AyeCode / **userswp** Public

Code | Issues 44 | Pull requests 1 | Actions | Projects | Security and quali

Commit `ca0c81b`

kprajapatii committed 2 weeks ago

```
Improve image validation during the cropping process - FIXED/SECURITY
```

`master` (#890) · 1.2.61 ••• 1.2.59

1 parent 7553587 commit ca0c81b

5 files changed +54 -43 lines changed

Top

Filter files…

- includes
  - class-forms.php
  - class-userswp.php
- templates
  - bootstrap
    - modal-profile-image-crop.php
    - profile-header.php
  - modal-profile-image-crop.php

5 files changed +54 -43 lines changed

Search within code

includes/class-forms.php

```
@@ -103,25 +103,24 @@ public function handler() {
103 103            }
104 104
105 105            if ( $processed ) {
106         -
```

```
107  106              if ( is_wp_error( $errors ) ) {
108      -                echo aui()->alert(
109      -                    array( // phpcs:ignore WordPress.Security.EscapeOutput.OutputNotEscaped
110      -                        'type'    => 'error',
111      -                        'class'   => 'text-center',
112      -                        'content' => wp_kses_post( $errors->get_error_message() ),
113      -                    )
114      -                );
115      -            } elseif ( $redirect ) {
     107  +                aui()->alert(
     108  +                    array(
     109  +                        'type'    => 'error',
     110  +                        'content' => wp_kses_post( $errors->get_error_message() )
     111  +                    ),
     112  +                    true
     113  +                );
     114  +            } else if ( $redirect ) {
116  115                      wp_safe_redirect( $redirect );
117  116                      exit();
118      -            } else {
119      -                echo aui()->alert(
120      -                    array( // phpcs:ignore WordPress.Security.EscapeOutput.OutputNotEscaped
121      -                        'type'    => 'success',
122      -                        'class'   => 'text-center',
123      -                        'content' => wp_kses_post( $message ),
124      -                    )
     117  +            } else {
     118  +                aui()->alert(
     119  +                    array(
     120  +                        'type'    => 'success',
     121  +                        'content' => wp_kses_post( $message )
     122  +                    ),
     123  +                    true
125  124                  );
126  125              }
127  126          }
```

```
@@ -197,6 +196,7 @@ public function process_upload_submit( $data = array(), $files = array(), $type
197 196         */
198 197        public function process_image_crop( $data = array(), $type = 'avatar', $unlink_prev_img = false ) {
199 198            global $wpdb;
    199 +
200 200            if ( ! is_user_logged_in() ) {
201 201                return false;
202 202            }
@@ -205,6 +205,27 @@ public function process_image_crop( $data = array(), $type = 'avatar', $unlink_p
205 205                return;
206 206            }
207 207
    208 +            $image_url = ! empty( $data['uwp_crop'] ) ? esc_url( $data['uwp_crop'] ) : '';
    209 +
    210 +            if ( empty( $image_url ) ) {
    211 +                return new WP_Error( 'empty_image', __( 'Upload valid image.', 'userswp' ) );
    212 +            }
    213 +
    214 +            // Ensure we have a valid URL with an allowed meme type.
    215 +            $image_url = $this->normalize_url( $image_url );
    216 +
    217 +            $content_url = str_replace( array( 'https://', 'http://' ) , '', untrailingslashit( WP_CONTENT_URL ) );
    218 +            $_image_url = str_replace( array( 'https://', 'http://' ), '', $image_url );
    219 +            if ( strpos( $_image_url, $content_url ) !== 0 ) {
    220 +                return new WP_Error( 'invalid_image', __( 'Invalid image url.', 'userswp' ) );
    221 +            }
    222 +
    223 +            $filetype = wp_check_filetype( $image_url );
    224 +
    225 +            if ( empty( $filetype['ext'] ) ) {
    226 +                return new WP_Error( 'invalid_image', __( 'Invalid image type.', 'userswp' ) );
```

```
                227 +           }
                228 +
208             229             // If is current user's profile (profile.php)
209             230             if ( is_admin() && defined( 'IS_PROFILE_PAGE' ) && IS_PROFILE_PAGE ) {
210             231                 $user_id = get_current_user_id();
                    @@ -216,19 +237,6 @@ public function process_image_crop( $data = array(), $type = 'avatar', $unlink_p
216             237                 $user_id = get_current_user_id();
217             238             }
218             239
219             -           // Ensure we have a valid URL with an allowed meme type.
220             -           $image_url = $this->normalize_url( esc_url( $data['uwp_crop'] ) );
221             -           $filetype  = wp_check_filetype( $image_url );
222             -
223             -           $errors = new WP_Error();
224             -           if ( empty( $image_url ) || empty( $filetype['ext'] ) ) {
225             -               $errors->add( 'something_wrong', __( 'Something went wrong. Please contact site admin.', 'userswp' ) );
226             -           }
227             -
228             -           if ( $errors->has_errors() ) {
229             -               return $errors;
230             -           }
231             -
232             240             // Retrieve current thumbnail.
233             241             $current_field     = 'avatar' === $type ? 'avatar_thumb' : 'banner_thumb';
234             242             $current_thumbnail = $this->normalize_url( uwp_get_usermeta( $user_id, $current_field, '' ) );
                    @@ -253,11 +261,12 @@ public function process_image_crop( $data = array(), $type = 'avatar', $unlink_p
253             261             $name                 = sanitize_file_name( pathinfo( $image_path, PATHINFO_FILENAME ) ); //file name without extension
254             262             $thumb_image_name     = $name . $thumb_postfix . '.' . $ext;
255             263             $thumb_image_location = str_replace( $name . '.' . $ext, $thumb_image_name, $image_path );
                264 +
256             265             //Get the new coordinates to crop the image.
257             -           $x = $data['x'];
258             -           $y = $data['y'];
```

```
259      -              $w = $data['w'];
260      -              $h = $data['h'];
         266 +          $x = $data['uwpx'];
         267 +          $y = $data['uwpy'];
         268 +          $w = $data['uwpw'];
         269 +          $h = $data['uwph'];
261      270            //Scale the image based on cropped width setting
262      271            $scale = $full_width / $w;
263      272            //$scale = 1; // no scaling
```

includes/class-userswp.php

```
         @@ -571,7 +571,7 @@ public function load_forms_actions_and_filters(
         $instance ) {
571      571
572      572            // general
573      573            add_action( 'init', array( $instance, 'init_notices' ), 1 );
574      -              add_action( 'uwp_loaded', array( $instance, 'handler' ) );
         574 +          add_action( 'init', array( $instance, 'handler' ), 11 );
575      575            add_action( 'init', array( $instance, 'privacy_submit_handler' ) );
576      576            add_action( 'uwp_template_display_notices', array( $instance,
         'display_notices' ), 10, 1 );
577      577            add_action( 'wp_ajax_uwp_upload_file_remove', array( $instance,
         'upload_file_remove' ) );
```

...ates/bootstrap/modal-profile-image-crop.php

```
         @@ -36,28 +36,28 @@
36       36                     echo aui()->input(array( // phpcs:ignore
         WordPress.Security.EscapeOutput.OutputNotEscaped
37       37                         'type'  =>  'hidden',
38       38                         'id'    =>  esc_html( $type.'-x' ),
39       -                          'name'  =>  'x',
         39 +                       'name'  =>  'uwpx',
40       40                         'value' =>  '',
41       41                         'no_wrap' => true,
42       42                     ));
43       43                     echo aui()->input(array( // phpcs:ignore
         WordPress.Security.EscapeOutput.OutputNotEscaped
```

```
44  44                      'type'  =>  'hidden',
45  45                      'id'    =>  esc_html( $type.'-y' ),
46      -                   'name'  =>  'y',
    46  +                   'name'  =>  'uwpy',
47  47                      'value' =>  '',
48  48                      'no_wrap' => true,
49  49                  ));
50  50                  echo aui()->input(array( // phpcs:ignore
        WordPress.Security.EscapeOutput.OutputNotEscaped
51  51                      'type'  =>  'hidden',
52  52                      'id'    =>  esc_html( $type.'-w' ),
53      -                   'name'  =>  'w',
    53  +                   'name'  =>  'uwpw',
54  54                      'value' =>  '',
55  55                      'no_wrap' => true,
56  56                  ));
57  57                  echo aui()->input(array( // phpcs:ignore
        WordPress.Security.EscapeOutput.OutputNotEscaped
58  58                      'type'  =>  'hidden',
59  59                      'id'    =>  esc_html( $type.'-h' ),
60      -                   'name'  =>  'h',
    60  +                   'name'  =>  'uwph',
61  61                      'value' =>  '',
62  62                      'no_wrap' => true,
63  63                  ));
```

templates/bootstrap/profile-header.php

```
    @@ -23,7 +23,9 @@
23  23          return;
24  24      }
25  25
26      - if ( ! $uwp_in_user_loop ){ ?>
    26  + if ( ! $uwp_in_user_loop ) {
    27  + do_action( 'uwp_template_display_notices', 'profile' );
    28  + ?>
27  29      <div class="card shadow-0 border-0 mw-100"><?php }
28  30
29  31          if ( ! $hide_cover ) {
```

templates/modal-profile-image-crop.php

```
@@ -34,10 +34,10 @@
34  34                  <div class="uwp-<?php echo esc_attr( $type ); ?>-crop-p-wrap">
35  35                      <div id="<?php echo esc_attr( $type ); ?>-crop-actions">
36  36                          <form class="uwp-crop-form" method="post">
37      -                           <input type="hidden" name="x" value="" id="<?php echo esc_attr( $type ); ?>-x" />
38      -                           <input type="hidden" name="y" value="" id="<?php echo esc_attr( $type ); ?>-y" />
39      -                           <input type="hidden" name="w" value="" id="<?php echo esc_attr( $type ); ?>-w" />
40      -                           <input type="hidden" name="h" value="" id="<?php echo esc_attr( $type ); ?>-h" />
    37  +                           <input type="hidden" name="uwpx" value="" id="<?php echo esc_attr( $type ); ?>-x" />
    38  +                           <input type="hidden" name="uwpy" value="" id="<?php echo esc_attr( $type ); ?>-y" />
    39  +                           <input type="hidden" name="uwpw" value="" id="<?php echo esc_attr( $type ); ?>-w" />
    40  +                           <input type="hidden" name="uwph" value="" id="<?php echo esc_attr( $type ); ?>-h" />
41  41                              <input type="hidden" id="uwp-<?php echo esc_attr( $type ); ?>-crop-image" name="uwp_crop" value="<?php echo esc_attr( $image_url ); ?>" />
42  42                              <input type="hidden" name="uwp_crop_nonce" value="<?php echo esc_attr( wp_create_nonce( 'uwp_crop_nonce_'.$type ) ); ?>" />
43  43                              <input type="submit" name="uwp_<?php echo esc_attr( $type ); ?>_crop" value="<?php esc_attr_e('Apply', 'userswp'); ?>" class="button button-primary" id="save_uwp_<?php echo esc_attr( $type ); ?>" />
```

Comments 0

Please sign in to comment.