DRUPALCON
ASIA
2016

How to publish a Module on drupal.org

Klaus Purer // klausi

Session Track: Contributions
February 2016

whoami

- drupal.org: klausi   Twitter: @_klausi_
- Software Engineer at epiqo
- drupal.org project application admin
- Security Team member
- Drupal 8 Rules and REST module maintainer
- Coding Standards maintainer (Coder)

Contribution

Before you start

❖ Duplication: does the module already exist?

❖ Join forces! Collaboration over competition

❖ Utility: is this useful for others?

❖ Dedication: can I maintain this?

Sandboxes

https://www.drupal.org/sandbox/klausi/2294607

← Sandbox URL

test sandbox

klausi's sandbox: test sandbox

View   Version control

Posted by klausi on *June 29, 2014 at 10:58am*

← Experimental warning

Experimental Project

This is a sandbox project, which contains experimental code for developer use only.

only testing!

Project Information

no releases

Maintenance status: Actively maintained
Development status: Under active development
Last modified: June 29, 2014

Rules

Namespaced URL

Full projects

View **Version control** **Automated Testing**

Posted by fago on *November 7, 2007 at 1:34pm*

The Rules module allows site administrators to define conditionally executed actions based on occurring events (known as reactive or ECA rules). It's a replacement with more features for the trigger module in core and the successor of the Drupal 5 workflow-ng module.

Example use cases

- Build flexible content publishing workflows changes
- Send customized mails to notify your users about important

Downloads

Recommended releases

> ⓘ   This module has a pre-release version for Drupal 8. To find out more, follow this **issue** or download below.

Packaged Downloads

Version	Download	Date
7.x-2.9	tar.gz (184.45 KB) | zip (223.02 KB)	2015-Mar-16
6.x-1.5	tar.gz (91.22 KB) | zip (119.68 KB)	2012-Aug-03

Other releases

Version	Download	Date
8.x-3.0-unstable7	tar.gz (137.18 KB) | zip (303.13 KB)	2016-Feb-01

Abandoned projects

- ❖ Take over unmainted projects instead of publishing a fork
- ❖ Avoids duplication
- ❖ Your code gets to a well known place already
- ❖ Existing users benefit of your new developments
- ❖ If the maintainer does not respond you can get access in 2-3 weeks
- ❖ Instructions: https://www.drupal.org/node/251466

❖ Required to push your code to drupal.org

❖ Version control tab on every project

❖ Branch name: 8.x-1.x

❖ Tag name: 8.x-1.0-beta1

❖ Docs: https://www.drupal.org/documentation/git

Coding Standards

❖ Important for readable & understandable code

❖ Whitespace and indentation

❖ Naming conventions

❖ Inline documentation of classes and functions

❖ Docs: https://www.drupal.org/coding-standards/

Coder + PHPCS

```
$ phpcs --standard=Drupal example.module

FILE: /home/klausi/workspace/coder/example.module
--------------------------------------------------------------------------------
FOUND 3 ERRORS AFFECTING 3 LINES
--------------------------------------------------------------------------------
3 | ERROR | [ ] Missing function doc comment
4 | ERROR | [ ] Opening brace should be on the same line as the declaration
5 | ERROR | [x] Line indented incorrectly; expected 2 spaces, found 1
--------------------------------------------------------------------------------
PHPCBF CAN FIX THE 1 MARKED SNIFF VIOLATION AUTOMATICALLY
--------------------------------------------------------------------------------
```

❖ Detects coding standard problems

❖ Can fix coding standard problems automatically

❖ Docs: https://www.drupal.org/project/coder

ESLint

```
$ eslint --config drupal-8/.eslintrc example.js
example.js: line 8, col 1, Error - Use the function form of 'use strict'. (strict)
example.js: line 8, col 10, Error - 'stationMap' is defined but never used (no-unused-vars)
example.js: line 34, col 55, Error - Don't make functions within a loop (no-loop-func)

3 problems
```

❖ Checks coding standards in JavaScript files
❖ Drupal 8 ships with a .eslintrc config file
❖ http://eslint.org

http://pareview.sh

DRUPALCON ASIA 2016

pareview.sh

Resources for Drupal Project Application reviewers

I receive **anonymously** on **Gratipay**.

Automated project review | Project application checklist

Review a drupal.org project online

About

This service performs automated reviews of drupal.org projects using klausi's PAReview.sh script. It is intended to ease the review of project applications but can be used to check any other project as well. This online service provides the recent pareview script without installing a local testing environment.

Used PHP CodeSniffer standards:

Review a branch

URL to git repository [optional: branch name] *

Example usage:
http://git.drupal.org/sandbox/patrickd/1182300.git
http://git.drupal.org/project/fail.git
http://git.drupal.org/project/fail.git 7.x-1.x

Submit branch

Licensing: GPLv2+

- ❖ **All code on drupal.org is automatically GPLv2+**
- ❖ **No third party code allowed in git**
- ❖ **Libraries API to include third party code**

Security

Security Review

- ❖ Most important: your code should not be a threat
- ❖ How could an attacker abuse your module?
- ❖ What weaknesses does your code contain?
- ❖ Is your code ready for a production web site?
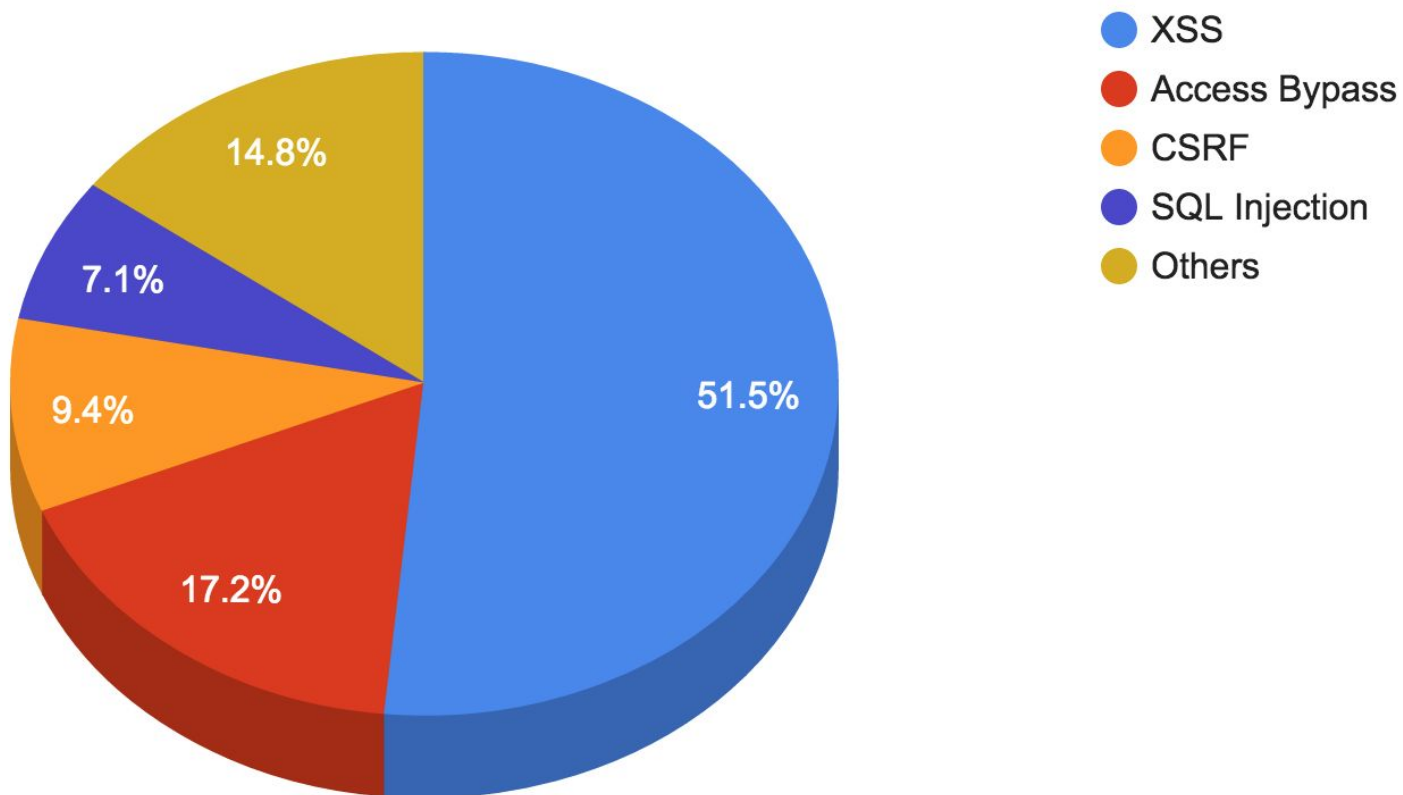- ❖ Are you familiar with security concepts in Drupal?
- ❖ https://www.drupal.org/writing-secure-code

Security vulnerabilities

Vulnerabilities in Drupal Contrib

- XSS
- Access Bypass
- CSRF
- SQL Injection
- Others

51.5%
17.2%
9.4%
7.1%
14.8%

Cross Site Scripting (XSS)

❖ Reflected XSS example:

```php
<?php
print 'You are on page number ' . $_GET['number'];
?>
```

❖ HTML:

```
You are on page number <script>alert("XSS");</script>
```

❖ Always sanitize user provided text (Drupal 7)

❖ Drupal 8: Twig auto escaping helps a lot

Cross sIte Request Forgery (CSRF)

❖ Changing data without verifying intent

`<img src="http://example.com/node/1/quickdelete" >`

❖ trick admins into executing actions by just following a link

❖ Fix: use confirmation forms or

❖ use per user tokens in the path with drupal_get_token() and drupal_validate_token()

`/node/1/quickdelete?token=tieya9bahhaeKeen6Oow`

Do you see the pattern?

❖ Don't trust any user provided data in the URL, the request, or content in the database.

❖ Attackers exploit missing/weak access control (permission setup)

❖ Attackers use browser features to perform actions behind the user's back (XSS, CSRF, open redirects).

Workflow

Review Checklist

- ❖ Duplication
- ❖ Security
- ❖ Licensing
- ❖ Documentation
- ❖ Coding Standards
- ❖ API usage and best practices
- ❖ This list explained at https://www.drupal.org/node/1587704

Project application queue

- ❖ Applying for permissions to create full projects
- ❖ A usual issue queue
- ❖ Other people review your code

https://www.drupal.org/project/projectapplications

Application workflow

- ❖ You open the application "needs review"
- ❖ Reviewer finds major problem: "needs work"
- ❖ You fix the problem: "needs review"
- ❖ Reviewer OK: "reviewed & tested by the community
- ❖ Git admin approves: "fixed"
- ❖ You get the "git vetted user role" and can promote your project(s)

Problems

Problems

- ❖ Very long wait times for applicants (months)
- ❖ Too few regular reviewers and git admins
- ❖ Only projects of new contributors need to get reviewed (unfair?)
- ❖ Superficial feedback

FFFFFFF
FFFFFFF
FFFFFF
FFFUU
UUUU
UUUU
UUUU
UUUU-
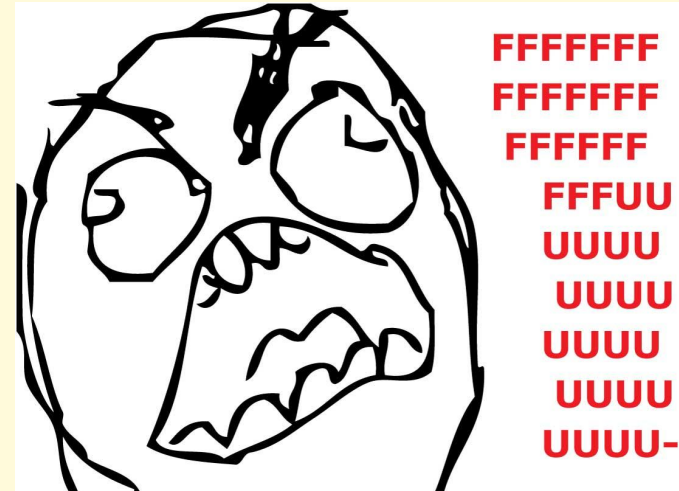
Considerations

Why can't just everyone publish projects?

❖ Prevent name space squatting by random users

❖ Security team wants to support all of contrib

❖ Drupal's reputation about contributed modules

❖ Encourage collaboration over competition
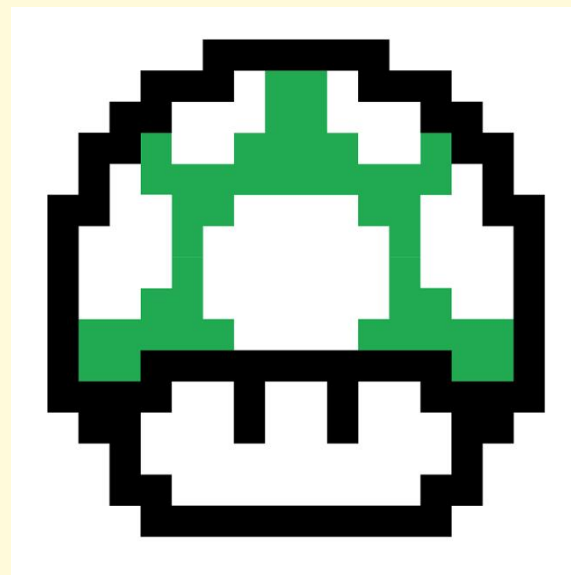
Review Bonus

Problem:

Lack of reviewers

Solution:

Applicants become reviewers

- ❖ 3 reviews of other projects
- ❖ issue tag "PAReview: review bonus"
- ❖ high priority list

Community networking

- ❖ Use and make connections with Druplistas
- ❖ Ask colleagues/friends to review your code
- ❖ Local meetups & user groups
- ❖ IRC
- ❖ Drupal Answers
- ❖ Blog about your project
- ❖ Help and contribute to make yourself known

Benefits of reviewing

- ❖ Learn Drupal by reviewing code
- ❖ Learn about alternative ways
- ❖ Learn how to analyze foreign code
- ❖ Learn how to write secure code
- ❖ Learn about best and worst practices
- ❖ Stay on top of what is new and hot
- ❖ Build your Drupal career by helping and mentoring

Plans

Plans

- ❖ Automated reviews integrated into drupal.org
- ❖ Every non-vetted user can promote 1 sandbox
- ❖ No stable releases (only alphas, betas, RCs)
- ❖ No security team support for unstable releases
- ❖ Same approval process after that
- ❖ See https://www.drupal.org/node/2453587

Get involved!

❖ Join the group of reviewers
   https://groups.drupal.org/code-review
❖ Become a git admin on drupal.org yourself
❖ Help implement the drupal.org plans
❖ Join the code sprints on Sunday
   https://events.drupal.org/asia2016/sprints

Questions?

DRUPALCON
ASIA
2016

WHAT DID YOU THINK?
EVALUATE THIS SESSION

asia2016.drupal.org/schedule