

Forum:[Hack Forums](#)

Thread: [Sending POST request with reCaptcha](#)

raisenn - February 4, 2021, 10:41 pm

Hello,

Right now I'm trying to figure out if it's possible to bypass reCaptcha, exactly the noCaptcha version which is submitted while sending form method POST.

While trying to POST it myself I cant get access to site because obviously I don't have captcha token. I found all ingredients, sitekey , some values which are dynamic and used with request to google APIs. I found JavaScript file with functions and even piece of code that triggers the login and if I fill out login and password I can paste it to consol and I will be logged in. But I keep wonder if it's possible to do that by just sending some request. Using right now JavaScript with axios.

Please help

remymartin - February 13, 2021, 8:54 pm

Dont know but ive bypassed Captchas with openbullet

linkinpork - February 13, 2021, 9:59 pm

(Feb 4, 2021 11:41 PM)raisenn Wrote: [\[CITE\]](#) While trying to POST it myself I cant get access to site because obviously I don't have captcha token. I found all ingredients, sitekey , some values which are dynamic and used with request to google APIs.

Hi,

Not sure if this is what you're looking for. This worked in some site-specific conditions two years ago. I reported this to Google but they said it isn't consistent with all reCaptcha installations. They left it to the end-users to manage. I'd hesitate to call it a zero day, but by definition it is.

Instead of removing g-captcha-response, give it a dummy string, like so

Code var=foo&g-captcha-response=1

or

var=foo&g-captcha-response=randomstringNote the presence of session cookies. I've met cases where CSRF tokens have to be managed. Don't change them nor remove them, even if it's a login attack.

This exploit has only worked twice in my entire career, both of which are Login-based Unauthenticated CSRF. There's a big chance it might not work for you.

Good luck and have fun!