Core - Analysis #7228

upload security issues

12/08/2014 13:09 - Anonymous

Status:	New	**Start date:**	12/08/2014
Priority:	Urgent	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Any visitor (anonymously) can upload files to chamilo-user folders via repository/php/ajax/upload_image.class.php. It suffices to send an HTTP POST request to chamilo's **ajax.php** with the following parameters:
context=repository
method=upload_image
user_id=<any user id>
Filedata=<arbitrary file>

This allows DoS attacks by flooding the servers filesystem, or attacks on specific users by flooding their folder and surpassing their quotas.

Secondly, **common/libraries/plugin/jquery-old/uploadify2/example/scripts/uploadify.php** contains example code that allows users to upload arbitrary files to arbitrary locations within a chamilo installation. The example script folder should be removed, or the **move_uploaded_file** line should be commented out.

History

#1 - 12/08/2014 13:45 - Anonymous

Similar bug. **common/extensions/external_repository_manager/implementation/soundcloud/plugin/soundcloud/demo/index.php** allows flooding the server with arbitrary audio files.

The demo script should be removed from the repository.

#2 - 20/08/2014 10:46 - Anonymous

- Project changed from Chamilo LCMS Connect to Core

#3 - 22/08/2014 13:18 - Anonymous

same issue in **common/extensions/external_repository_manager/implementation/soundcloud/plugin/soundcloud/demo/index.php**