Securing a Web Hidden Service

Quick guide on how to preserve a .onion anonymity

x0rz · Follow
Published in Just another infosec blog type of thing
4 min read · Oct 24, 2017

Listen Share

While browsing the darknet (Onion websites), it's quite stunning to see the number of badly configured Hidden Services that will leak directly or indirectly the underlying clearnet IP address. Thus canceling the server anonymity protection that can offer Tor Hidden Services.

Here are a few rules you should consider following before setting up a Onion-only website. This guide covers both **Apache** and **Nginx**.

1) Listen to localhost only

Don't let anyone reach your Onion web application through the clearnet. Plain and simple. Your web server should only listen to 127.0.0.1 so that uniquely the Tor daemon can connect to it. If you can't listen to localhost (for whatever reasons), use

a god damn firewall (iptables/nftables) to prevent any leak or — at the very least — make sure the default virtual host isn't redirecting to your Onion application.

The reasons why you shouldn't be accessible on clearnet are ***scanners***. Scanners from Shodan or Censys (or even Google) are constantly scanning all the IPv4 public space (what we can call 0.0.0.0/0) and will scan and index your server as well. You'll be easily uncloaked if scanners find matching HTML content of your website, or even matching HTTP headers (see examples below).

On **Apache**, change */etc/apache2/ports.conf* so that it contains:

```
Listen 127.0.0.1:80
```

On **Nginx**, you should add a listen statement in the */etc/nginx/nginx.conf* file, (inside a *sever* section):

```
listen 127.0.0.1:80;
```

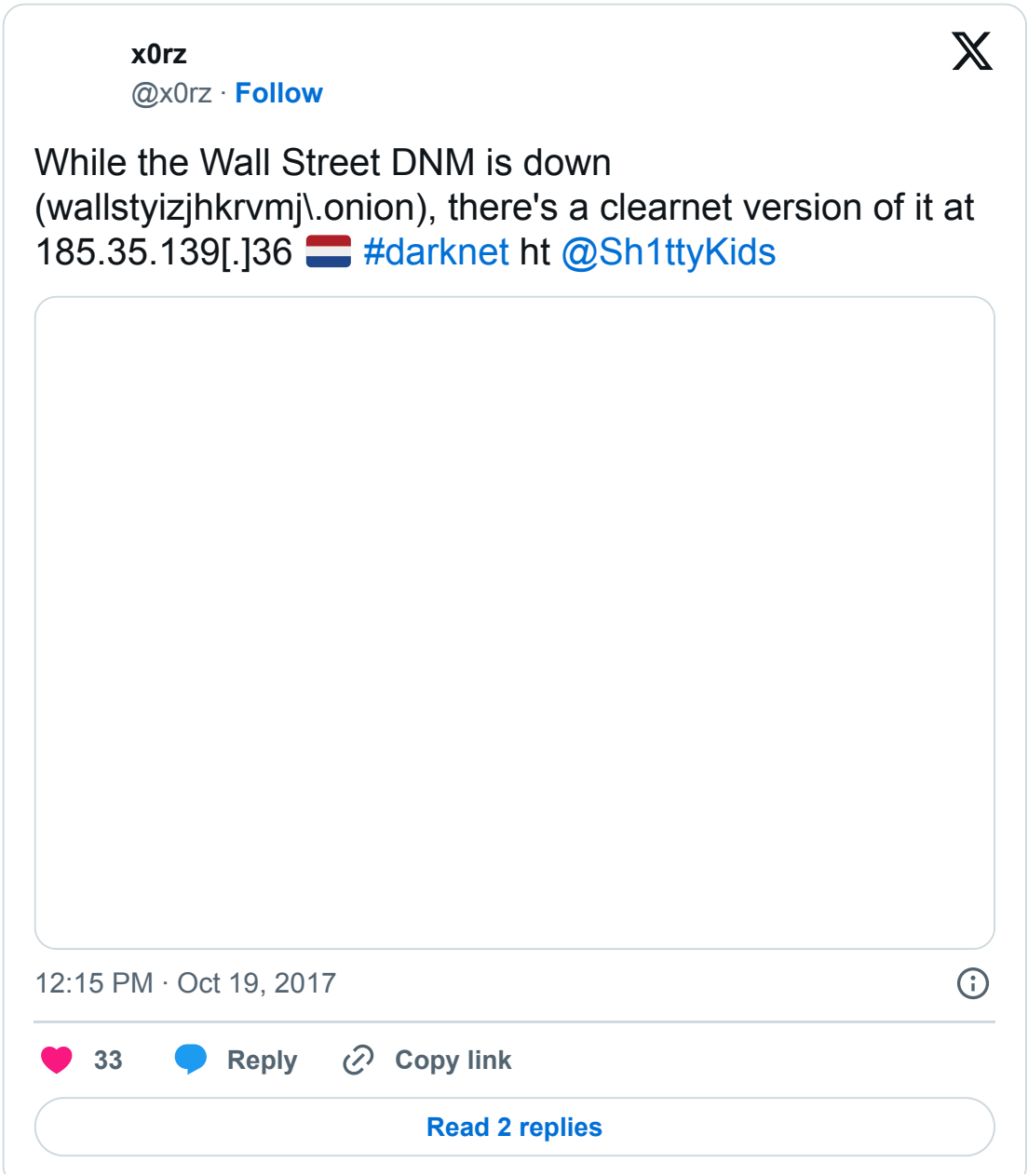
There are some pitfalls to this method but it's the least you can do (and quickest way to prevent any major leak). If you're using Apache and want to go further I encourage you reading Alec Muffett comment on that:

Listening to "localhost" is kinda-okay because it is better than the threat as-described; however...

See this thread for details: https://twitter.com/AlecMuffett/status/922924914893398017

medium.com

Most notorious fails



2) Disable directory listing

"Directory listing" or "directory indexing" is a known plague, even for clearnet websites. It's considered by OWASP as a common vulnerability, but given the sensitivity of most hidden services it is just unacceptable to leave this open on a serious HS.

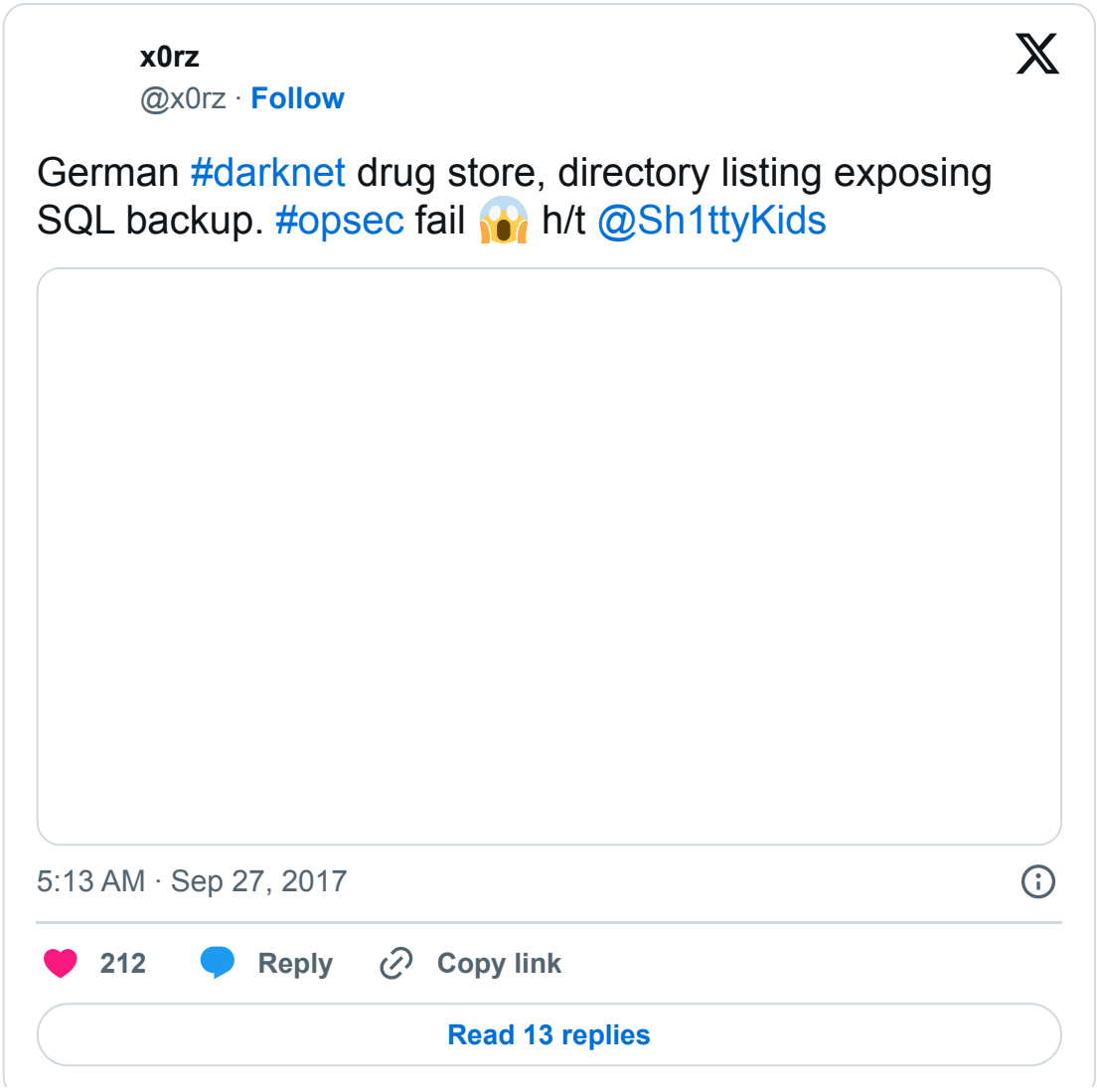
On **Apache** you can either disable the *mod_autoindex* (as root, simply type `a2dismod autoindex`) or add a `Options -Indexes` directive to your root web directory:

```
<Directory /var/www/>
Options -Indexes
</Directory>
```

On **Nginx**, disable the autoindex module in *nginx.conf* file:

```
location / {
    autoindex off;
}
```

Most notorious fails



3) Disable verbose signature and error reporting

This is to ensure your server have a tiny fingerprint, no specific headers or unique version number to track you down.

3.1) Disable server-info and server-status (Apache only)

On some configuration Apache is showing by default */server-info* and */server-status* pages leaking internal data (such as URL requested from other users).
You can easily disable it by removing the mod_info from *httpd.conf* or by

commenting out the `<Location/server-info>` and `<Location/server-status>` directives in the configuration file.

3.2) Removing the server signature

This will ensure that the version of your webserver and the OS server name won't leak in the *Server* header and inside default error webpages (404, 500, ...).

On **Apache** simply add these directives your default *httpd.conf* file (on Debian 8 you can directly edit */etc/apache2/conf-enabled/security.conf*):

```
ServerSignature Off
ServerTokens Prod
```

On **Nginx**, disable the server_tokens in *nginx.conf*:

```
http {
    server_tokens off;
}
```

3.3) Disable application error reporting

This depends on the backend language you're using (PHP, NodeJS, Python, etc.), I won't go into the details for each on how to disable error reporting, Google is your friend. Most error reporting (stack traces, memory dumps, etc.) are likely to leak your IP address or other relevant information: disable them all! FYI, this may be how the Silk Road DMN was taken down.

Most notorious fails

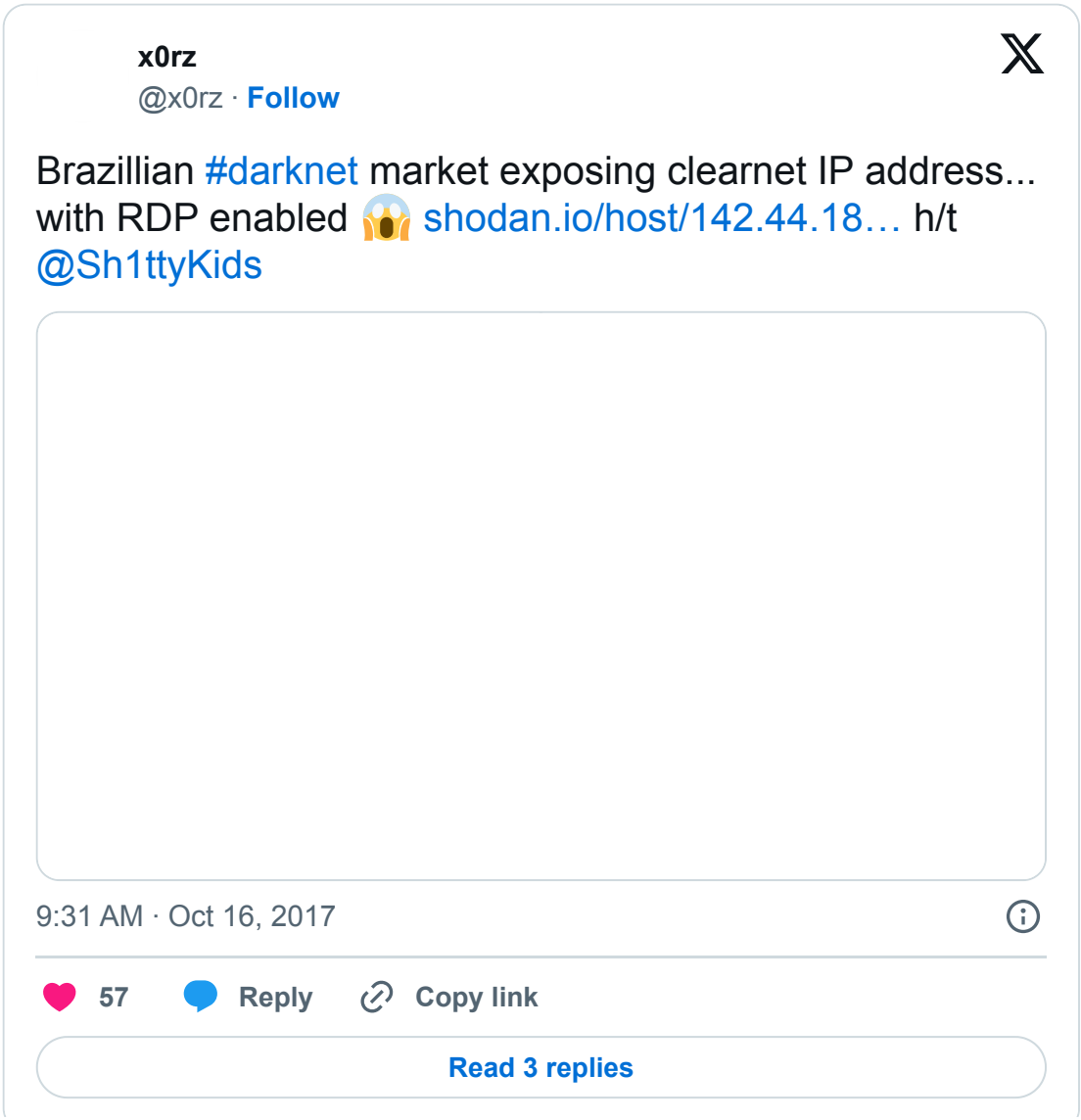
x0rz
@x0rz · **Follow**

Yet another poorly configured #darknet market (server-status) 🤦
xdsa5xcrrrxxxolc[.]onion
wacky2yx73r2bjys[.]onion
tdupp6lmgnpex5ss[.]onion

8:59 AM · Oct 2, 2017

64 Reply Copy link

Read 6 replies



4) Fix your flaws

Patch your god damn server (**keep it up to date**), write code that isn't shit and riddled with SQL injections, and you should be *fine*. If you're reading this guide and learning new sysadmins tricks, my best advice is that you should probably stay away from darknet entrepreneurship (especially darknet markets and all form of illegal activities online).

Apply some basic security measures as disabling unwanted services, respect the principle of least privilege and compartmentalize the different layers of your web application. For the rest, use common sense.

If it helps, you can follow some security hardening guide to tighten your configuration. Bonus points if you install grsecurity/PaX on your box.

5) Route only Tor traffic (advanced)

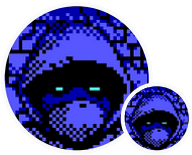
Some web applications are sending verification e-mails that might leak your IP address to the recipient. This can also happen if your app tries to reach any third

party through clearnet (bitcoin payment API, analytics, Twitter, ...). In order to prevent this from happening, I recommend you to transparently route all outgoing traffic through Tor. The Tor Project has a guide on how to set up a Transparent Proxy.
TL;DR: set your firewall to deny all outgoing connections except from those coming from the Tor process.

> Keep in mind nothing is bulletproof and 0day can (or must) be part of your threat-model if you're somewhat serious about anonymity.

If you liked this article, you can also buy me a coffee ☕ anytime!

Privacy Cybersecurity Sysadmin Apache Censorship



Written by x0rz

3.2K Followers · Editor for Just another infosec blog type of thing

Security Researcher

More from x0rz and Just another infosec blog type of thing

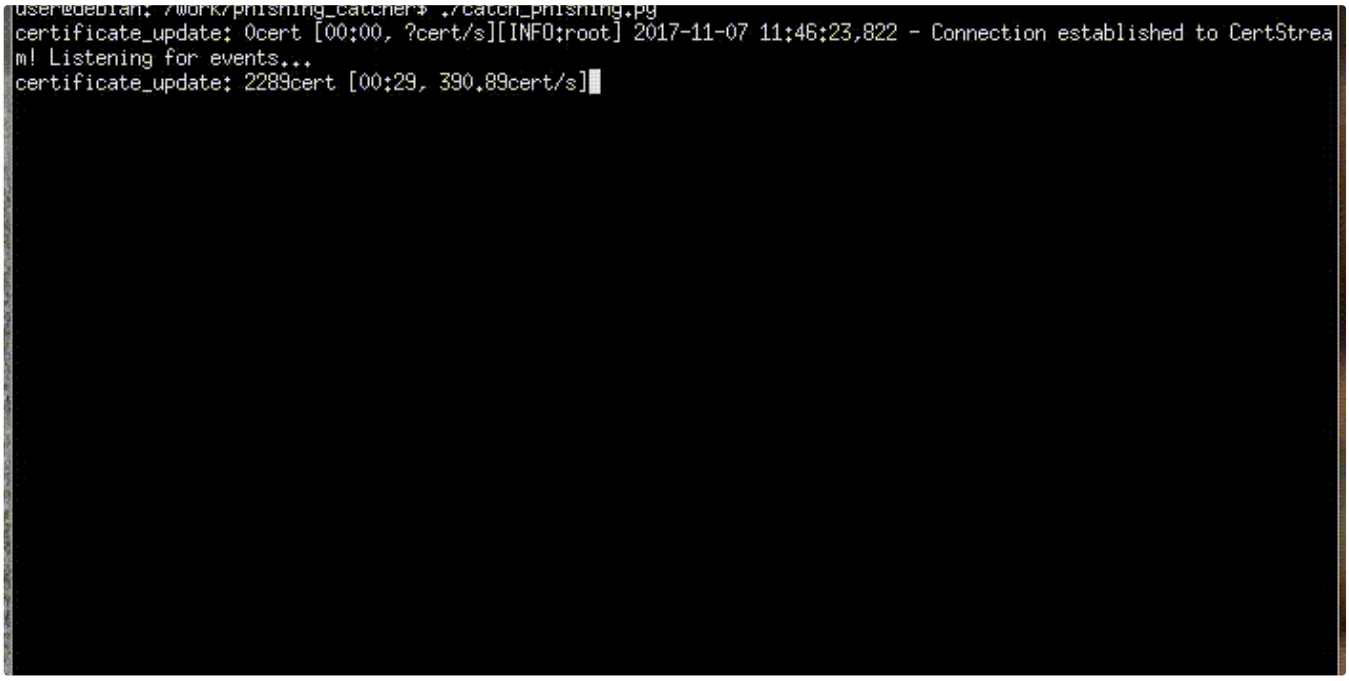
x0rz in Just another infosec blog type of thing

Abusing Gmail to get previously unlisted e-mail addresses

A classic user enumeration attack on Gmail that allowed me to retrieve thousands of e-mail addresses

3 min read · Apr 1, 2017

118 9



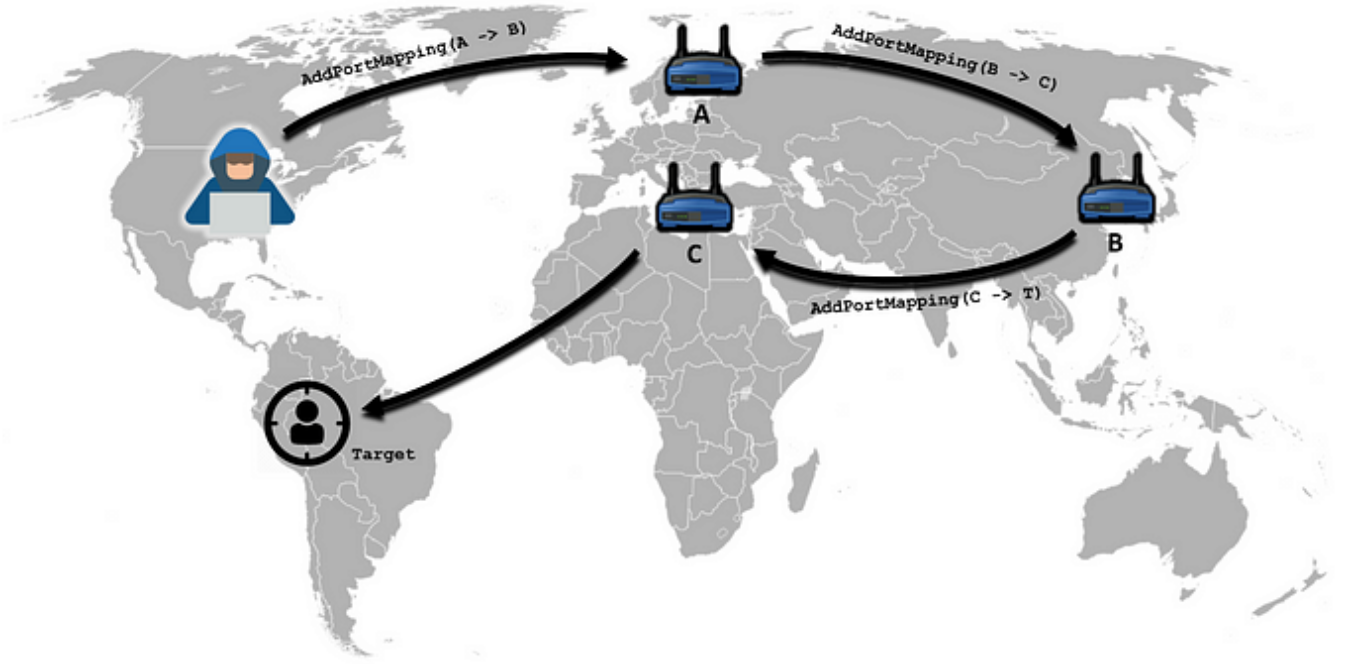
x0rz in Just another infosec blog type of thing

Catching phishing before they catch you

Paypal phishing, paypal phishing everywhere

2 min read · Nov 7, 2017

769 3



x0rz in Just another infosec blog type of thing

Hiding Through a Maze of IoT Devices

How to create the perfect anonymizing botnet by abusing UPnP features—and without any infection

7 min read · Nov 29, 2018

405 1

x0rz in Just another infosec blog type of thing

Starting in cybersecurity?

Here are my few tips on how to get started on the technical side of computer hacking

4 min read · Sep 22, 2017

Abhinav in Stackademic

Building a Telegram Bot and Integrating it with a Golang: A Step-by-Step Guide

Telegram is a popular messaging platform that allows users to create and interact with bots. In this tutorial, we'll walk you through the...

✦ · 4 min read · Aug 5

5

ILLA Cloud

9 Low Code Dashboard Builders for Developers in 2023

By Eric Y

11 min read · Jul 26

1

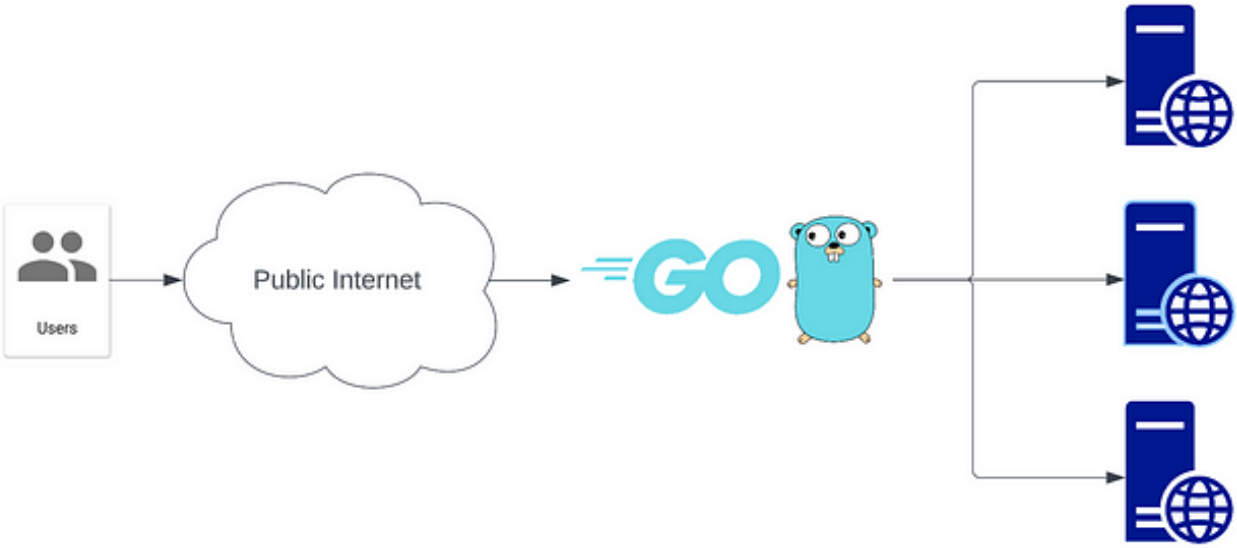
Lists

data science and AI

38 stories · 23 saves

Natural Language Processing

1042 stories · 516 saves



Alex

Dynamic Hostname-Based Reverse Proxy With GoLang

I use Traefik in production scenarios and was curious if I could build something similar in a day. Not the same product, as traefik is...

4 min read · Jul 10

1

Michael Chen

End-to-end example of setting up superset embedded dashboard

Hello, this marks the beginning of my journey in sharing insights on Machine Learning, SRE, and Analytics. I hope someone finds it useful...

8 min read · Aug 30

30 1

Martin Tonev

Writing Code like a Senior Developer in Laravel

Laravel has emerged as one of the prominent PHP frameworks for building elegant applications

4 min read · Dec 22

81 2

Lionel Aimerie

Integrating Chart.js into Elixir Phoenix for visual impact

You want to create an eye-catching chart because you know that in today's data-driven world, the ability to visualize information...

7 min read · Aug 21