Introduction

Starting with vtenext version 26.01, all variables outputted by Smarty templates (for example `{$VARIABLE}`) by default have all applicable characters are converted to html `&...;` notation. For instance, the string `"nice & 'smooth' à > è"` is converted to `"nice &amp; &039;smooth&039; &agrave; &gt; &egrave;"`

The conversion is done with the `htmlentities` function, without double encoding existing entities.

The reason of this change is to reduce as much as possible exposure to XSS attacks, since it was extremely difficult to track every possible variable in templates and ensure it was properly escaped.

There are of course some exceptions on the escaping and some edge cases that should be understood. The next chapter presents the rules to follow to write simple and secure code.

Revision #1
Created 2026-01-23 15:26:58 UTC by m.maporti
Updated 2026-01-23 15:28:30 UTC by m.maporti