

## Récapitulatif des quelques bonnes pratiques que nous avons observées

Vulnerability	Solution
HTML Content Injection	• Utilisation de <code>v-text</code> ou <code>{{ }}</code> fourni par le moteur Vue JS pour nettoyer les entrées de l'utilisateur.
URL Injection	Eviter l'utilisation de <code>v-bind:href="url"</code> ou <code>:href="url "</code> . Préconiser les fonctions natives telles que <code>: router-link</code> etc..
Poor road protection	Sans authentification aucune route n'est accessible.
Non-trusted Templates	<pre>`&lt;div&gt;` + userProvidedString + `&lt;/div&gt;`.</pre> de tels usages pour ne pas qu'un utilisateur injecte du code.