Hidden services and the effectiveness of CloudFlare or any similar service live from hiding the origin servers IP. Simple small mistakes can reveal the IP. This allows attacking a website that uses CloudFlare directly (bypassing the WAF, Rate Limits, DDoS Protection and much more) or even un-hiding a TOR hidden services operator identity. The mistakes depend on what type of service or technology you are working with, not all methods work for every technology (e.g. MX records don’t exist for TOR hidden services).

1. SSL certificates
   1.1 Using a given domain name
You are hosting a controversial service on xyz123boot.com. Your origin server IP is 136.23.63.44. CloudFlare is providing you with a DDoS Protection, Web Application Firewall and a couple of other services, that protect your project from the people, that would like to see your project offline. Your web server supports SSL and has a certificate, so the communication between CloudFlare and your server is encrypted just like the communication between your users and CloudFlare (i.e. no Flexible SSL). Everything else would be a false sense of security. So far so good.

The problem is the fact you’re also exposing the SSL certificate when directly connecting to your IP on port 443 (https://136.23.63.44:443). Scanning 0.0.0.0/0, the whole internet, on port 443 for a certificate valid for xyz123boot.com will give your web servers IP to the attacker.

Censys is doing the scan for you. The only thing you have to do is translating the above search terms described in words into actual search queries.

Certificates for xyz123boot.com: parsed.names: xyz123boot.com
Just show valid ones: tags.raw: trusted

Combining multiple parameters on Censys can be done by using simple Boolean logic.

Search term: parsed.names: xyz123boot.com and tags.raw: trusted
Censys will show you all the certificates matching the above criteria, which they found in their scans.
Clicking on the search results one by one, you can open a drop-down with several tools by clicking on "Explore" on the right side. Choose **What's using this certificate? > IPv4 Hosts**.

You'll be presented a list of IPv4 Hosts using the specific certificate. One
You can verify by navigating to the IPs on port 443. Does it redirect to xyz123boot.com? Does it show the website directly on the IP?

1.2 Using a given SSL certificate

You are the FBI and want to shut down a child porn hidden service available under cheeseep5vaogohv.onion. To do that, you need the origin IP so you can contact the host and possibly also hunt down the operator then by following the money for example.

The hidden service has an SSL certificate. Finding IPv4 Hosts that use the same certificate can be done by just pasting its SHA1 fingerprint.
(without the colons) into the Censys IPv4 Hosts search. A badly configured web server can easily be found with this method.

2. DNS records

After suffering from multiple attacks, you decided to start using CloudFlare. Data-driven services like Censys for DNS records still have your old A records pointing to your web servers IP address.

A platform doing exactly this is SecurityTrails. Just enter the website domain into the search field and press enter. The "Historical Data" can be found in the sidebar on the left side.

Besides the old A records, even current DNS records can leak the origin servers IP. MX records, for example, are a common way of finding your IP. If the website is hosting its own mail server on the same server and IP as the web server, the origin server IP will be in the MX records.

3. HTTP Headers
3. HTTP Headers

With data-driven platforms that let anyone do powerful searches across a huge amount of data, even finding origin servers by comparing HTTP headers is a possibility.

Especially when having a pretty unique server header with various software including subversions, finding you is getting much easier. This is also not limited to a single parameter. As mentioned in 1.1, you can combine search parameters on Censys. The likelihood of being found with this method is increasing with every less common header key or value you are sending.

Let’s say you are sharing your server HTTP header with 1500 other web servers, which are sending the same header key and value combination. You are also using a new PHP framework sending a unique HTTP header (for example: X-Generated-Via: XYZ Framework). About 400 webmasters are using that framework in production yet. The intersection consists of a final amount of three servers. Going through those manually takes a few seconds and you found IP.

As an example, the search parameter at Censys for matching server headers is `80.http.get.headers.server:`.

Finding websites being served by CloudFlare works like this:

`80.http.get.headers.server: cloudflare`
4. Applications and Services

A TOR hidden service or a website being served through CloudFlare is a normal website. Starting a quick pentest could reveal the IP as well.

Headers like the HTTP server header can be used to find possible exploits for the services and versions in use. When gaining access to the server, you can obviously easily find the IP.

Another attempt would be to find edge cases triggering errors. Error messages can reveal sensitive information. Those pieces of information could be just the IP itself or anything that can be used as parameters for the other methods described here. This is all about being creative, doing recon and combining.

Running gobuster to find files and directories during the recon phase should be done in every pentest. Things you could find are logs, database dumps/backups and more.
Also, worth a check is to find out if you can make the application powering the website to interact with other services. If you’re not the NSA, you probably can’t get the IP if they are just consuming an API. But as an example, maybe you can set an avatar on the website and provide an URL to the picture instead of uploading it. If they are downloading it, they are probably doing it from their origin server. Now the IP is in your logs.

This was just a quick overview. You can do a large portion of all the pen-test magic you would normally do and there are many mistakes webmasters could have made.

5. Content

In case the origin server IP is returning the content of the website as well, the massive amount of data searchable on the web got you again.

Going through the websites source code, you are looking for unique pieces of code. Third party services (e.g. Google Analytics, reCAPTCHA) with access/identifier keys in the JavaScript are a good start.

Example Google Analytics Tracking Code taken from HackTheBox website:

```javascript
ga('create', 'UA-93577176-1', 'auto');
```

Filtering Censys data by the body/source can be done with the `80.http.get.body:` parameter.

Unfortunately, the normal search field has limitations. You can request research access at Censys, which allows you to do much more powerful queries via Google BigQuery.

Shodan, a service similar to Censys, provides a `http.html` search parameter, too.

An example search:
Final notes

In the end, finding the origin IP behind TOR hidden services or reverse-proxy services like CloudFlare mostly requires a certain amount of understanding of the web and creativity.

Securing a Web Hidden Service by x0rz explains countermeasures for TOR hidden service operators against several methods covered in this article. It also contains glorious fails, in which hidden services didn’t master opsec, so security researchers could unmask them.
Do you run a hidden service or are you using CloudFlare? Made any of the mistakes described above?

What other methods could reveal origin IPs? I’d be glad to hear about them so we can make this an even more comprehensive resource.

Main Image Credit: The awesome piece of artwork used to head this article is called 'Mystic Cat' and it was created by graphic designer Alexa Erkaeva.

Update Note (19/8/2018) in response to Higinio “w0rmer” Ochoa (CloudFlare Security Engineer)

Shortly after publishing the article, a Security Engineer at CloudFlare added a couple of valid comments. Kudos to CloudFlare as their security team seems to be up to date in terms of new articles and everything related to security especially regarding their own service.

Oooh looks like someone hasn’t heard of Argo Tunnels
https://t.co/aVWJBMX4N5

— Higinio “w0rmer” Ochoa (@0x686967) 19. August 2018

All examples in this article work like this when making the mistakes do