WordPress: JavaScript e il rischio di attacchi XSS

Moltissimi temi e plugin WordPress utilizzano dati presi dal database o dall'input utente (nel caso peggiore) per generare codice JavaScript in modo dinamico inserendolo direttamente nella marcatura della pagina. Questa pratica se implementata senza precauzioni espone il sito ad eventuali attacchi XSS.

Come viene giustamente ricordato nel volume Web Application Security Guide:

> If it is possible to place anything in a place of the document structure where it is not supposed to go (e.g. outside a JavaScript string literal), it is a security issue that must be fixed. It might not be exploitable - or you may simply not be seeing the way to exploit it. Don't take that risk!

Inoltre bisogna assolutamente fare in modo che caratteri come < che hanno un significato speciale in HTML vengano correttamente filtrati usando sia le funzioni di WordPress (come `esc_html()`) sia quelle di PHP.

Esempio:

```
<script>
var CURRENT_VALUE = <?php echo json_encode($text,
JSON_HEX_QUOT | JSON_HEX_TAG | JSON_HEX_AMP |
JSON_HEX_APOS); ?>;
$( "#valueBox" ).text( CURRENT_VALUE );
</script>
```

Bisogna prestare attenzione a ciò che dal server viene passato come input a JavaScript: tendenzialmente ogni tipo di input è potenzialmente pericoloso. L'input diretto dell'utente è in assoluto quello con il maggior rischio, quindi quando dobbiamo gestire form, sia nel backend che nel frontend di un sito in WordPress, tutto il flusso di input deve essere filtrato e validato.