

Forum:[Hack Forums](#)

Thread: [Cloudflare bypass via smtp headers? Information Disclosure?](#)

Venture - September 11, 2019, 6:09 am

So I've noticed that a website that sends emails; does so on the back-end through php function; I also know that when receiving an email, the headers of the email usually contain the mail servers ip; Would this lead to disclosure of the servers IP address?

BTC - September 11, 2019, 6:12 am

No it would just appear with a proxy address

SIGRU - September 11, 2019, 6:14 am

If the backend server sends emails yes, it will leak the site IP, obviously.

This has been a well known method for "bypassing" CloudFlare for some time, and HF even used to be vulnerable to it many years ago.

BTC - September 11, 2019, 6:15 am

(Sep 11, 2019 06:14 AM)SIGRU Wrote: [\[CITE\]](#) If the backend server sends emails yes, it will leak the site IP, obviously.

This has been a well known method for "bypassing" CloudFlare for some time, and HF even used to be vulnerable to it many years ago.

Only if your mail server's records are not configured properly in cloudflare. Most people know how to do that, in fact it did it automatically for me.

SIGRU - September 11, 2019, 6:43 am

(Sep 11, 2019 06:15 AM)BTC Wrote: [\[CITE\]](#) Only if your mail server's records are not configured properly in cloudflare. Most people know how to do that, in fact it did it automatically for me.

CloudFlare doesn't proxy email traffic. The emails still originate from the mail server, which will be the backend and will therefore be found in the email header.