



Protects Against Web Spam

It is typical for "SEO Marketing Companies" to take advantage of forums and blogs by creating worthless posts and comments with links to a website they are promoting.

If your web-property allows user-generated content, you are likely to use CAPTCHA. CAPTCHAs are not perfect:

- They annoy your visitors.
- They provide an illusory sense of security.

Today it is possible to [buy access to an API](#) which solves any CAPTCHA for just \$0.70 per 1000 CAPTCHA images. And do you think your customer will be happy to try to solve one of these [ridiculous CAPTCHAs](#)?



Secures Against Brute Force Attacks

Many modern web-applications are susceptible to brute force attacks.

Take a typical login form, for example. Hackers can compromise account security by trying every possible password combination. They can also leverage a large network of proxy servers to parallelize this attack.

Forcing their browser to work hard makes it too expensive and slow for hackers to perform a brute force attack.

Applications in GIS

- Throttle server requests (DDoS attacks)
- Comment forms for user input
- Brute force password requests
- Reducing SPAM email!!