hpj233 Create v7 History

1 contributor

12 lines (11 sloc) | 477 Bytes

```
#The problem occurred in line 1312 of the file ewebeditor\3.1.1\kindeditor.js,directly output the value obtained after switching the mode:
```javascript
if (KE.g[id].filterMode) {
                obj.newTextarea.value = KE.util.outputHtml(id, obj.iframeDoc.body);
```
#You can see that there is no escape processing.

#url:
http://localhost/member/post.php?job=postnew
#Build a website to publish articles,change the editor mode to HTML.
#payload:
<img src=1 onerror=alert(1)>
```