you don't need anubis

In the past years, scrapers operated by LLM training companies have become more relentless. They no longer respect `` `robots.txt` ``, spoof their User Agents and IP addresses and even DDoS small sites with aggessive requests.[1]

This has led to more and more websites using Anubis, a proof-of-work based bot protection solution that requires all visitors to solve a small cryptographic problem on their device before proceeding.

But here’s the thing: **Anubis doesn’t work.** Well, alright, it does - it can be a good DDoS protection solution, especially for people who don’t want to use Cloudflare. But it seems like most users of Anubis *don’t need DDoS protection* - only protection against agressive LLM scrapers. And if that’s your only usecase, you probably **don’t need Anubis**.

People often claim that Anubis stops bots by making it too computationally expensive to access your website. Unfortunately, the price LLM companies would have to pay to scrape every single Anubis deployment out there is approximately $0.00.

But it still works, right? People use Anubis because it actually stops LLM bots from scraping their site, so it must work, right?

Yeah, but only because the LLM bots simply **don’t run JavaScript**.

I recently selfhosted Redlib, and despite not sharing my instance with anyone, it got rate-limited by Reddit due to all the scraper bots trying to get that sweet Reddit content. Here is my solution to the issue, a 12-line Caddyfile:[2]

```
domain.com {
    # Match all requests without a "verified" cookie"
    @unverified not header Cookie *verified*

    # Serve them a JS page that sets the cookie
    handle @unverified {
        header Content-Type text/html
        respond <<EOF
            <script>
            document.cookie = 'verified=1; Path=/;';
            window.location.reload();
            </script>
        EOF 418
    }

    # Proxy all other requests normally
    reverse_proxy localhost:3001
}
```

Yes, it works, and does so as effectively as Anubis, while not bothering your visitors with a 10-second page load time.

Sure, the bots may start running JS code one day, and then this will no longer work. But this also applies to Anubis - even people who use it often say that it’s just “a temporary stopgap until the bots learn how to bypass it”.[3] So if you use a temporary solution anyway, why not use one that is practically invisible for your users?

Unfortunately, Cloudflare[4] is pretty much the only reliable way to protect against bots. While the higher protection modes are still very annoying, especially to users on a VPN, there are some situations like actual DDoS attacks where you don’t have any other options. Even Anubis’ own README says:

> *“In most cases, you should not need this and can probably get by using Cloudflare to protect a given origin. However, for circumstances where you can’t or won’t use Cloudflare, Anubis is there for you.”*

I get that many people are strongly against Cloudflare’s internet monopoly, and I don’t blame them for using solutions like Anubis to protect their sites against real attacks. I’m also obviously not trying to throw shade on the Anubis project or its developers. I think it has a use as a DDoS protection solution - it’s just extremely overused by people who don’t need it.

So if your only concern is ClaudeBot, which seems to be the case for most of the websites that use Anubis, please, go and replace your annoying stopgap solution with a non-annoying one.

← prev |webring| next →