web-soudan / **mw-wp-form** Public

forked from inc2734/mw-wp-form

Code | Issues 2 | Pull requests 2 | Actions | Projects | Security and quality

Commit `f872ab1`

mt8 authored 19 hours ago · ✓ 1 / 1 · Verified

```
Merge pull request #32 from web-soudan/security/fix-file-upload-path-validation
security: ファイルアップロード処理のパス検証を強化 (5.1.2)
```

`master` (#32) · 5.1.2

2 parents 3b2c157 + a6ae8e5 commit f872ab1

7 files changed +203 -20 lines changed

Top

Filter files…

- classes
  - controllers
    - class.main.php
  - models
    - class.data.php
    - class.directory.php
  - mw-wp-form.php
  - readme.txt
- tests/classes/models
  - test-data.php
  - test-directory.php

7 files changed +203 -20 lines changed

Search within code

`classes/controllers/class.main.php`

```
@@ -332,9 +332,16 @@ protected function _get_attachments() {
332 332                     continue;
333 333                 }
334 334
335     -               $form_id  = MWF_Functions::get_form_id_from_form_key( $this->Data->get_form_key() );
336     -               $filepath = MW_WP_Form_Directory::generate_user_filepath( $form_id, $key, $upload_filename );
337     -               if ( ! file_exists( $filepath ) ) {
    335 +               $form_id = MWF_Functions::get_form_id_from_form_key( $this->Data->get_form_key() );
    336 +
    337 +               try {
    338 +                   $filepath = MW_WP_Form_Directory::generate_user_filepath( $form_id, $key, $upload_filename );
    339 +               } catch ( \Exception $e ) {
    340 +                   error_log( $e->getMessage() );
    341 +                   continue;
    342 +               }
    343 +
    344 +               if ( ! $filepath || ! file_exists( $filepath ) ) {
338 345                     continue;
339 346                 }
340 347
```

classes/models/class.data.php

```
@@ -607,8 +607,17 @@ public function regenerate_upload_file_keys() {
607 607             foreach ( $upload_file_keys as $key => $upload_file_key ) {
608 608                 $upload_filename = $this->get_post_value_by_key( $upload_file_key );
609 609                 $form_id         = MWF_Functions::get_form_id_from_form_key( $this->get_form_key() );
610     -               $filepath        = MW_WP_Form_Directory::generate_user_filepath( $form_id, $upload_file_key, $upload_filename );
611     -               if ( ! $upload_filename || ! file_exists( $filepath ) ) {
    610 +
    611 +               try {
    612 +                   $filepath = MW_WP_Form_Directory::generate_user_filepath( $form_id, $upload_file_key, $upload_filename );
```

```
      613 +             } catch ( \Exception $e ) {
      614 +                 error_log( $e->getMessage() );
      615 +                 unset( $upload_file_keys[ $key ] );
      616 +                 $this->set( $upload_file_key, '' );
      617 +                 continue;
      618 +             }
      619 +
      620 +             if ( ! $upload_filename || ! $filepath || ! file_exists( $filepath ) ) {
612   621                   unset( $upload_file_keys[ $key ] );
613   622                   $this->set( $upload_file_key, '' );
614   623               }
```

classes/models/class.directory.php

```
@@ -39,6 +39,10 @@ public static function generate_user_dirpath( $form_id ) {
39    39                throw new \RuntimeException( '[MW WP Form] Failed to create user directory.' );
40    40            }
41    41
      42 +         if ( ! preg_match( '/^\d+$/', (string) $form_id ) ) {
      43 +             throw new \RuntimeException( '[MW WP Form] Invalid form ID.' );
      44 +         }
      45 +
42    46            $user_dir = path_join( static::get(), $saved_token );
43    47            $user_dir = path_join( $user_dir, (string) $form_id );
44    48
@@ -54,9 +58,17 @@ public static function generate_user_dirpath( $form_id ) {
54    58         * @throws \RuntimeException When directory name is not token value.
55    59         */
56    60        public static function generate_user_file_dirpath( $form_id, $name ) {
      61 +         if ( ! static::_is_valid_path_segment( $name ) ) {
      62 +             throw new \RuntimeException( '[MW WP Form] Invalid file reference requested.' );
      63 +         }
      64 +
57    65            $user_dir      = static::generate_user_dirpath( $form_id );
58    66            $user_file_dir = path_join( $user_dir, $name );
```

```
59  67
        68  +         if ( ! static::_is_within_expected_dir_candidate( $form_id, $user_file_dir ) ) {
        69  +             throw new \RuntimeException( '[MW WP Form] Invalid file reference requested.' );
        70  +         }
        71  +
60  72              return $user_file_dir;
61  73          }
62  74
            @@ -140,20 +152,20 @@ public static function generate_user_filepath( $form_id, $name, $filename ) {
140 152              return false;
141 153          }
142 154
        155 +         if ( ! static::_is_valid_path_segment( $filename ) ) {
        156 +             throw new \RuntimeException( '[MW WP Form] Invalid file reference requested.' );
        157 +         }
        158 +
143 159          $user_file_dir = static::generate_user_file_dirpath( $form_id, $name );
144 160          if ( ! $user_file_dir || ! is_dir( $user_file_dir ) ) {
145 161              return false;
146 162          }
147 163
148     -         $normalized_filename = wp_normalize_path( $filename );
149     -         if (
150     -             wp_basename( $normalized_filename ) !== $normalized_filename ||
151     -             strstr( $normalized_filename, "\0" )
152     -         ) {
        164 +         $filepath = path_join( $user_file_dir, $filename );
        165 +         if ( ! static::_is_within_expected_dir_candidate( $form_id, $filepath ) ) {
153 166              throw new \RuntimeException( '[MW WP Form] Invalid file reference requested.' );
154 167          }
155 168
156     -         $filepath      = path_join( $user_file_dir, $filename );
157 169          $filepath      = wp_normalize_path( $filepath );
```

```
158  170            $user_file_dir = trailingslashit( wp_normalize_path( $user_file_dir )
     );
159  171
     @@ -176,6 +188,92 @@ public static function generate_user_filepath(
     $form_id, $name, $filename ) {
176  188            return $filepath;
177  189        }
178  190
     191    +    /**
     192    +     * Return true when path segment is valid.
     193    +     *
     194    +     * @param string $value Path segment.
     195    +     * @return boolean
     196    +     */
     197    +    protected static function _is_valid_path_segment( $value ) {
     198    +        if ( ! is_string( $value ) || '' === $value ) {
     199    +            return false;
     200    +        }
     201    +
     202    +        $value = wp_normalize_path( $value );
     203    +
     204    +        if ( strstr( $value, "\0" ) ) {
     205    +            return false;
     206    +        }
     207    +
     208    +        if ( '.' === $value || '..' === $value ) {
     209    +            return false;
     210    +        }
     211    +
     212    +        if ( path_is_absolute( $value ) ) {
     213    +            return false;
     214    +        }
     215    +
     216    +        if ( wp_basename( $value ) !== $value ) {
     217    +            return false;
     218    +        }
     219    +
     220    +        return true;
     221    +    }
     222    +
```

```
223 +     /**
224 +      * Return true when candidate path is inside the current user's temp
      directory.
225 +      *
226 +      * @param int    $form_id Form ID.
227 +      * @param string $path    Target path.
228 +      * @return boolean
229 +      */
230 +     protected static function _is_within_expected_dir_candidate( $form_id,
      $path ) {
231 +         $path = wp_normalize_path( $path );
232 +
233 +         $user_dir = static::_get_expected_user_dir( $form_id, static::get() );
234 +         if ( false === $user_dir ) {
235 +             return false;
236 +         }
237 +
238 +         $path           = untrailingslashit( $path );
239 +         $user_dir       = untrailingslashit( $user_dir );
240 +         $user_dir_slash = trailingslashit( $user_dir );
241 +
242 +         return $path === $user_dir || 0 === strpos( $path, $user_dir_slash );
243 +     }
244 +
245 +     /**
246 +      * Return the expected user directory path.
247 +      *
248 +      * @param int         $form_id  Form ID.
249 +      * @param string|bool $base_dir Base directory path.
250 +      * @return string|false
251 +      */
252 +     protected static function _get_expected_user_dir( $form_id, $base_dir ) {
253 +         $saved_token = MW_WP_Form_Csrf::saved_token();
254 +         $saved_token = $saved_token ? $saved_token : MW_WP_Form_Csrf::token();
255 +         if ( ! preg_match( '|^[a-z0-9]+$|', $saved_token ) ) {
256 +             return false;
257 +         }
258 +
259 +         if ( ! preg_match( '/^\d+$/', (string) $form_id ) ) {
260 +             return false;
```

```
261 +         }
262 +
263 +         if ( ! $base_dir ) {
264 +             return false;
265 +         }
266 +
267 +         $base_dir = wp_normalize_path( $base_dir );
268 +
269 +         return wp_normalize_path(
270 +             path_join(
271 +                 path_join( $base_dir, $saved_token ),
272 +                 (string) $form_id
273 +             )
274 +         );
275 +     }
276 +
179 277         /**
180 278          * Returns a list of saved file paths.
181 279          *
```

mw-wp-form.php

```
@@ -3,7 +3,7 @@
3 3       * Plugin Name: MW WP Form
4 4       * Plugin URI: https://mw-wp-form.web-soudan.co.jp
5 5       * Description: MW WP Form is shortcode base contact form plugin. This plugin
          have many features. For example you can use many validation rules, inquiry data
          saving, and chart aggregation using saved inquiry data.
6   -     * Version: 5.1.1
  6 +     * Version: 5.1.2
7 7       * Requires at least: 6.0
8 8       * Requires PHP: 8.0
9 9       * Author: websoudan
```

readme.txt

```
@@ -5,7 +5,7 @@ Tags: plugin, form, confirm, preview, shortcode, mail, chart,
graph, html, conta
5 5 Requires at least: 6.0
```

```
6   6     Requires PHP: 8.0
7   7     Tested up to: 6.4
8       - Stable tag: 5.1.1
    8   + Stable tag: 5.1.2
9   9     License: GPLv2 or later
10  10    License URI: http://www.gnu.org/licenses/gpl-2.0.html
11  11
      ↓   @@ -79,13 +79,16 @@ Do you have questions or issues with MW WP Form? Use
      ↑   these support channels appr
79  79    4. List page of inquiry data that has been saved.
80  80    5. Supports chart display of saved inquiry data.
81  81
82      - == Changelog ==
83      -
84      - = 5.1.1 =
85      - * Security Fix insufficient file path validation in upload file handling
86      -
87      - = 5.1.0 =
88      - * Security Use wp_kses_post to form content/complete message
    82  + == Changelog ==
    83  +
    84  + = 5.1.2 =
    85  + * Security Fix insufficient file path validation in upload file handling
    86  +
    87  + = 5.1.1 =
    88  + * Security Fix insufficient file path validation in upload file handling
    89  +
    90  + = 5.1.0 =
    91  + * Security Use wp_kses_post to form content/complete message
89  92
90  93    = 5.0.6 =
91  94    * Fixed Fixed an error during uninstallation. ( later 5.0.0 )
      ↓
```

tests/classes/models/test-data.php

```
      ↑   @@ -679,6 +679,24 @@ public function regenerate_upload_file_keys() {
679 679             unlink( $dirpath . '/1.txt' );
680 680         }
681 681
    682 +     /**
```

```
683 +      * @test
684 +      * @group regenerate_upload_file_keys
685 +      */
686 +     public function regenerate_upload_file_keys_should_drop_invalid_keys() {
687 +         $Data = $this->_instantiation_Data( array(
688 +             MWF_Config::UPLOAD_FILE_KEYS => array( '/var/www/wordpress',
    '../../../wordpress' ),
689 +         ) );
690 +
691 +         $Data->set( '/var/www/wordpress', 'wp-config.php' );
692 +         $Data->set( '../../../wordpress', 'wp-config.php' );
693 +         $Data->regenerate_upload_file_keys();
694 +
695 +         $this->assertEquals( array(), $Data->get_post_value_by_key(
    MWF_Config::UPLOAD_FILE_KEYS ) );
696 +         $this->assertSame( '', $Data->get_post_value_by_key(
    '/var/www/wordpress' ) );
697 +         $this->assertSame( '', $Data->get_post_value_by_key(
    '../../../wordpress' ) );
698 +     }
699 +
682 700         /**
683 701          * @test
684 702          * @group push_uploaded_file_keys
```

tests/classes/models/test-directory.php

```
    @@ -76,4 +76,52 @@ public function
    generate_user_filepath_should_reject_windows_absolute_path() {
76  76             $this->expectException( '\RuntimeException' );
77  77             MW_WP_Form_Directory::generate_user_filepath( $form_id, $name,
    'C:\\tmp\\evil.php' );
78  78         }
79  +
80  +     /**
81  +      * @test
82  +      * @group generate_user_file_dirpath
83  +      */
84  +     public function
    generate_user_file_dirpath_should_reject_absolute_path_name() {
```

```
85  +         MW_WP_Form_Csrf::save_token();
86  +         $form_id = $this->_create_form();
87  +
88  +         $this->expectException( '\RuntimeException' );
89  +         MW_WP_Form_Directory::generate_user_file_dirpath( $form_id,
      '/var/www/wordpress' );
90  +     }
91  +
92  +     /**
93  +      * @test
94  +      * @group generate_user_file_dirpath
95  +      */
96  +     public function generate_user_file_dirpath_should_reject_nested_path_name()
      {
97  +         MW_WP_Form_Csrf::save_token();
98  +         $form_id = $this->_create_form();
99  +
100 +         $this->expectException( '\RuntimeException' );
101 +         MW_WP_Form_Directory::generate_user_file_dirpath( $form_id,
      'nested/file-1' );
102 +     }
103 +
104 +     /**
105 +      * @test
106 +      * @group generate_user_file_dirpath
107 +      */
108 +     public function
      generate_user_file_dirpath_should_reject_path_outside_user_dir() {
109 +         MW_WP_Form_Csrf::save_token();
110 +         $form_id = $this->_create_form();
111 +
112 +         $this->expectException( '\RuntimeException' );
113 +         MW_WP_Form_Directory::generate_user_file_dirpath( $form_id,
      '../../../wordpress' );
114 +     }
115 +
116 +     /**
117 +      * @test
118 +      * @group generate_user_file_dirpath
119 +      */
```

```
+     public function generate_user_file_dirpath_should_reject_windows_absolute_path_name() {
+         MW_WP_Form_Csrf::save_token();
+         $form_id = $this->_create_form();
+
+         $this->expectException( '\RuntimeException' );
+         MW_WP_Form_Directory::generate_user_file_dirpath( $form_id, 'C:\\xampp\\htdocs\\wordpress' );
+     }
  }
```

Comments 0

Please sign in to comment.