

Forum:[Hack Forums](#)

Thread: [Cloudflare WAF Bypass Origin server IP address](#)

Money- - November 10, 2022, 6:24 am

Just wondering , do you guys got anymore methods for this attack vector?
What's the latest methodology for it now at the moment?

kayla_90 - November 10, 2022, 4:11 pm

There is no way around it, you lucky if they left a service out of the cloudflare.

Blazin - November 10, 2022, 4:42 pm

There is no method, you hope they didn't put all sub domains on cloudflare.
You check if email server leaks IPS,

or lastly you check whois records and see if they leak the info.

Sekhmet - November 11, 2022, 2:01 am

(Nov 10, 2022 05:42 PM)Blazin Wrote: [\[CITE\]](#) There is no method, you hope they didn't put all sub domains on cloudflare.

You check if email server leaks IPS,

or lastly you check whois records and see if they leak the info.

+200 for this but also i have found a well known and widely used scripts that expose the real ip behind cloudflare if it's installed on the server ofc this is not " method " or even vulnerability it's just how this scripts work

Tip : look for misconfigured files

Brief - November 13, 2022, 10:17 pm

(Nov 11, 2022 03:01 AM)Sekhmet Wrote: [\[CITE\]](#) +200 for this but also i have found a well known and widely used scripts that expose the real ip behind cloudflare if it's installed on the server ofc this is not " method " or even vulnerability it's just how this scripts work

Tip : look for misconfigured files

Speaking of scripts, there might be some tools. I have seen a scanner report about a web application that has the real IP of the web application, even though the site was behind cloudflare.