Plugin Review

report_myfeedback

For

UCL

by

Catalyst IT Europe Limited

Version: 1.0

February 2021

Commercial in Confidence

catalyst

open source technologists

Olivier House, 18 Marine Parade, Brighton, East Sussex, BN2 1TL, United Kingdom
+44 (0) 1273 929 450 // info@catalyst-eu.net // www.catalyst-eu.net

Table of Contents

Revision History			
Modified By	**Date**	**Version**	**Change**
Conn Warwicker	16 Feb 2021	1.0	Initial Retroactive Review

Introduction

Overview

The following review of the report_myfeedback plugin has been carried out in accordance with our Code and Deployment Process Standard.

Summary

The plugin report_myfeedback falls into the ● **High Risk (Red)** category due to a number of security and coding standards issues. This means the plugin is not authorised for use on your service, until the issues are fixed.

About Our Plugin Review Risk Ratings

● **Low Risk (Green)**

The plugin is free from any noticeable issues. Performance impacts are unlikely and no security threats are present. The plugin is well maintained by the third party maintainer.

Plugin may be deployed to your service.

● **Medium Risk (Amber)**

The plugin review has presented concerns or issues with the plugin. It may show potential performance issues or be poorly maintained by the third party maintainer.

The plugin may be released to your service but Catalyst reserve the right to remove it without warning and without permission, should it place our SLA at risk.

● **High Risk (Red)**

The plugin review has identified issues in the plugin, most likely related to security or performance. You will receive clear reasoning in your plugin review document.

The plugin is not authorised for use on your service until issues are fixed.

Plugin Overview

From the README file:

"A Moodle Report that shows all user feedback on one page.

This report displays a searchable and sortable table with the User's grades and feedback across Moodle courses."

Item	Result
Version	2019062400
Release	2.15 (Build: 2019062400)
Requires	2017051500 (Moodle 3.3)
Usage	UCL
Author/copyright holder	Jessica Gramp <j.gramp@ucl.ac.uk> Delvon Forrester <delvon@esparanza.co.uk>
Online reviews	N/A
Compatibility	N/A

Review Results

Security

General

- Various files reference $_POST directly. These references should be replaced with optional_param() or required_param() function calls, or custom forms replaced with Moodle forms, where appropriate,
- Data from the database is inserted directly into HTML without any filtering/sanitisation.
- Some queries insert PHP variables into the SQL string, rather than using placeholders and prepared statements. Whilst this *can* be okay if the data is sanitised first, it is much safer to use placeholders, as it removes the human error aspect.
- Some files missing the MOODLE_INTERNAL check.
- Some files are missing capability checks and it is not clear if they should be open to everyone, or restricted.

Item	Result
Permissions	NOT OK – Some files are missing capability checks.
Authentication	NOT OK – Some files are missing login checks.
Form inputs	Form inputs are often referenced directly from $_POST. It appears that they are always used in the standard way as placeholders, so it should be secure, but if there are any areas overlooked where they are inserted directly into SQL, that could be an SQL injection risk.
Other inputs	N/A
External data in HTML	Some data from the database is inserted into HTML strings without sanitisation.
Cross site scripting	OK

Item	Result
SQL parametrised	OK – All queries appear to use the standard Moodle database API and placeholders.
Data exposure	UNKNOWN – Some files - such as export.php – can be accessed without any capability checks. It is unclear if this might expose data to users who should have see it.
Shell commands	N/A
CSRF	Custom HTML forms do not check for the user's session when it is processed. Most of these forms are POST forms, so it should not be a problem, but it is still good practice to make sure their session is valid on form submission, especially if there are any GET actions which will do something which could be exploited.
Data leakage	Unknown
Transmission to third parties	N/A

Coding Quality

In general, the code is quite old is generally done in a procedural way, rather than making use of classes (except for the one, very large class). It also has lots of coding standards violations, some of which are minor, but some of which are important and should be addressed ASAP.

Recommendations

If you want to update the plugin to more match the current Moodle standards, the following would be the recommendations to consider:

- Go through the codechecker results (attached to WR348550) and address all of the errors and warnings.
- Run the moodlecheck documentation checker and resolve any issues.
- Remove HTML content created in PHP where possible and replace with Mustache templates.
- Remove references to $_GET/$_POST and replace with optional_param() or required_param()
- Tidy up commented-out code
- Tidy up SQL queries.
- If you run some action (e.g. a database update) from the POST of a file, and you are not using Moodle forms, you should always make sure that the user's session is submitted along with it, to avoid cross site forgery.
- The lib.php file is very long and the class has a lot of very long methods. This could do with some refactoring, to make methods which are more concise and specific, and/or separate classes rather than one very long class.
- Remove javascript from the bottom of pages and make use of AMD Modules.
- When you are redirecting, you should use the Moodle redirect() function, not setting the header

manually.
- Your settings page seems to suggest that years are hard-coded and only supported up to 2015. If that setting is important, you may want to change it so its not hard-coded.
- You do not need to include jQuery manually, if you use AMD modules you can require it as part of them.
- Remove custom HTML forms where possible and replace with Moodle forms.

Item	**Result**
Outstanding bugs upstream	N/A
Installation	OK
Notices seen	**Logged in as a student (several tried):** - Went to report/myfeedback – Saw "Error reading from database". **Logged in as Staff Observer (12803):** - Clicked Module Tutor tab, selected CHEM0005, clicked Analyse – Saw "Error reading from database". - Clicked Personal Tutor tab – Saw "Error reading from database" - Clicked My Students tab, clicked on a student – Saw "Error reading from database". - Clicked Overview tab – Saw "Error reading from database". - Clicked Feedback tab – Saw "Error reading from database". **Logged in as admin:** - Clicked Overview tab – Saw "Error reading from database". - Clicked Feedback Comments tab – Saw "Error reading from database".
Basic functionality	NOT OK – It appears that lots of the functionality is broken and lots of the tabs have error messages.
Admin functionality	N/A
Backup	N/A
Restored	N/A
Removed	OK
Coding standards violations	A TOTAL OF 6954 ERRORS AND 1070 WARNINGS WERE FOUND IN 37 FILES
Abstraction	Abstraction is poor and plugin is mostly procedural, with one very large class with a lot of large methods.
Unit testing	N/A
Side effects	OK
Code documentation	Code could definitely use more commenting. There are some very long methods with little-to-no documentation, which makes it hard to know what it is supposed to be doing.

Performance

No performance issues were noticed during testing, however with the nature of the plugin – collecting feedback from various sources in one go, it is possible that some of the queries could be slow.

Item	Result
Really big synchronous jobs	N/A
Database killing queries	OK – There do not appear to be any queries so large which would kill the database. However, not all functionality could be tested.
Page response time	It is possible that some report pages may be slow, due to the database queries collecting data from lots of different sources.
Disk usage	OK

Review Environment

Item	Result
Plugin name	report_myfeedback
Plugin git hash	4e7432d699241cd7179c144e9d59c72da17c2b76
Plugin upstream repository	git.catalyst-eu.net:ucl/moodle-report_myfeedback
Plugin repository	git.catalyst-eu.net:ucl/moodle-report_myfeedback
Main git hash	0fb459175246aaca4cdae983bb007a9f34de4b20
Main git repo	git.catalyst-eu.net:ucl/moodle
Database version	mysqlnd 5.0.12-dev - 20150407
Database character encoding	utf-8
Database dump date	N/A
Site data dump date	N/A