CVE-2020-29254

About:

- https://github.com/S1lkys/CVE-2020-29254
- https://nvd.nist.gov/vuln/detail/CVE-2020-29254

That is a feature for admins only (people that already have full permissions via tiki_p_admin). It is designed for admins to do things. It can't do its job and prevent XSS.

But then, this could be exploited via privilege escalation. Thus, for this and other similarly powerful features, we did this in Tiki22: Risky Preferences.

We didn't backport for Tiki 21.x because it would risk breaking for some users that are depending on this feature.

HOW TO DO IN TIKI 21.X AND OLDER?

Just use System Configuration to deactivate preferences identified as risky here: Risky Preferences