[Uncover Hidden Subdomains to Reveal Internal Services with CT-Exposer](https://null-byte.wonderhowto.com/how-to/uncover-hidden-subdomains-reveal-internal-services-with-ct-exposer-0187286/)

* BY [**KODY**](https://creator.wonderhowto.com/kody/)
* 09/26/2018 2:29 PM

Most companies have services like employee login portals, internal-only subdomains, and test servers they would prefer to keep private. Red teams and white hat hackers can find these obscure and often vulnerable services using a tool designed to help protect users from fraudulent certificates.

What Is a Certificate Trust Log?

Certificates are issued to companies operating online services by a certificate authority to protect users from being directed to fraudulent websites. In 2011, limitations in the ability of certificates to protect users were demonstrated by attacks against certificate authority companies Comodo and DigiNotar. Because it took a long time for the fraudulent certificates to be discovered, certificate trust logs were created to provide better transparency for users.

* **Don't Miss:**[**Use the Buscador OSINT VM for Conducting Online Investigations**](https://null-byte.wonderhowto.com/how-to/use-buscador-osint-vm-for-conducting-online-investigations-0186611/)

Facebook has used CT logs to discover mis-issued TLS certificates and stop them from being used to intercept HTTPS traffic. This success prompted them to release a [CT log tool to the public](https://developers.facebook.com/tools/ct), with the ability to "subscribe" to a domain to quickly see certificates issued to it.

Ironically, releasing this tool led directly to several bug bounty reports in which Facebook test servers that didn't have the same permission checks as production servers were discovered, potentially leading to free access to all kinds of information. This perfectly illustrates how CT trust logs can reveal an unintended amount of information at the company while intending to detect domains using fraudulent certificates.

* **Don't Miss:**[**How to Use SpiderFoot for OSINT Gathering**](https://null-byte.wonderhowto.com/how-to/use-spiderfoot-for-osint-gathering-0180063/)

Hidden subdomains can reveal hidden pages like employee logins, web applications in use, internal-only domains that can only be visited from an internal DNS, and old or deleted domains. While we can use [Facebook's CT monitoring tool](https://developers.facebook.com/tools/ct) online to find hidden subdomains, we'll be using a local tool for more anonymity. It's called CT-exposer, a Python OSINT scanner that's easy to run on any platform. It won't show us much data as Facebook's tool does, nor provide as many results, but the information is much easier to wade through.

What You'll Need

To get started using CT-exposer, you'll need to make sure Python3 is installed on your computer. If you don't have it, you can download it from the [Python.org](https://www.python.org/downloads/" \t "_blank)website. Once you have Python installed, you can ensure you have the right version by typing **python3** into a terminal window. If the output looks similar to the below output, you should be good. You can type **quit()** after the >>> to exit.

python3

Python 3.6.4 (v3.6.4:d48ecebad5, Dec 18 2017, 21:07:28)

[GCC 4.2.1 (Apple Inc. build 6996) (dot 3)] on husker

Type "help", "copyright", "credits" or "license" for more information.

>>> quit()

If you're running Kali Linux, make sure to update and upgrade your system as well with the following commands.

apt update

apt upgrade

Step 1Download & Install Requirements

With Python installed and your system fully updated, you can begin by navigating to the [GitHub page](https://github.com/chris408/ct-exposer" \t "_blank) for CT-exposer. Once there, copy the URL under the clone or download button and run the **git clone** command in a terminal window, as such:

git clone https://github.com/chris408/ct-exposer.git

Once the files finish downloading, [change directories](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-2-creating-directories-files-0147234/) to root, **cd** to the **ct-exposer**folder, then install the requirements, like this:

cd ct-exposer

sudo pip3 install -r requirements.txt

Once the requirements are installed, you should be ready to go!

Step 2Select Domain & Run Scan

To begin exploring what CT logs can reveal, take a test domain and see what information can be revealed from an attacker's perspective. To start, try priceline.com.

The main URL for this nonsense is priceline.com, so run CT-exposer on the URL to see what you can find. Make sure you are in the ct-exposer folder. Once you're in the ct-exposer folder, you can run the following command to scan the certificate trust logs for the **priceline.com** domain.

python3 ct-exposer.py -d priceline.com

Step 3Break Down & Interpret the Scan

In the output below, we see the results of the priceline.com scan. Wow! There are a lot of results, but how could they be useful?

sudo python3 ct-exposer.py -d priceline.com

[+]: Downloading domain list...

[+]: Download of domain list complete.

[+]: Parsed 33 domain(s) from list.

[+]: Domains found:

23.23.126.26 admin.groupcommerce.com

178.250.2.116 app-install.priceline.com

35.241.46.146 appinstall.priceline.com

64.6.22.95 bomgar.corp.priceline.com

161.47.16.153 careers.priceline.com

209.202.133.98 cruises.priceline.com

64.6.22.95 dealreveal.corp.priceline.com

69.195.35.215 enet.qahotelportal.priceline.com

151.101.196.65 g.ssl.fastly.net

185.28.222.22 h.priceline.com

185.28.222.21 hsecure.priceline.com

64.6.22.100 mail.corp.priceline.com

104.196.14.36 media.priceline.com

64.6.22.95 phantom.corp.priceline.com

104.131.82.197 picme.priceline.com

151.101.196.204 priceline.map.fastly.net

69.195.35.246 qahotelportal.priceline.com

64.6.22.95 splunkes.corp.priceline.com

64.6.22.95 ssh.corp.priceline.com

69.195.35.226 travela.a1.qa.priceline.com

64.6.21.26 travela.priceline.com

69.195.35.166 www.a1.dev.priceline.com

69.195.35.245 www.a1.qa.priceline.com

64.6.23.56 www.a309.corp.priceline.com

69.195.35.167 www.b1.dev.priceline.com

151.101.130.186 www.priceline.com

69.195.35.143 www.qaa.priceline.com

[+]: Domains with no DNS record:

none enet.hotelportal.priceline.com

none fs.corp.priceline.com

none pcln04.corp.priceline.com

none rsecure.priceline.com

none secure.priceline.com

Example 1Subdomains with DNS That Does Not Resolve

You can attempt to navigate to the various subdomains that appear. If they do not resolve, it can have one of several meanings.

See what happens when you attempt to access an internal service, as in a service you have to be connected to an internal DNS server to access. For instance, if you attempt to navigate to **mail.corp.priceline.com** from your web browser, you're met with the following.

This is different than what you see when the page you're trying to go to does not exist. This does exist, you just can't see it on a public server. To a red team or an attacker, a piece of internal infrastructure was just discovered. A simple [Nmap](https://null-byte.wonderhowto.com/collection/nmap/) will show a Microsoft-IIS/8.5 server sitting at that address.

Example 2Subdomains with DNS That Does Resolve (1)

Some subdomains do resolve and aren't that secret at all. However, to an attacker, knowing about this can let you make an early pass to explore a possible avenue of attack.

For one example, you see a careers subdomain at **careers.priceline.com**. As an attacker, I've just learned what kind of resume I need to copy and drop into these job postings to get the attention of an HR employee at Priceline. Maybe I can even get them to open a PDF resume with an exploit, but even if they use an outsourced hiring company, I can learn about the physical locations they operate from and the type of systems they use by carefully reading the job requirements.

Example 3Subdomains with DNS That Does Resolve (2)

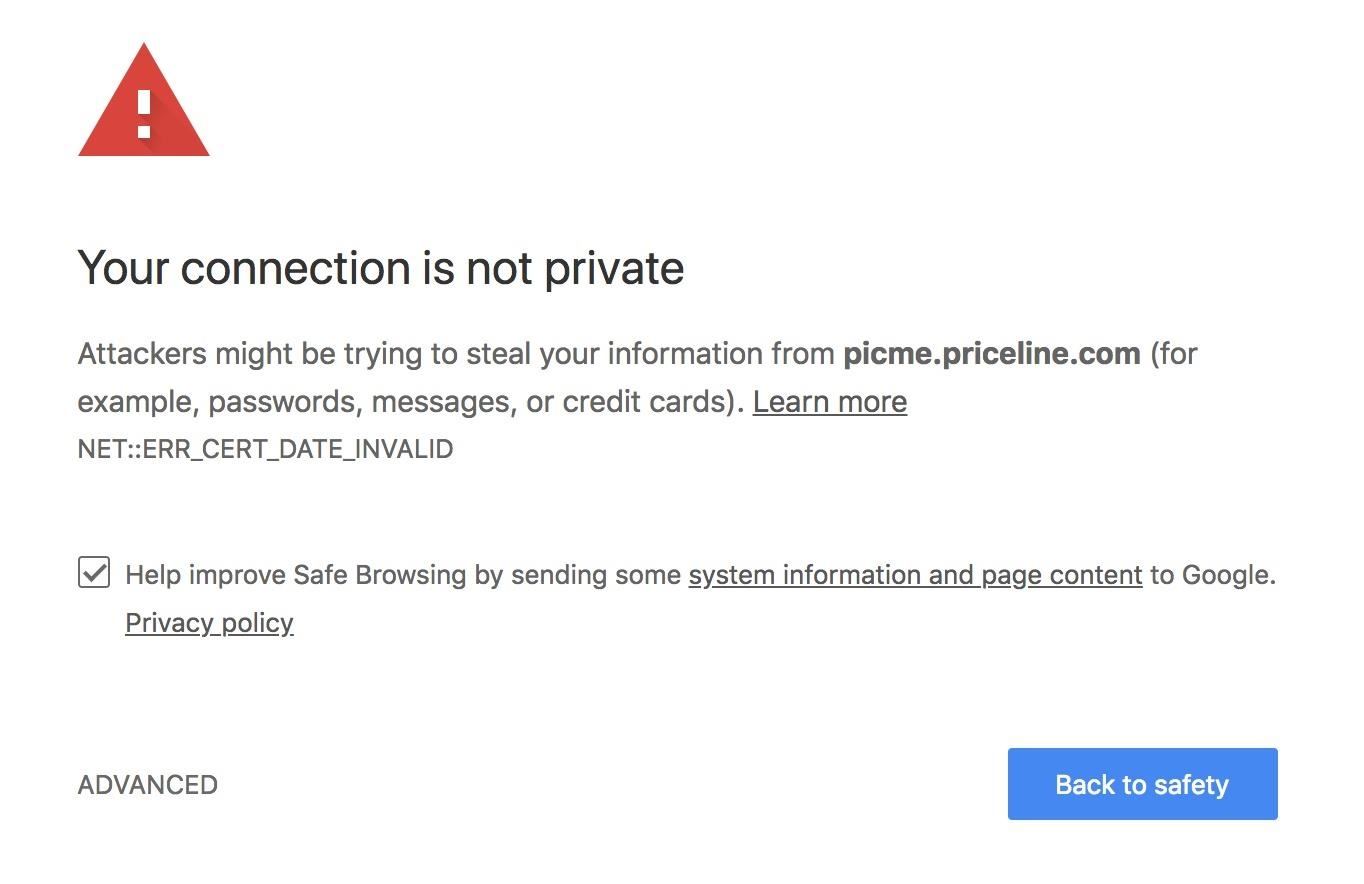
By following the subdomain breadcrumbs, you can continue to discover subdomains where the DNS does resolve. Another example, **h.priceline.com**, which resolves to an insecure website with a very old copyright date. The page talks about a bunch of services they either no longer offer or advertise.

Example 4Subdomains with DNS That Does Resolve (3)

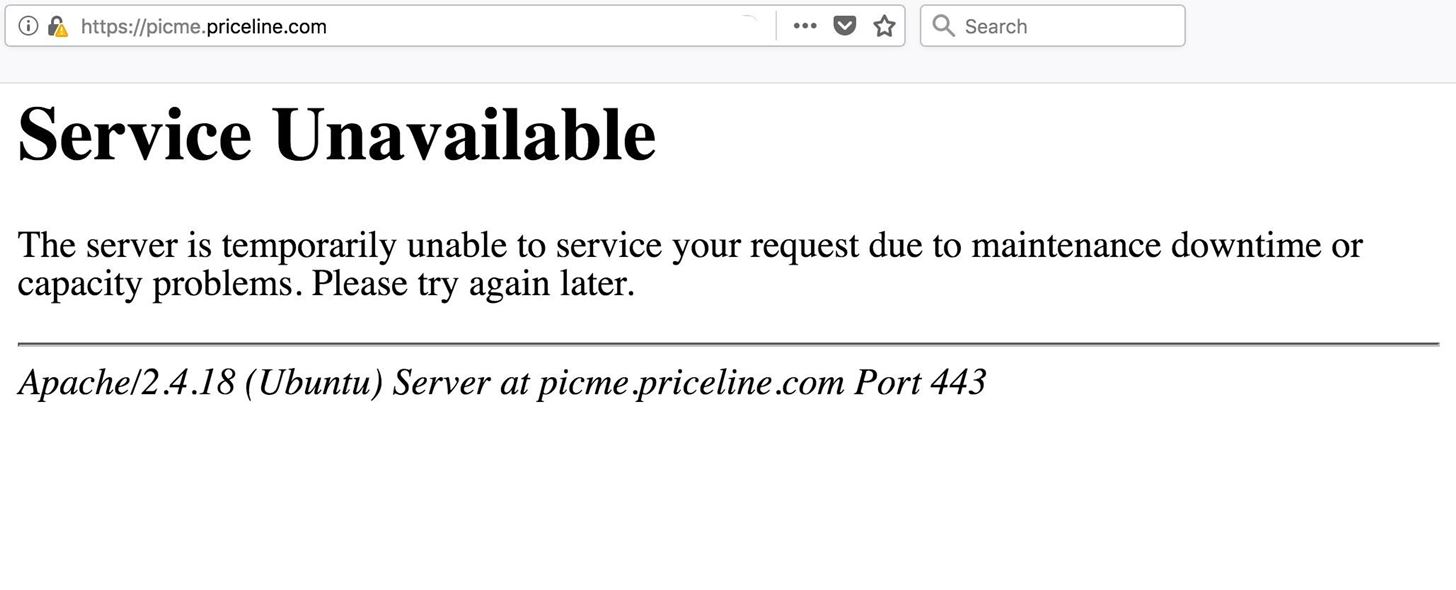
Similarly, **media.priceline.com** does actually resolve, this time to a secure website using HTTPS for press like myself, but also last updated in 2014. I'm sure nothing has changed since then.

Example 5Subdomains with DNS That Does Resolve (4)

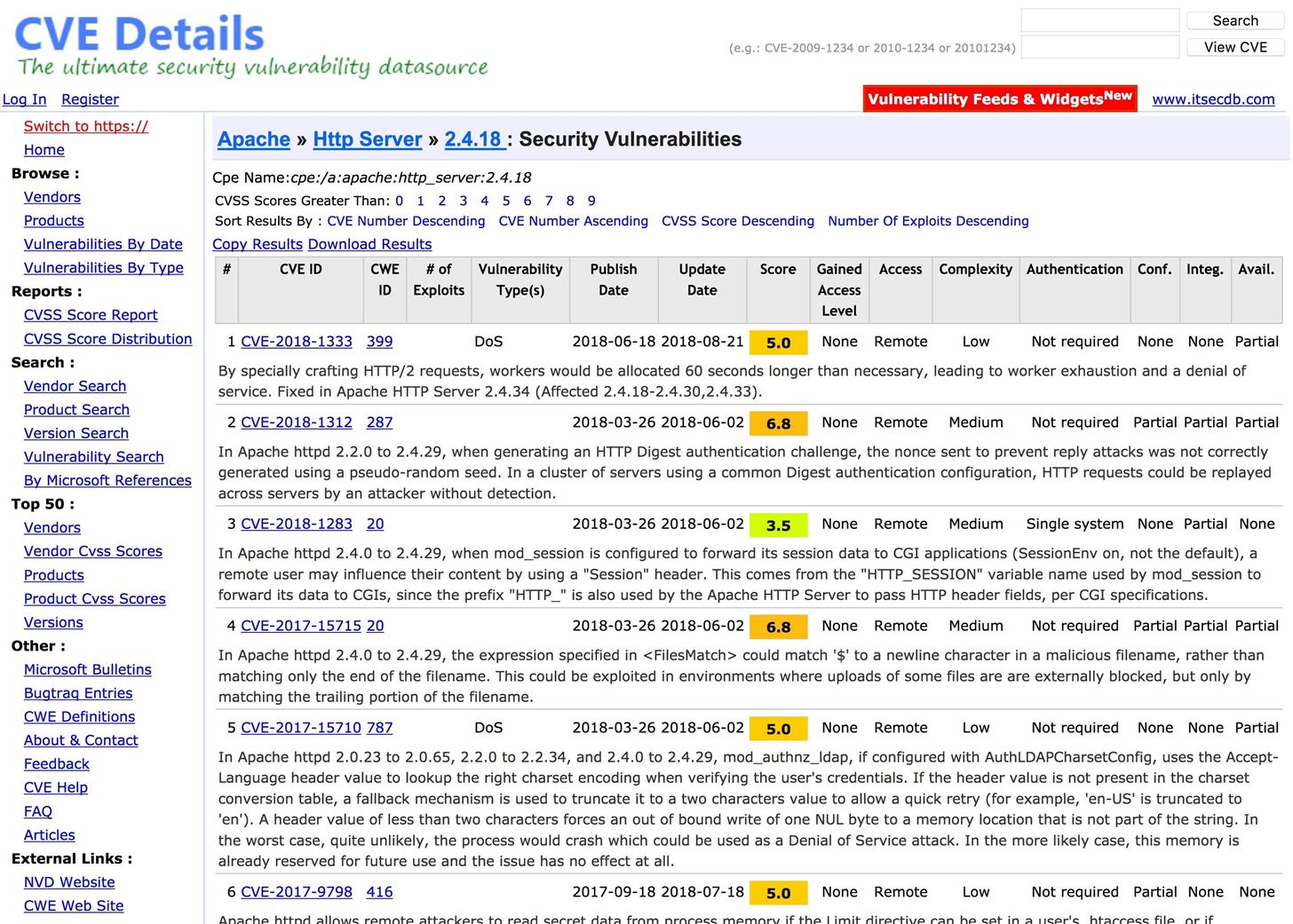
In some instances, the transportation layer security will be broken, and you'll get a big warning like that below when trying to resolve **picme.priceline.com**, for instance.

[](https://img.wonderhowto.com/img/original/62/15/63673563610857/0/636735636108576215.jpg)

If you ignore it and proceed, you can see that the whole server is broken, giving an error message with more information about it. (Gee, thanks for the needless information.)

[](https://img.wonderhowto.com/img/original/77/92/63673563802513/0/636735638025137792.jpg)

As you can see, there's an Apache 2.4.18 server sitting on an Ubuntu on port 443. Hmm, that seems kind of old. Go ahead and Google that exactly to see if there could be anything wrong. Surely the fortress of information that is priceline.com couldn't be exposing an old, vulnerable server to the internet.

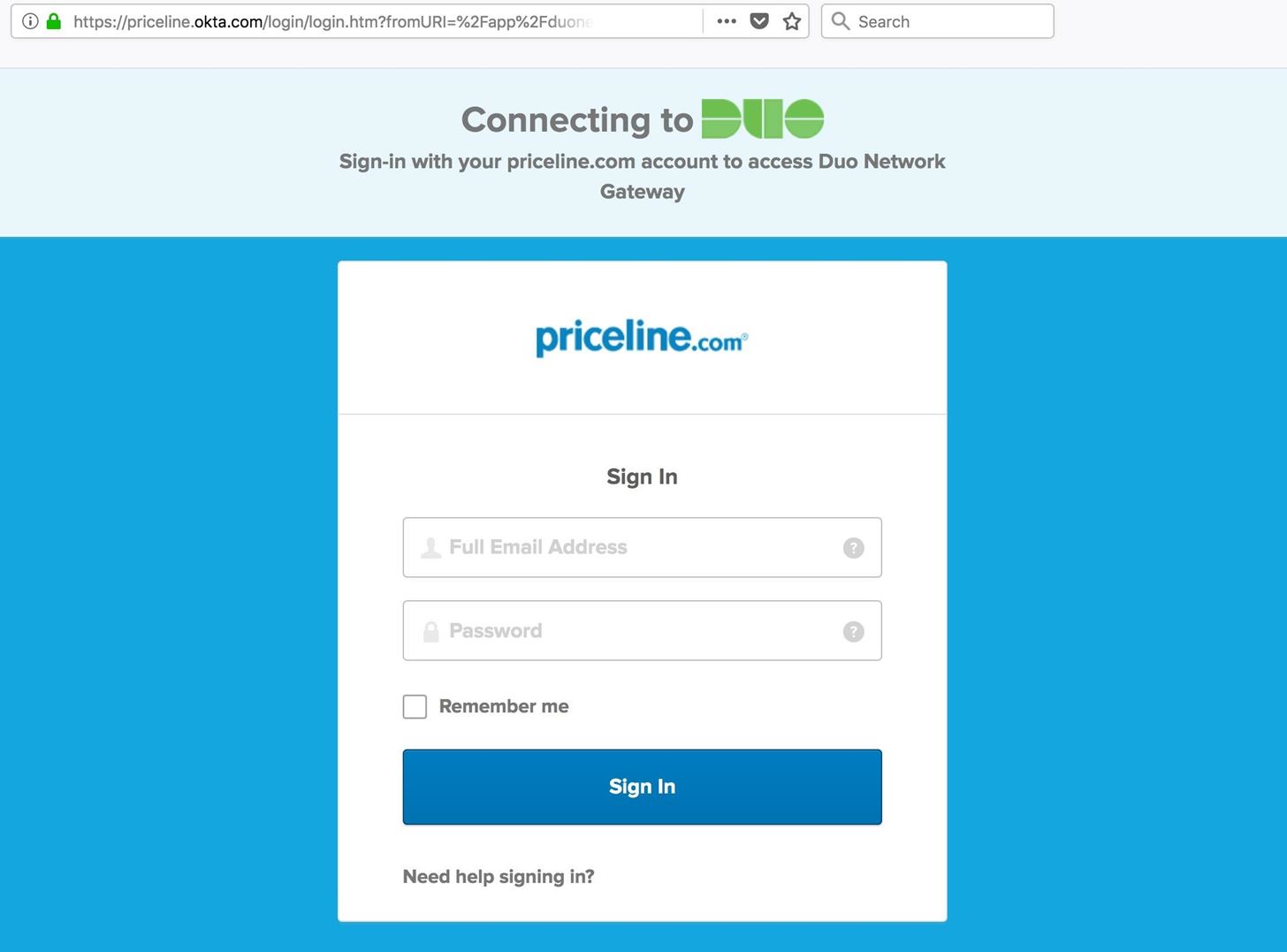
[](https://img.wonderhowto.com/img/original/80/79/63673564180763/0/636735641807638079.jpg)

Oh my god. There are 16 different vulnerabilities. In this case, you could just move on, assuming this is so riddled with issues that it's probably a honeypot. Wouldn't you feel bad kicking this poor thing?

* **Don't Miss:**[**Research a Person or Organization Using the Operative Framework**](https://null-byte.wonderhowto.com/how-to/recon-research-person-organization-using-operative-framework-0176323/)

Example 6Subdomains with DNS That Does Resolve (5)

Finally, there's the crown jewel of the discovery: employee login and application endpoints! These watering holes are where you can learn about the security of your targets and attempt to grab passwords. For example, when you attempt to resolve **phantom.corp.priceline.com**, you are greeted with the following page challenging for a login.

[](https://img.wonderhowto.com/img/original/31/28/63673565176451/0/636735651764513128.jpg)

So, does this mean that Priceline is running a phantom corporation? In may feel like it but, in fact, these are just endpoints to things like email, hotel logins, and other services employees access from outside the Priceline network.

Here, the two important things you can learn are that Priceline is using okta.com for authentication and requires two-factor authentication through "Duo" security.

If I was an attacker, I now know that employees receive a push notification each time they log into a company resource on a new device. This means capturing usernames and passwords are useless without also capturing this authentication layer.

Example 7Subdomains with No DNS Record

You will also likely have several domains which have no DNS record. This means you cannot navigate to them because no known route exists on the public internet. So what does this mean?

[+]: Domains with no DNS record:

none enet.hotelportal.priceline.com

none fs.corp.priceline.com

none pcln04.corp.priceline.com

none rsecure.priceline.com

none secure.priceline.com

This means they are serviced by an internal DNS server or require you to be logged into a VPN to access. This makes these subdomains some of the most interesting of all, as they represent internal attack surfaces you do not yet have access to. They also act as targeting information for your initial attacks and a potential way of tricking employees into thinking they are on a private network when they are really on a public one.