

Introducing mCaptcha

No-nonsense, privacy-focused CAPTCHA system with seamless UX

[Aravinth Manivannan](#) | [@realaravinth](#)

mcaptcha.org



mCaptcha

Overview

- 1) How does it work?
 - 1.1) Proof of work based rate limiting
 - 1.2) Variable difficulty Proof of work
 - 1.2) Performance and Protection Scope
- 2) Accessibility
- 3) Privacy
- 4) Reasons for not choosing mCaptcha

How does it work?

PoW based rate limiting

- Make the user do more work to send the request than the work the server needs to do to serve the request

Generating proof^[1]: 50,000 x hash()

Verifying proof: 1 x hash()

- Fully transparent process:
 - i. mCaptcha sends PoW^[2] challenge to user
 - ii. user generates PoW with challenge and sends PoW to mCaptcha
 - iii. mCaptcha verifies proof; if valid: send access token else: deny access
 - iv. Access token is sent to client server(ex: codeberg.org)
 - v. client server verifies authenticity of access token with mCaptcha

[1]: 50,000 hashes is an approximation, reality might be significantly higher.

[2]: Pow is short for [Proof of Work](#)

Variable difficulty Proof of work

(or how mCaptcha ups the ante when under attack)

- Difficulty factor increases when under attack, i.e, when number of requests increases in given time

Add Sitekey [Advance Options](#)

Description

Average Traffic of your website

Maximum traffic that your website can handle

Traffic that broke your website(Optional)

Add Sitekey [Easy Options](#)

Description

Cooldown Duratoin(in seconds)

Level 1

Visitor Difficulty

Level 2

Visitor Difficulty

Level 3

Visitor Difficulty

Difficulty factor is configured based on a website statistics in easy and advance modes.

Performance and Protection Scope

- Effective against DDoS attacks
- Doesn't detect spam: advertisements on comments/issues isn't covered

Join

Username

Password

Confirm Password

I'm not a robot



mCaptcha
Privacy Terms

Register

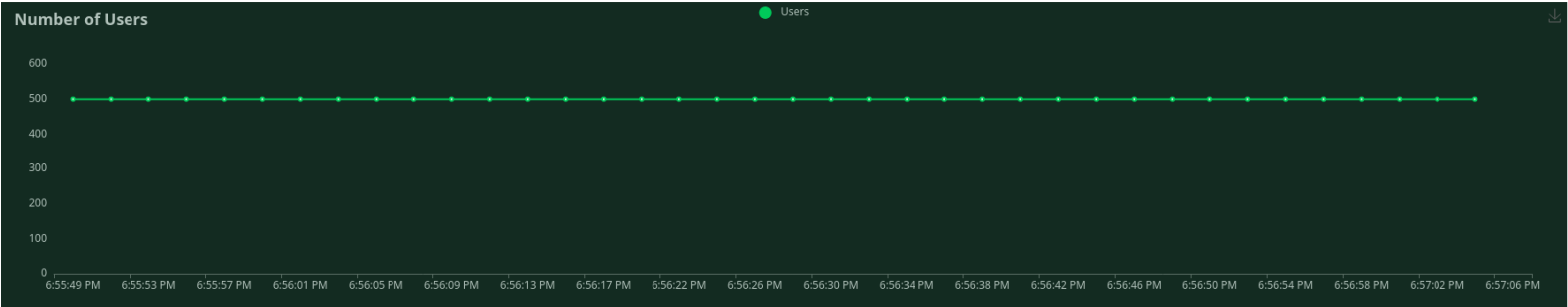
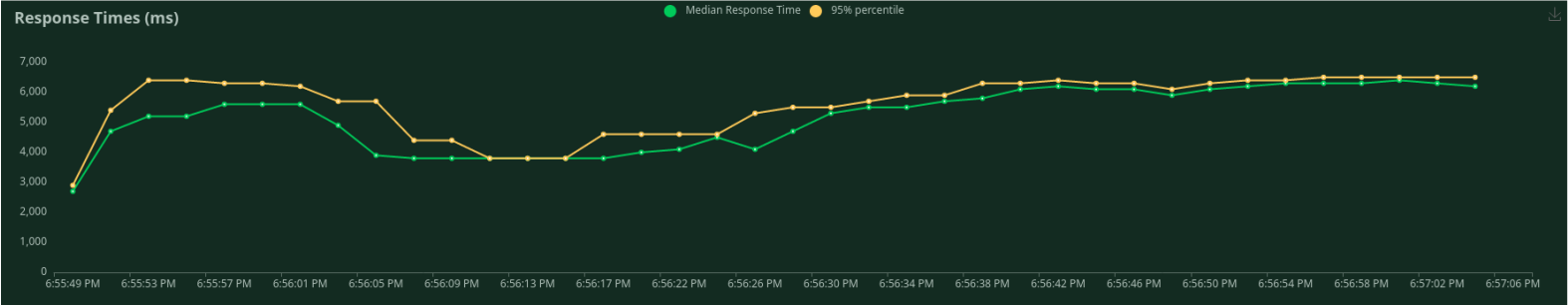
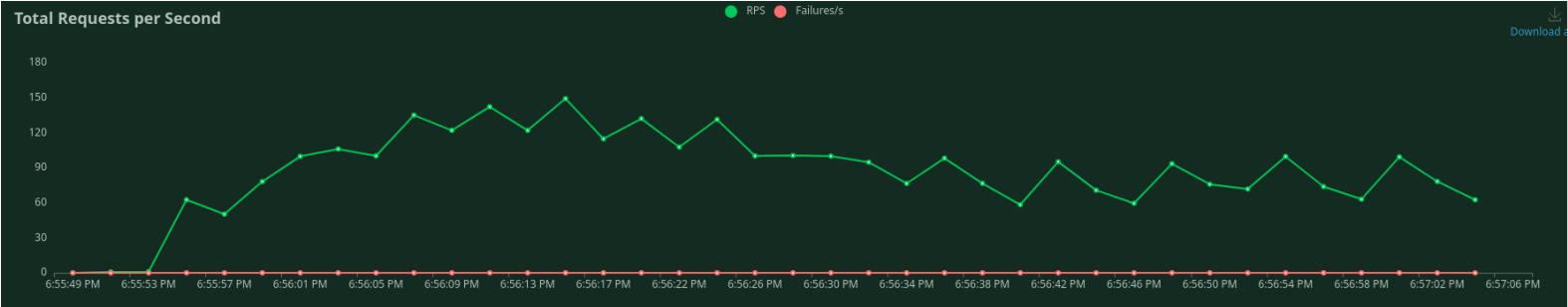


mCaptcha

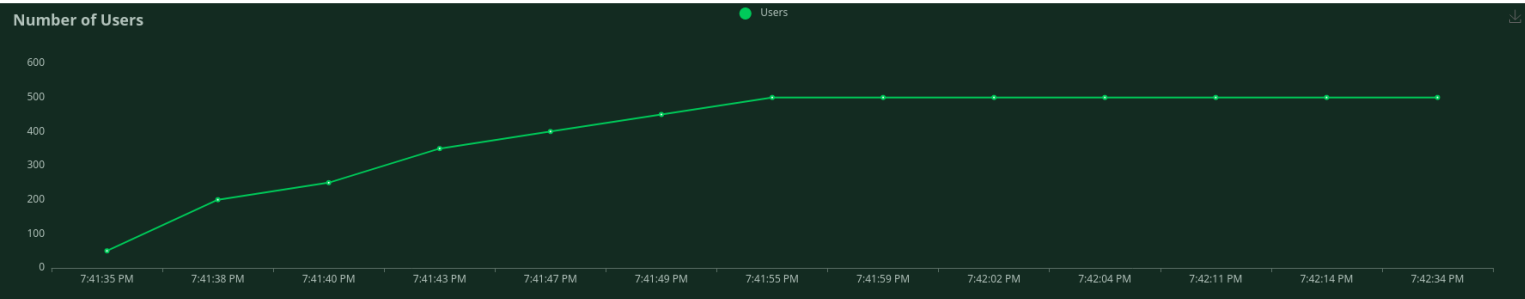
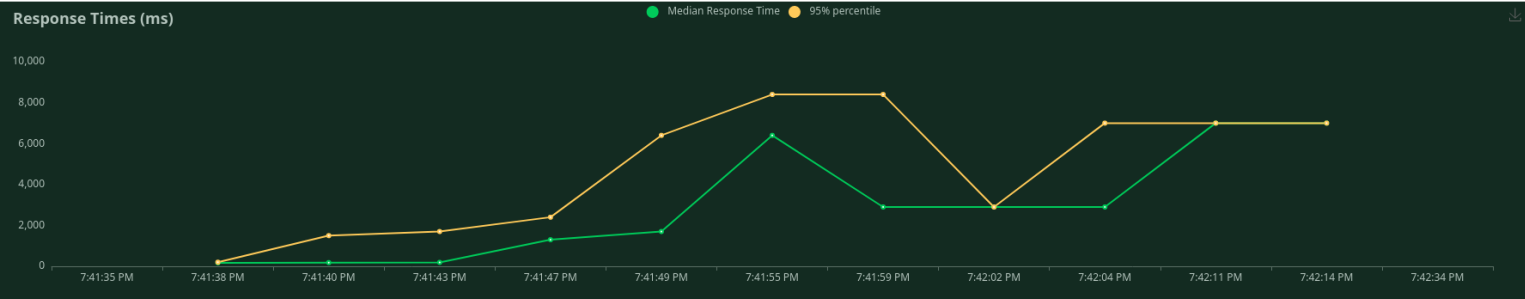
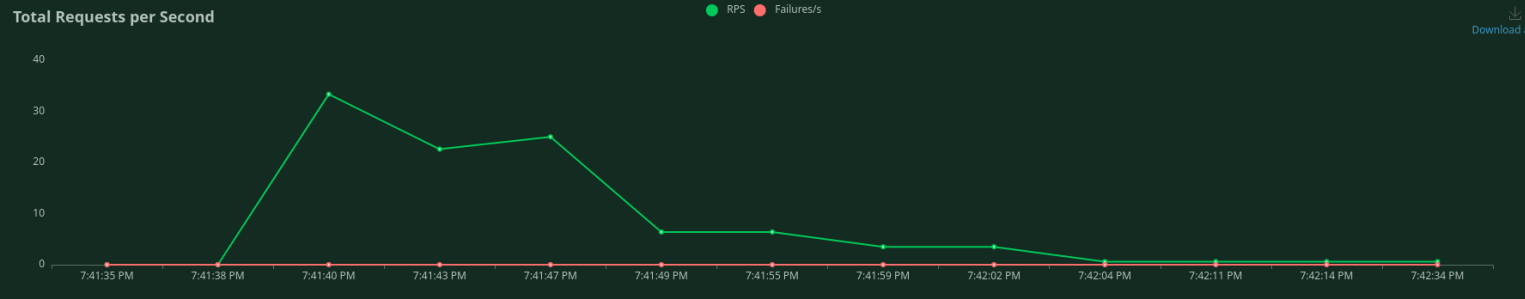
Performance and Protection Scope: Benchmark

- demo-server is a demo implementation with two endpoints that do the exact same thing: process and register a user but differ in the fact the one of them(/protected) is protected by mCaptcha.
- DDoS Benchmarks source code is available at: <https://github.com/mCaptcha/dos>

Benchmark: unprotected endpoint stats



Benchmark: protected endpoint stats



Accessibility

PROS

- All validation happens at the a click of a button. No images, no text and no audio.

CONS

- Hasn't been audited for accessibility
- Older, slow devices may fail validation. Can be mitigated by expert configuration but might still happen. survey.mcaptcha.org is WIP, should help admins when data is available.

Privacy

- No cookies
- IP is not logged; IP rate-limiting
- Works in Tor
- All JavaScript executed(and full project) is Free Software

Reasons for not choosing mCaptcha

- Single-person project
- Hasn't been audited
- Doesn't protect against spam

Resources

- Homepage: <https://mcaptcha.org>
- Source code: <https://github.com/mCaptcha>
- Matrix space: <https://matrix.to/#/#mcaptcha:matrix.batsense.net>
- Fediverse: [@mCaptcha@batsense.net](https://matrix.to/#/@mCaptcha@batsense.net)