# Archive:Web security

The package **[web security]** contains extensions to make the wiki more secure, which is important especially for public wikis. Protect your wiki against spam, bots and any kinds of abuse.

In the table shown below you find all included extensions of **[web security]** and a link to the single extensions with more information and descriptions how to use it or how it works.

| Function | Description | |
| --- | --- | --- |
| AbuseFilter | Allows privileged users to set specific controls on actions by users, such as edits, and create automated reactions for certain behaviors. | [●] |
| CheckUser | Check which IPs are used by a given username and which usernames are used by a given IP, without having to run queries directly against the database by hand. | [●] |
| ConfirmEdit | lets you use various different CAPTCHA techniques, to try to prevent spambots and other automated tools from editing your wiki, as well as to foil automated login attempts that try to guess passwords. | [●] |
| AntiBot | Simple framework for protection against spambots. | [●] |
| AntiSpoof | Preventing confusable usernames from being created. It blocks the creation of accounts with mixed-script, confusing and similar usernames. | [●] |
| SpamBlacklist | Prevents edits that contain URLs whose domains match regular expression patterns defined in specified files or wiki pages. When someone tries to save a page, SpamBlacklist checks the text against a (potentially very large) list of illegal host names. If there is a match, the extension displays an error message to the user and refuses to save the page. | [●] |
| TorBlock | Automatically applies restrictions to Tor exit nodes with access to the wiki's front-door server. | [●] |
| Robot Configuration | Script for controlling of search robots. | ◎ |