

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Finding a websites IP behind Cloudflare/Reverse Proxy](#)

guardian - December 29, 2020, 8:23 am

Lots of sites hide their real server's IP using a service such as Cloudflare

In this tutorial I am going to present you a few ways, in order to find out the IP, even if the website uses some kind of portection

Let it be said that all these methods rely on poor configuration, so it will not work for sites that know how to configure their infrastructure

1. Web Server Errors

Web Server can return error codes, such as 404 or 403

In some cases the web server will reveal it's real IP, when returning an error of that type

This picture presents such a misconfiguration

If the site's owner does not set the web server hostname to the domain or even better, creates custom error messages, this kind of leakage could be prevented

2. Application Errors

Causing an error in an application, might cause the server to leak it's IP address

If the error reporting is not set to off and the website has kind of the settings it had in development still running in production, you can play around a bit and try to cause an error

When it works, you will get something like "unexpected parameter ' in application.php at xx.xxx.x.xxx"

I wanted to showcase this with a real life example I had saved for my tutorial, but cannot seem to find it right now, will edit should I find it

3. Historical DNS data

One of the most promising methods if you ask me that will at least point you in a good direction

The dnstrails feature of [securitytrails](#) will help your with this

It shows every DNS records that have ever been published for this domain

Lots of admins tend to first assign their domain to a single server, because "the site is not known yet"

However, this is a big mistake

The data can later be found and thus the real IP of the server

I would love to see some input on this and maybe methods you use for this

This Thread will probably be edited some time in the future to provide an example for #2 or to expand it by more methods that come to my mind

drneed - December 29, 2020, 9:43 am

here's something to check out, good article though

<https://dnsdumpster.com>

guardian - December 29, 2020, 9:49 am

(Dec 29, 2020 10:43 AM)drneed Wrote: [\[CITE\]](#) here's something to check out, good article though

<https://dnsdumpster.com>

Yes, DNSdumpster is also a great site, which shows all kinds of IPs that have to do with the site, thanks for adding it!