Logo|GNUUnify Logo]]
'''GNUUnify''' is an annual gathering consisting of Workshops, Talks, Seminars and BOFs (Birds of a feather) held by the [[Pune Linux User Group]] [http://plug.org.in/] and the [[Symbiosis Institute of Computer Studies and Research (SICSR)|Symbiosis Institute of Computer Studies and Research]] in [[Pune]], [[India]]. It is an event held to help increase the awareness of [[FOSS]] in India especially in Pune.Its a forum to unite open minds.

GNUUnify (a play on the words [[GNU]] and Unify) is generally held during the second week of February. GNUUnify has featured eminent people like [[Richard Stallman]]<ref name="richard-stallman-gnunity">[http://gnu.gds.tuwin.ac.at/wwwin/events.html FSF India's events page in 2003]</ref>, [[Brian Behlendorf]], [[David Axmark]] <ref name="technetra-gnunity-2008">[http://opensourcebuzz.technetra.com/2008/02/18/gnunity-2008-it-only-gets-better Article in Feb 2008 on Technetra's Blog]</ref>, [[Danese Cooper]] <ref name="danese-blog">[http://danese.cooper.blogs.com/divablog/2006/02/gnunity_2006.html Danese Cooper's Blog entry on GNUUnify]</ref>, [[Robert Adkins]], [[Alolita Sharma]], Prof. [[Tony Wasserman]], Prof. [[Louis Pott]], Niyam Bhushan, Sankarshan, Zahira Bohrat and Anant Narayanan <ref name="technetra-gnunity-2009">[http://opensourcebuzz.technetra.com/2009/03/08/gnunity-2009-community-support-matters Technetra's Blog Entry on GNUUnify 2009]</ref> This year GNUUnify is going to be held in February on 11th and 12th with the name GNUUnify'11.The meetings have already started and the students of SICSR are ready with their ideas.

GNUUnify 2011 is scheduled on 11 & 12 February 2011.

== GNUUnify 2011==

As stated above, GNUUnify 2011 is scheduled to be held on the 11th and 12 of February, 2011.

```

- Invites ANY user to edit a web page in a web browser w/o addons
- Wiki markup for styling
- The idea is to make it easy to edit and apply styling without knowledge of HTML

Article [Discussion](#) [Read](#) [Edit](#) [View history](#)

Revision history of GNUify

From Wikipedia, the free encyclopedia
[View logs for this page](#)
 View or restore [4 deleted edits](#)?

Browse history

From year (and earlier): From month (and earlier): [all](#) Tag filter: Deleted only [Go](#)

For any version listed below, click on its date to view it. For more help, see [Help:Page history](#) and [Help:Edit summary](#).
 External tools: [Revision history statistics](#) · [Contributors](#) · [Revision history search](#) · [Number of watchers](#) · [Page view statistics](#)

(cur) = difference from current version, (prev) = difference from preceding version, **m** = *minor edit*, **→** = *section edit*, **←** = *automatic edit summary*

[Compare selected revisions](#) [Del/undelet selected revisions](#)

- [\(cur | prev\)](#) [08:27, 7 February 2011](#) [Giraffedata](#) ([talk](#) | [contribs](#)) (3,224 bytes) ("*comprising of*") ([undo](#))
- [\(cur | prev\)](#) [20:14, 26 January 2011](#) [Birajdarpriyanka22](#) ([talk](#) | [contribs](#)) (3,224 bytes) ([undo](#))
- [\(cur | prev\)](#) [18:59, 22 January 2011](#) [122.169.12.183](#) ([talk](#)) (3,224 bytes) (*→Tracks*) ([undo](#))
- [\(cur | prev\)](#) [17:55, 21 January 2011](#) [AninditAdhikary](#) ([talk](#) | [contribs](#)) (2,984 bytes) ([undo](#))
- [\(cur | prev\)](#) [10:55, 14 January 2011](#) [202.71.143.2](#) ([talk](#)) (2,980 bytes) ([undo](#))
- [\(cur | prev\)](#) [13:27, 7 December 2010](#) [Tej10030142085](#) ([talk](#) | [contribs](#)) (2,314 bytes) (*→Tracks*) ([undo](#))
- [\(cur | prev\)](#) [13:26, 7 December 2010](#) [Tej10030142085](#) ([talk](#) | [contribs](#)) (2,367 bytes) ([undo](#))
- [\(cur | prev\)](#) [17:47, 25 August 2010](#) [Kezbeth](#) ([talk](#) | [contribs](#)) (2,367 bytes) (*cat*) ([undo](#))

-
- Intended for serious collaboration rather than just casual visitors
- Revision control – easy to CORRECT mistakes rather than making it difficult to MAKE them

Article [Discussion](#) [Read](#) [Edit](#) [View history](#) ☆ ▼

GNUUnify

From Wikipedia, the free encyclopedia
(Difference between revisions)

Revision as of 20:14, 26 January 2011 (edit)
Birajdarpriyanka22 (talk | contribs)
(del/unde)
← Previous edit

Current revision as of 08:27, 7 February 2011 (edit) (undo)
Giraffedata (talk | contribs)
("comprising of") (del/unde)

Line 1:

<pre>[[File:Gnunity.png thumb alt=GNUUnify Logo GNUUnify Logo]] '''GNUUnify''' is an annual gathering comprising of Workshops, Talks, Seminars and BOFs (Birds of a feather) held by the [[Pune Linux User Group]] [http://plug.org.in/] and the - [[Symbiosis Institute of Computer Studies and Research (SICSR) Symbiosis Institute of Computer Studies and Research]] in [[Pune]], [[India]]. It is an event held to help increase the awareness of [[FOSS]] in India especially in Pune.Its a forum to unite open minds.</pre>	<pre>[[File:Gnunity.png thumb alt=GNUUnify Logo GNUUnify Logo]] '''GNUUnify''' is an annual gathering consisting of Workshops, Talks, Seminars and BOFs (Birds of a feather) held by the [[Pune Linux User Group]] [http://plug.org.in/] and the + [[Symbiosis Institute of Computer Studies and Research (SICSR) Symbiosis Institute of Computer Studies and Research]] in [[Pune]], [[India]]. It is an event held to help increase the awareness of [[FOSS]] in India especially in Pune.Its a forum to unite open minds.</pre>
<pre>GNUUnify (a play on the words [[GNU]] and Unify) is generally held during the second week of February. GNUUnify has featured eminent people like [[Richard Stallman]]<ref name="richard-stallman-gnunity">[http://gnu.gds.tuwien.ac.at/wwwin/events.html FSF India's events page in 2003]</ref>, [[Brian Behlendorf]], [[David Axmark]] <ref name="technetra-gnunity-2008">[http://opensourcebuzz.technetra.com/2008/02/18/gnunity-2008-it-only-gets-better Article in Feb 2008 on Technetra's Blog]</ref>.</pre>	<pre>GNUUnify (a play on the words [[GNU]] and Unify) is generally held during the second week of February. GNUUnify has featured eminent people like [[Richard Stallman]]<ref name="richard-stallman-gnunity">[http://gnu.gds.tuwien.ac.at/wwwin/events.html FSF India's events page in 2003]</ref>, [[Brian Behlendorf]], [[David Axmark]] <ref name="technetra-gnunity-2008">[http://opensourcebuzz.technetra.com/2008/02/18/gnunity-2008-it-only-gets-better Article in Feb 2008 on Technetra's Blog]</ref>.</pre>

The diffs, to see what changed

Why should I hack Mediawiki?

- Because you can
- Fix a problem with the software
- 'Scratch an itch'
- Public work record
- Mentor and be mentored
- Put the 'ww' in 'www'
- Support an awesome vision


Imagine a world in which every single human being can freely share in the sum of all knowledge.

- * Global community
- * Why is the community awesome?

Hacking the Software: What to Hack

- Bug fixes (<http://bit.ly/geY1u0>)
- Core code (<http://bit.ly/geY1u0>)
- Parser hooks
- External tools with the API (<http://bit.ly/eBloi>)
- SpecialPages (<http://bit.ly/323H1o>)

Template hacking/parser hooks:

parser function extensions  for pimping out templates {to handle wiki text generation that involves logic that is too complex or confusing to write using

normal http://www.mediawiki.org/w/index.php?title=Manual:Developing_extensions template-writing techniques.}

variable extensions  extending parameters in templates

extending syntax, etc

Diving in with VariablePage extension



<http://www.flickr.com/photos/aknacer/2588798719/>

Extension developed for the fundraiser

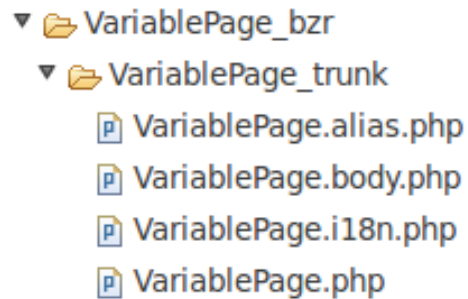
To facilitate A/B testing

Gives you the ability to psuedo-randomly send users to a particular page x% of the time

How we used it during the fundraiser

VariablePage

```
$ svn co \  
http://svn.wikimedia.org/svnroot/mediawiki/  
trunk/extensions/VariablePage
```



We have a SVN repository that is free and accessible for anyone to check out from.

To be able to commit, you need special permission

How to get the extension

Code layout

Setup: ExtensionName.php

Goal:

To simplify and centralize installation and configuration

```
1 <?php
2 require_once( "$IP/extensions/ExtensionName/Ext
  extensionName.php" );
3 $wgExtNameFoo = true;
4 $wgExtNameBar = 'baz';
...

```

Open VariablePage.php

- define/validate configuration variables in global scope
- over-rideable in LocalSettings
- Give them GOOD UNIQUE NAME
- extensive documentation = GOOD
- auto-load classes
- immediate/deferred setup
- define hook functions

Open up LocalSettings.php

Setup... continued

- Possible to defer extension setup until after LocalSettings.php has been run

```
1 <?php
2 ...
3 ...
4 ...
5 $wgExtensionFunctions[] = 'efExtensionNameSetup';
6
7 function efExtensionNameSetup() {
8     # do post-setup stuff here
9 }
...

```

This is handy for using variables/scripts that might not be loaded when LocalSettings first gets to your script

Setup: database tables

```
39 ...
40 # Schema updates for update.php
41 $wgHooks['LoadExtensionSchemaUpdates'][] = 'fnMyHook';
42 function fnMyHook() {
43     global $wgExtNewTables, $wgExtModifiedFields;
44     $wgExtNewTables[] = array(
45         'tablename',
46         dirname( __FILE__ ) . '/table.sql'
47     );
48     $wgExtModifiedFields[] = array(
49         'table',
50         'field_name',
51         dirname( __FILE__ ) .
52         '/table.patch.field_name.sql'
53     );
54     return true;
55 }
```

- <http://bit.ly/fk9uyf>

Not covering in detail

Possible to load db schema stuffs via setup file

Execution: VariablePage.body.php

- 'VariablePage' is a 'SpecialPage' extension
- `function execute() {}`
- <http://path/to/mediawiki/Special:VariablePage>
- For details on how to set up other types of extensions, see: <http://bit.ly/eaDnLT>

Open VariablePage.body.php

Demonstrate

Show execution, go over code

Coding Best Practices

- Security
- Scalability/Performance
- Security
- Concurrency
- Security

Did I mention, 'Security'?

Security is Important. Really.

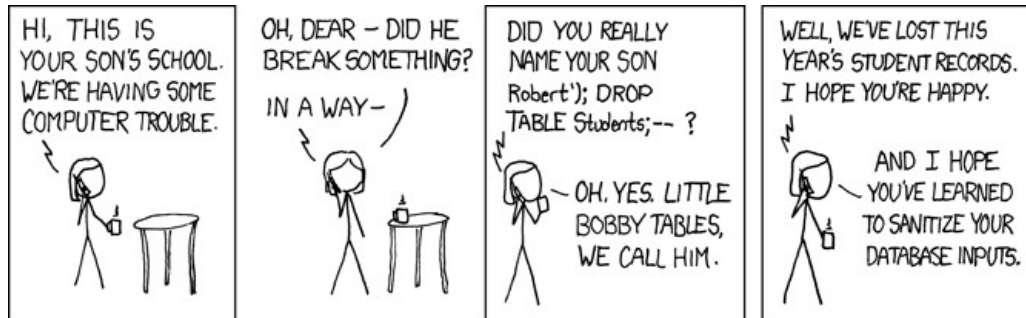
- Insecure extension in SVN = security risk for unwitting 3rd party admins and their users
- Insecure extension Wikipedia = potential security risk for hundreds of millions of users

Common Vulnerabilities to Avoid

- SQL Injection
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)

There are of course others, but these are the most common ones that are easy to defend against

SQL Injection



haha

SQL injection

Problem:

```
$sql = "INSERT INTO Students VALUES ($name, ... );";  
INSERT INTO Students VALUES ( 'Robert' ); DROP TABLE  
Students; --', ... );
```

User inserts malicious query into a text input or
whatevs, which can cause bad things to happen.

SQL injection

Problem:

```
$sql = "INSERT INTO Students VALUES ($name, ... );";  
INSERT INTO Students VALUES ( 'Robert' ); DROP TABLE  
Students; --', ... );
```

Fix:

```
INSERT INTO Students VALUES ( 'Robert\'); DROP TABLE Students;  
-', ... );
```

Prevent SQL Injection with MW functions

BAD:

```
$dbr->query( "SELECT * FROM foo WHERE foo_id=' $id'" );
```

Acceptable:

```
$escID = $dbr->addQuotes( $id );
```

```
$dbr->query( "SELECT * FROM foo WHERE foo_id= $escID" );
```

Correct:

```
$dbr->select( 'foo', '*', array( 'foo_id' => $id ) );
```

Considered extra nice if you use the built-in mediawiki functions (roan says Tim will like you more)

XSS

Imagine:

```
40 $val = $wgRequest->getVal( 'input' );  
41 $wgOut->addHTML( "<input type=\"text\"  
value=\"\"$val\" />" );
```

XSS

Imagine:

```
40 $val = $wgRequest->getVal( 'input' );  
41 $wgOut->addHTML( "<input type=\"text\"  
value=\"$val\" />" );
```

User submits:

```
"/><script>do evil stuff</script>
```

XSS

Imagine:

```
40 $val = $wgRequest->getVal( 'input' );  
41 $wgOut->addHTML( "<input type=\"text\"  
value=\""$val\" />" );
```

User submits:

```
"/><script>do evil stuff</script>
```

EVIL STUFF GETS EXECUTED!!!

Exploits trust a user has in a site, or link

One of many scenarios:

- * Bob's website has an XSS vulnerability
- * Alice crafts a URL with malicious code in the `$_GET` or `$_POST`, and sends it to Bob
- * Bob clicks link, executing Alice's malicious script in Bob's browser
- * Could allow Alice to steal sensitive information otherwise only available to Bob

Preventing XSS

- ALWAYS escape inputs

```
39 ...
40 // better
41 $val = htmlspecialchars( $val );
42 $html = "<input type=\"text\"
name=\"foo\" value=\"$val\" />";
43
44 // best, using Mediawiki functions
45 $html = Html::input( 'foo', $val );
46 ...
```

EVIL STUFF DOESN'T GET EXECUTED :D

MW functions like `Html::input()` automatically sanitize input so you don't have to worry about it

Cross Site Request Forgery (CSRF)

Insecure extension code:

```
40 ...
41 global $wgUser;
42 if ( $wgUser->isAllowed( 'delete' ) &&
isset( $_POST['delete'] ) ) {
43     $this->deleteItem( $_POST['delete'] );
44 }
45 ...
```

Sometimes pronounced 'Sea Surf' because it allows for 'session riding' – essentially hijacking a user's session.

Exploits the trust a site has in a browser

CSRF

Attack Vector:

'Bob' is logged in to Wikipedia. Mallory lures Bob to a website with the following HTML:

```
40 
```

CSRF

Attack Vector:

'Bob' is logged in to Wikipedia. Mallory lures Bob to a website with the following HTML:

```
40 
```

Article gets deleted by Bob,
but he doesn't know!!!

CSRF Prevention

```
40 ...
41 global $wgUser, $wgOut, $wgRequest;
42
43 $html .= Html::hidden( 'token',
    $wgUser->editToken() );
44 $wgOut->addHtml( $html );
45
46 ...
47 $token = $wgRequest->getText( 'token' )
48 if ( $wgUser->isAllowed( 'delete' )
49     && isset( $_POST['delete'] )
50     && $wgUser->matchEditToken( $token ) ) {
51     $this->deleteItem( $_POST['delete'] );
52 }
53 ...
```

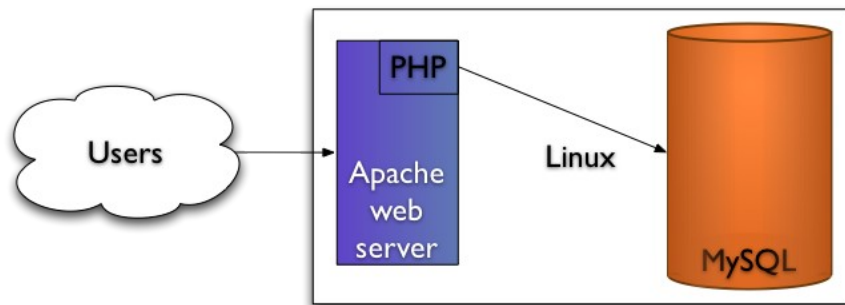
Easy to prevent with token checking

- * token gets generated and stored in a cookie
- * a hash of token (plus a salt) gets stored in a hidden form field
- * on form submit, logic checks to see if the salt + token hash from the cookie matches that of the form submit

If mismatch, session is considered 'over' and request invalid

Scalability, Performance and Concurrency

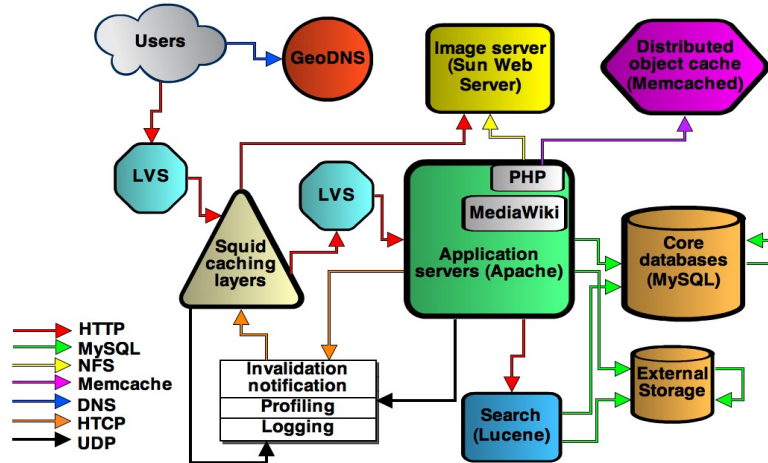
Typical LAMP setup:



Mediawiki is cool because it can run on such a simple, basic set up

Scalability, Performance and Concurrency

On steroids:



But we put the setup on 'roids.

Introduces a level of complexity that coder must be aware of

Scalability, Performance and Concurrency

- Secure
- Performant
- Secure
- Scalable
- Secure
- Tolerant of concurrency
- Secure

* High performance code that's not going to crash under load

* Concurrency problems:

** On Wikipedia, we use many DB's – selecting which DB to use is possible in the code

** Database lag (use DB_MASTER for reads if data needs to be up-to-date)

** Attaching timestamps to things like counters is a good idea

I18n: VariablePage.i18n.php

- Translate performed by volunteers via translatewiki.net
- Putting the 'ww' in 'www'
- Even if you only know one language, your extension can be globally translingual
- Translations to your code happen automatically by SVN commits from translatewiki.net

Overview of i18n

You only need to know 1 language, but your code will work in useable by many!

SUPER COOL! Go Translators!!!

Go over the i18n file

Demonstrate on the localhost!



translatewiki.net

MediaWiki:Viewdeleted_short/hi

Suggestions from translation memory

- देखें: {{संयोजन:\$ 1 | एक संयोजित नोट कर दिया | \$ 1 हटा}} संयोजन | Google
- दृश्य {{संयोजन:\$ 1|one हटा edit|\$ 1 हटाए गए संयोजन}} | Microsoft
- {{PLURAL:\$1एक हटाया हुआ|\$1 हटाये हुए}} बदलाव | 90.38% match •

Information about message "Viewdeleted_short" (contribute)

Tab label for the undelete button when the user has permission to view the deleted history but not undelete.

Message definition (MediaWiki)

View {{PLURAL:\$1|one deleted edit|\$1 deleted edits}}

Summary: Save page (a) Save and open next (s) Skip to next (d)

MediaWiki	Current message text
↓tog-nocache	!!FUZZY!!पन्ने कैश में ना रखें
↓tog-externaleditor	!!FUZZY!!मूल रूप से बाह्य संयोजन तंत्र का इस्तेमाल करें (केवल विशेषज्ञों के लिए, इसके लिए संगणक पर खास जमाव चाहिए होंगे)
↓tog-externaldiff	!!FUZZY!!मूल रूप से अंतर देखने के लिए बाहरी तंत्र का इस्तेमाल करें (केवल विशेषज्ञों के लिए, इसके लिए संगणक पर खास जमाव करने होंगे)
↓viewdeleted_short	View {{PLURAL:\$1 one deleted edit \$1 deleted edits}}
↓pool-timeout	Timeout waiting for the lock
↓pool-queuefull	Pool queue is full
↓welcomecreation	स्वागत सृजन
↓php-mail-errno-unknown	Unknown error in PHP's mail() function

Example of translation interface on translate wiki.

Anyone can do it!

EN → Hindi

I18n Best Practices

- 'qqq'
- wfmsg();
- Only make message changes to 'en'
- Remove unused messages (only from 'en')

Be sure to explain your messages in the 'qqq' array – it is reserved for documentation

Typically, messages are initially written in English

Removing your message from English will automatically remove the corresponding messages from other langs

I18n Best Practice Highlights

- Gender-specific, plurals, parameters all supported
- Avoid patchwork messages, but avoid message reuse
- Separate date and times in messages
- Do not include CSS/Javascript/HTML/etc
- Think about both LTR and RTL
- Avoid jargon/slang

I18n: not exactly intuitive

- Tough for new and veteran developers
- Thoroughly read the i18n guide for more:
<http://bit.ly/fjYtLX>
- TALK TO TRANSLATORS!
 - #mediawiki-i18n (irc.freenode.net)
 - <http://translatewiki.net/wiki/Support>

How to Engage the Community

- Discuss, Engage, Participate
- Mailing lists: (<http://bit.ly/77INC7>)
- IRC (#mediawiki on irc.freenode.net)
- Comment and document
- Commit your code (<http://bit.ly/hsTaIT>)

Community engagement best-practices

- Be patient...
- But don't expect patience
- RTFM
- Communicate changes
- Be concise
- Be HELPFUL
- Give credit where credit is due
- Return the favor
- CONTRIBUTE

IRC

#mediawiki

```
MediaWiki software support and dev: <http://www.mediawiki.org/> | Bugs: http://bit.ly/wmbugz | Read the FAQ <http://bit.ly/yr
10:57 < mw-bot2> http://www.mediawiki.org/wiki/Manual:SwgDifferenceEngine
11:02 < wikibugs> (NEW) I get redirected after rating a redirect page - https://bugzilla.wikimedia.org/27252 enhancement;
Normal; MediaWiki extensions; ReaderFeedback; (Liangent)
11:02 -!- tomaszf [-tomaszf@216.219.78.194.adsl-static.isp.belgacom.be] has joined #mediawiki
11:03 -!- LauraHale [-laurahale@CPE-58-169-16-252.lns2.civ.bigpond.net.au] has quit [Quit: wiki wiki wack!]
11:08 < wikibugs> (NEW) ref names should be anchor-decoded when displayed in error messages -
https://bugzilla.wikimedia.org/27253 enhancement; Normal; MediaWiki extensions; Cite; (Liangent)
11:12 < Delta> !dump
11:12 < mw-bot2> For information on how to get dumps from Wikimedia Wikis, see http://meta.wikimedia.org/wiki/Data_dumps
11:12 < Delta> !backupvisionlog
11:12 < mw-bot2> See http://www.mediawiki.org/wiki/Manual:Backing_up_a_wiki_for_information_about_backing_up_your_wiki. For
Revision 75285 - @restoring your wiki, see http://www.mediawiki.org/wiki/Manual:Moving_a_wiki#Import_the_database_backup
11:12 < codurr> hcatlin * <http://www.mediawiki.org/wiki/Special:Code/MediaWiki/81714> /trunk/extensions/WikimediaMobile/
File size: 1950 bytes
11:12 < codurr> brion * <http://www.mediawiki.org/wiki/Special:Code/MediaWiki/81715> /trunk/phase3/skins/common/upload.js:
Don't throw JS error when AJAX license selection is on but there's no license selector because this is a
re-upload.
11:13 < codurr> brion * <http://www.mediawiki.org/wiki/Special:Code/MediaWiki/81716>
Special:Code/MediaWiki/81716
/branches/wmf/1.17wmf1/skins/common/upload.js:
11:13 < codurr> MFT r81715
11:13 < codurr> Don't throw JS error when AJAX license selection is on but there's no license selector because this is a
re-upload.
11:13 < wikibugs> (FIXED) Regression: change to the redirection of the iPad users - https://bugzilla.wikimedia.org/27238
+comment (hcatlin)
11:13 -!- zaiphoo [-zaiphoo@194.19.110.196] has quit [Read error: Operation timed out]
11:14 < codurr> brion * <http://www.mediawiki.org/wiki/Special:Code/MediaWiki/81717>
/branches/REL1_17/phase3/skins/common/upload.js:
11:14 < codurr> MFT r81715
11:14 < codurr> Don't throw JS error when AJAX license selection is on but there's no license selector because this is a
re-upload.
11:14 < wikibugs> (FIXED) Android tablets that don't report themselves as "Mobile" should not redirect to mobile site -
https://bugzilla.wikimedia.org/27245 +comment (hcatlin)
11:15 awjr( 1) 9:#mediawiki( Cfjnt #wikimedia-overflow 5:10) Act: 3 7 10
[#mediawiki]
```

See, it's neat!

Plus when you contribute or do something with a bug, the bot tells the channel. People watch this and will see what you're up to and often engage YOU

Open Source Software Pro-tip

“The goal should be a solution to the problem – not simply inclusion of your code.”

- Jonathan Corbet (paraphrased from keynote address at FOSDEM 2011)

This is paraphrased.

The point is, LET GO OF CONTROL.

Absolutely Essential Reading

- Security for Developers: <http://bit.ly/1XFGPt>
- I18n guide: <http://bit.ly/esS0Bs>
- MW Coding conventions: <http://bit.ly/e9ASl9>
- How to become a Mediawiki Hacker:
<http://bit.ly/2rSaLX>

Key Resources

- [Http://www.mediawiki.org](http://www.mediawiki.org)
- [Http://wikitech.mediawiki.org](http://wikitech.mediawiki.org)
- <http://svn.wikimedia.org/doc/>
- <http://www.mediawiki.org/wiki/API>
- http://www.mediawiki.org/wiki/Security_for_developers
- http://www.mediawiki.org/wiki/How_to_become_a_MediaWiki_hacker
- IRC
 - #mediawiki
 - #mediawiki-dev

Any Questions?!

Special thanks to:

- Ryan Lane
- Roan Kattouw
- Tomasz Finc
- Danese Cooper
- Alolita Sharma
- Harshad, the rest of the staff and all of the awesomely energetic/enthusiastic students who helped put GNUify on!
- SICSR

Presentation slides can be found at: <http://bit.ly/fJVTIN>