Risky preferences

Some of Tiki's preferences are quite powerful (and thus dangerous) and should be used only by experts. These risky preferences are disabled and hidden by default, since Tiki 22 and only the system administrator can make them visible through Tiki's system configuration file.

Introduced in Tiki22

This addresses CVE-2020-29254

These are the preferences marked as risky:

- feature_editcss
- feature_edit_templates
- feature_purifier
- smarty_security_functions
- smarty_security_modifiers
- smarty_security_dirs
- tiki_allow_trust_input

Enable/Show risky preferences

First, in order to enable these features first is needed to activate the system configuration.
If you don’t have one, you will need to declare the path of the tiki.ini file where rules can be stored.

Sample configuration file placed in db/local.php, with a relative path

```
$system_configuration_file = 'db/tiki.ini';
```

In your configuration file, add new rules to Tiki's configuration file that allows showing these features.
See the following example:

System configuration file sample(db/tiki.ini) that enable to show "smarty_security_functions" preference

```
rules.0 = show smarty_security_functions
```

Set Specific Risky Prefs in tiki.ini

Alternatively you can set these "disabled by default" prefs to specific values in your tiki.ini file, like this:

preference.smarty_security_dirs[] = "/home/tiki/mycustomtheme_repo/themes/themename/templates/"
preference.smarty_security_dirs[] = "/home/tiki/myothertheme_repo/themes/othertheme/templates/""
Read more about System configuration here.