



“ ” URL

WordPress “ ”

WordPress “current_user_can()” CSRF



URL URL 123

```
http://example.com/wp-admin/post.php?post=123&action=trash
```

URL WordPress cookie URL

```

```

WordPress cookie WordPress

WordPress URL

```
http://example.com/wp-admin/post.php?post=123&action=trash&_wpnonce=b192fc4204
```

WordPress 123 WordPress “403 Forbidden”



URL

AJAX JavaScript



URL

`wp_nonce_url()` URL

```
$complete_url = wp_nonce_url( $bare_url, 'trash-post_'. $post->ID );
```

`wp_nonce_url()` `_wpnonce`

```
$complete_url = wp_nonce_url( $bare_url, 'trash-post_'. $post->ID, 'my_nonce' );
```

`wp_nonce_field()` `wp_nonce_field()` URL

```
wp_nonce_field( 'delete-comment_'. $comment_id );
```

```
<input type="hidden" id="_wpnonce" name="_wpnonce" value="796c7766b1" />
<input type="hidden" name="_wp_http_referer" value="/wp-admin/edit-comments.php" />
```

`no` `wp_nonce_field()`

`wp_create_nonce()`

```
$nonce = wp_create_nonce( 'my-action_'. $post->ID );
```

295a686963

URL AJAX

XXXXXXXXXX

XXXX check_admin_referer() XXXXXXXXXX

XXX

```
check_admin_referer( 'delete-comment_'.$comment_id );
```

XXXXXXXXXXXXXXXXXXXXXXXXXXXX"403 Forbidden"XXXXXXXXXXXX

XX _wpnonce)XXXXXXXXXX(

XXX

```
check_admin_referer( 'delete-comment_'.$comment_id, 'my_nonce' );
```

XX AJAX XXXXXXXXXX

XX [check_ajax_referer\(\)](#) XXXXXXXXXX

```
check_ajax_referer( 'process-comment' );
```

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

_wpnonce _ajax_nonce check_ajax_referer() XXXXX

XXXXXXXXXXXX

wp_verify_nonce() XXXXXXXXXXXXXXX

XXX

```
wp_verify_nonce( $_REQUEST['my_nonce'], 'process-comment_'.$comment_id );
```

XXXX wp_nonce_ays() XXXXXXXXXXXX"403 Forbidden"XXX

XXnonceXX

XXXXXXXXXXXXXXXXXXXX

XXXXXXXXXX

nonce_life

```
add_filter( 'nonce_life', function () { return 4 * HOUR_IN_SECONDS; } );
```

check_admin_referrer() check_admin_referer

```
function wporg_additional_check ( $action, $result ) {  
    ...  
}  
add_action( 'check_admin_referer', 'wporg_additional_check', 10, 2 );
```

check_ajax_referer() check_ajax_referer

```
function my_nonce_message ($translation) {  
    if ($translation === 'Are you sure you want to do this?') {  
        return 'No! No! No!';  
    }  
  
    return $translation;  
}  
  
add_filter('gettext', 'my_nonce_message');
```

WordPress

WordPress “”WordPress

1 2

WcNONCE_KEYNONCE_SALTwp-config.php

current_user_can()

check_admin_referrer()check_ajax_referrer()

wp_create_nonce()wp_verify_nonce()wp_nonce_tick()

wp_nonce_ays(), wp_nonce_field(), wp_nonce_url(), wp_verify_nonce(), wp_create_nonce(),
check_admin_referer(), check_ajax_referer(), wp_referer_field()

nonce_life, nonce_user_logged_out, explain_nonce_verb-noun, check_admin_referer

#1
Vcanson 18 2023 11:22:16
Vcanson 26 2023 15:34:10