Captcha mechanisms exist to verify humans are making the calls and not robots or automation tools. Though far from foolproof, this security mechanism is very important and while it started out simply as a way to improve OCR software by showing you 1 known and 1 unknown word, it has evolved drastically over the course of a few years. Bypassing captcha can have disastrous consequences such as brute-forcing the application or even DoS'ing it on an application level.

Known bypasses are:

- Simply not sending the captcha along with the request or leaving it empty. The developers might have forgotten to implement the verification.
- Changing the request from GET to POST and vica versa while leaving the captcha out of the request
- Trying to re-use captcha tokens as this might enable an attacker to simply request a captcha code and enter it along with every request (The captcha is not requested bound)
- Trying to predict the next captcha code
- Using an OCR to solve them. This is why captcha is not as good as they used to be, OCR's can solve the text-based captchas