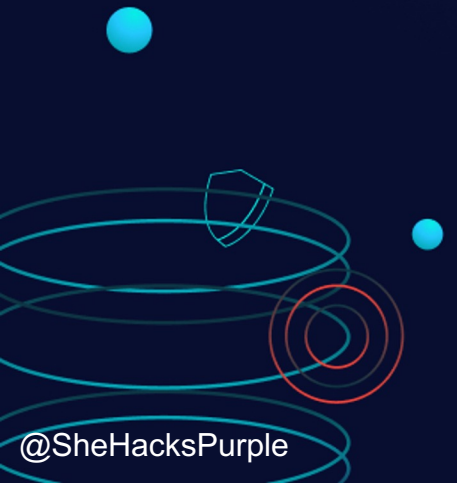
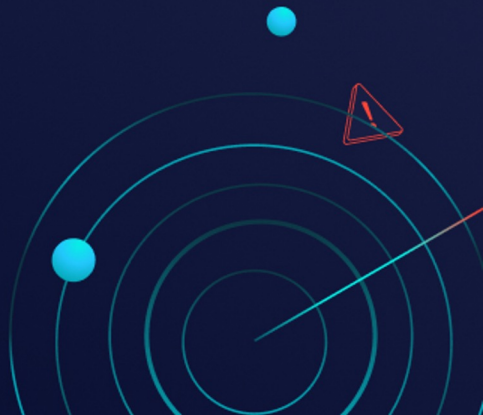
Bright

# Top Ten Security Tips for APIs

Tanya Janca
DevRel @ Bright Security
We Hack Purple





@SheHacksPurple

# What are we going to talk about today?

- APIs rule the web, but they are being attacked
- Top Ten API Security Best Practices
- Resources
- PDF of this talk's 10 tips
- Free Mini Course

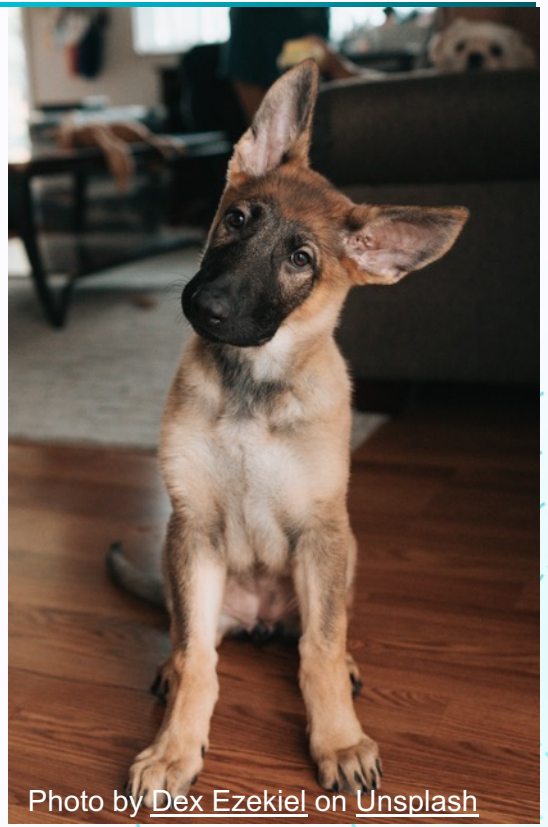


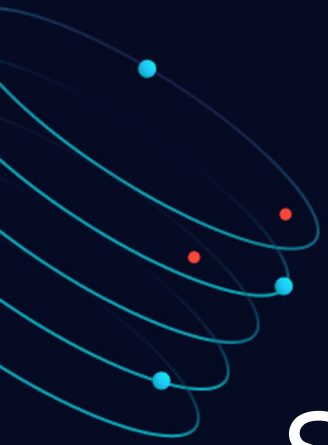
Photo by Dex Ezekiel on Unsplash

# Tanya Janca

About Me

- Director of Developer Relations and Community at Bright Security
- CEO & Founder @ We Hack Purple
- AKA @SheHacksPurple
- Author: **Alice and Bob Learn Application Security**
- Advisor: Nord VPN, Cloud Defense, Aiya
- 25 years in tech, Sec + Dev
- Blogger, Podcaster, Streamer, Builder, Breaker
- Giant Nerd

# Let’s do this!

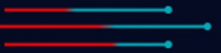


So… I lied.

There aren’t ten.

I’m going to give you way more than just ten.

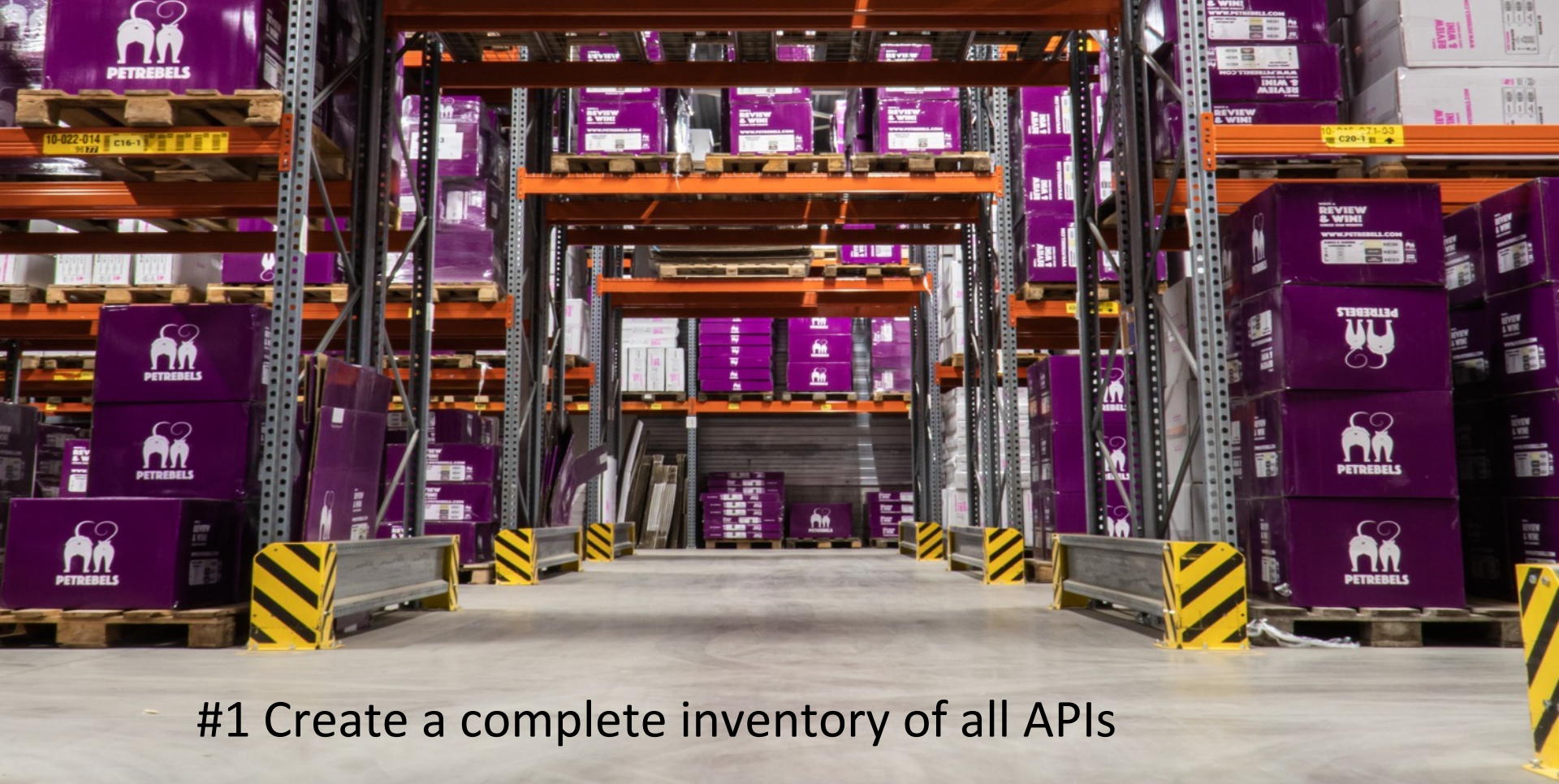
Sorry/not sorry.



# The Problem

APIs still need just as much security attention as web applications; not having a front end does not make them invisible to attackers.

Web apps are the #1 cause of data breach, and most web apps are now just a bunch of APIs with a GUI in front.




# #1 Create a complete inventory of all APIs

Photo by Petrebels on Unsplash

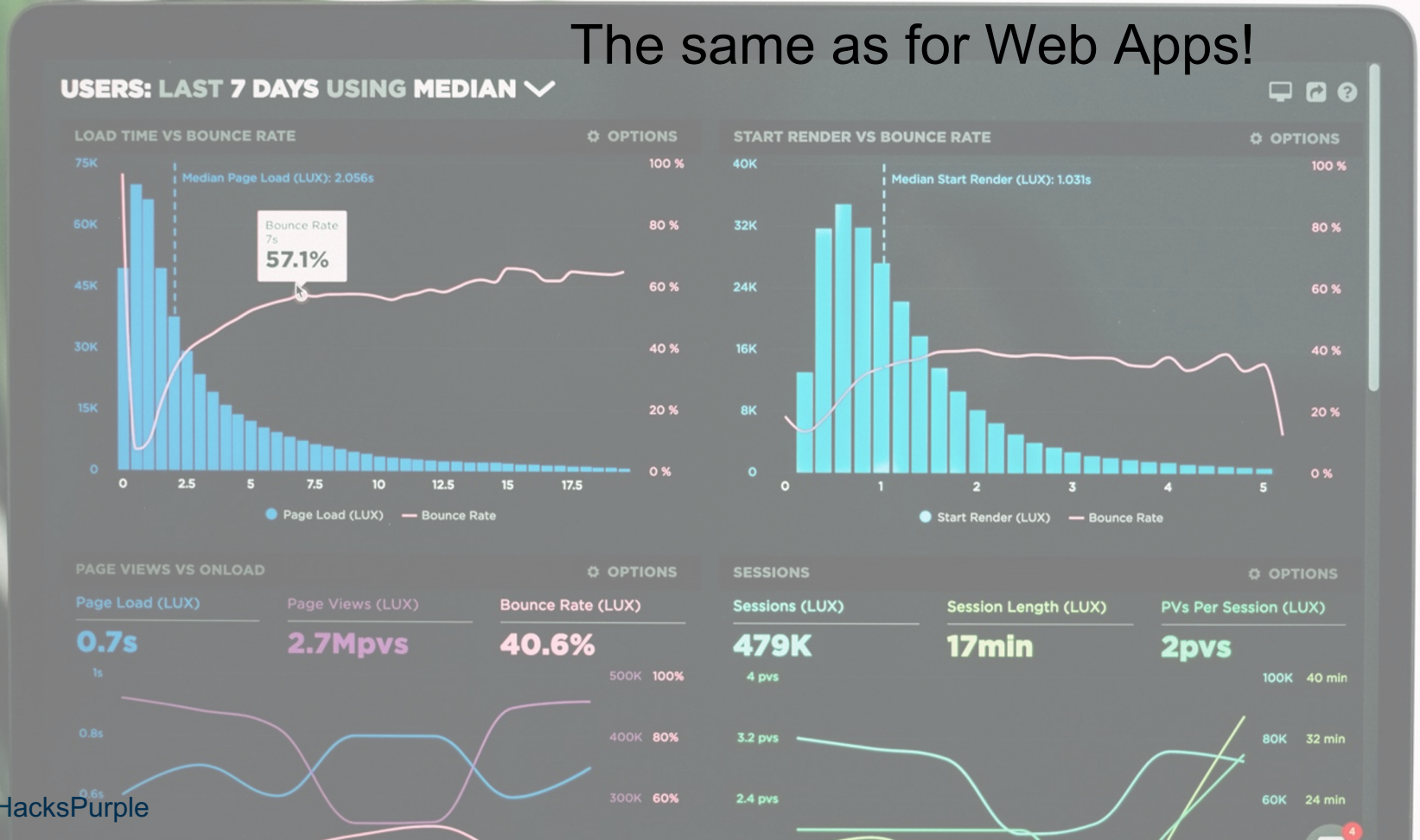
# #2 All external APIs are connected to via an API gateway

# Throttling and Resource Quotas

Photo by Donald Giannatti on Unsplash

# Logging, monitoring and alerting

The same as for Web Apps!



# Block all unused HTTP methods/verbs

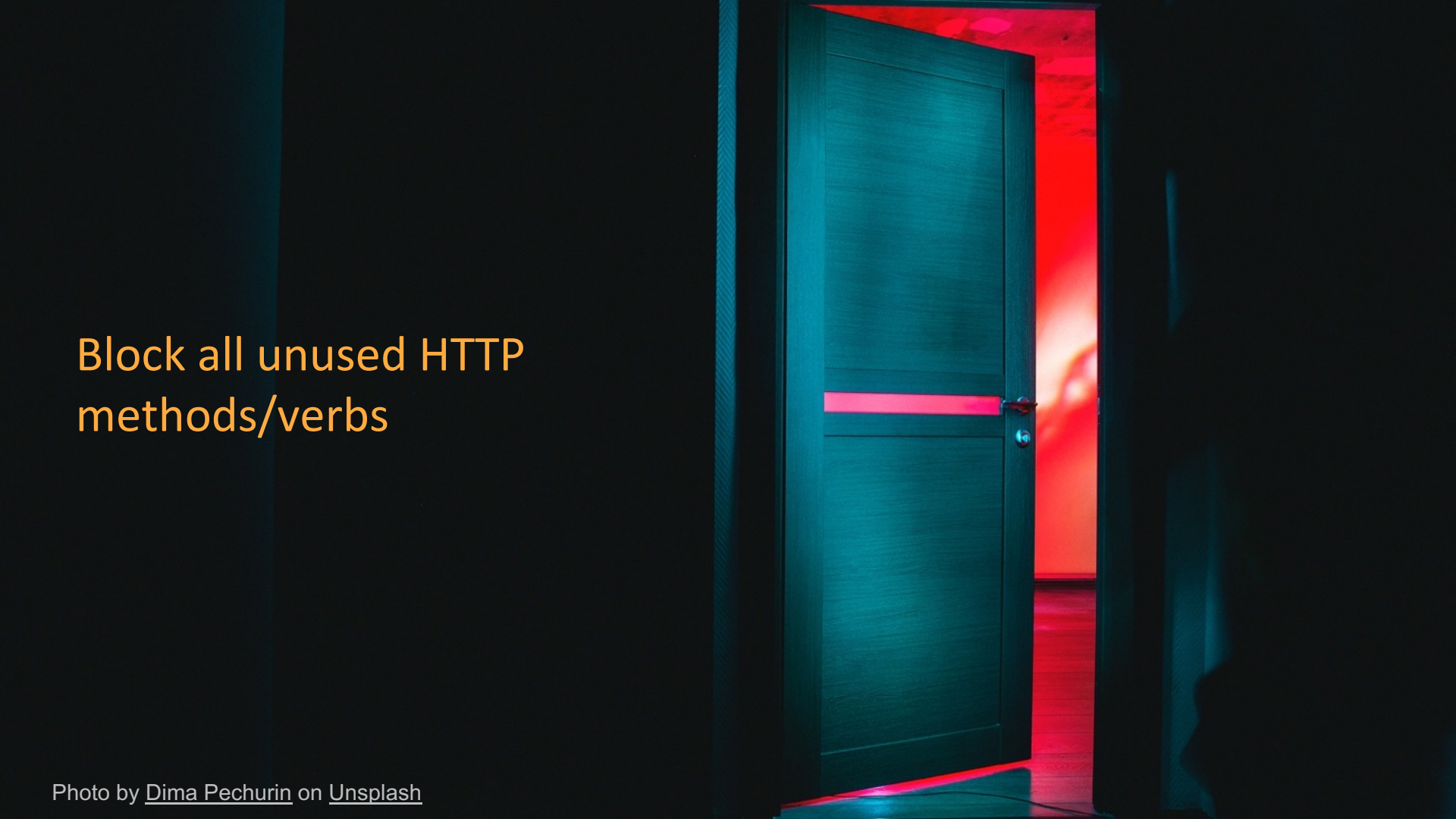


Photo by Dima Pechurin on Unsplash


Use a service mesh for communication management


Enforce Them.

# Strict Linting

Photo by Wes Hicks on Unsplash


# Avoid verbose error messages

Photo by Markus Spiske on Unsplash


Decommission old or
unused versions of APIs.

All the same secure coding practices you normally do; input validation using approved lists, parameterized queries, bounds checking, etc.

# What did we learn today?

APIs need just as much attention as web apps!

Best practices are doable!

Secure SDLCs produce secure software

# Resources

newsletter.
wehackpurple.com/
api-security

# Free PDF of This Talk!

newsletter.wehackpurple.com/api-security

# Free API Security Mini Course!

https://community.wehackpurple.com/

Go to ‘courses’ on the left!

# THANK YOU

Tanya Janca
DevRel @ Bright
We Hack Purple