

Top Ten Security Tips for APIs

Tanya Janca
DevRel @ Bright Security
We Hack Purple

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

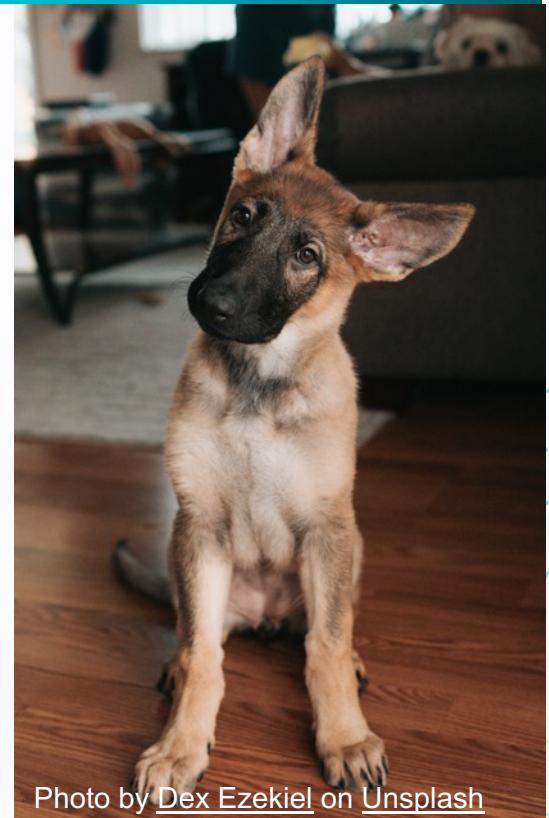


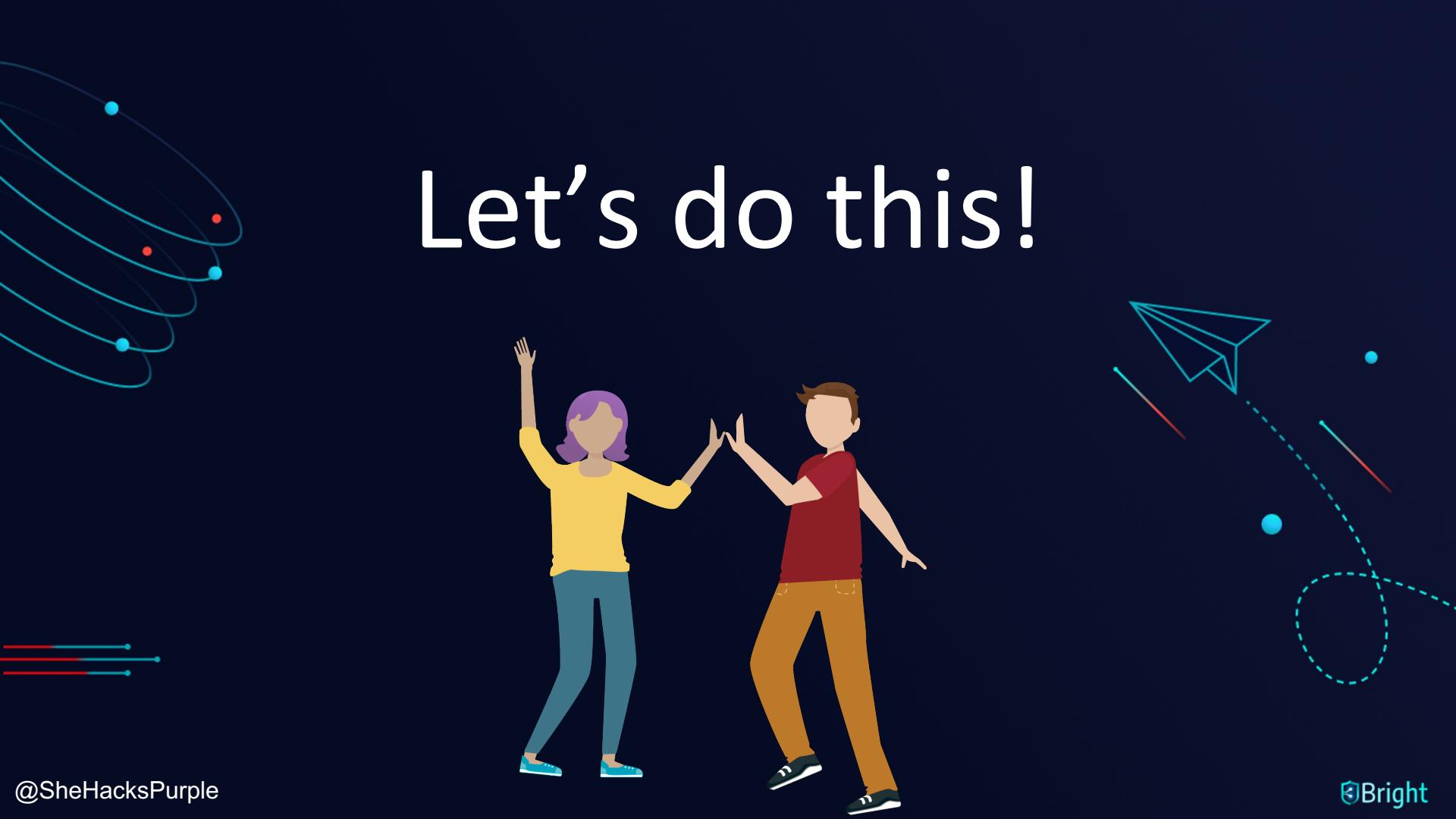
Photo by [Dex Ezekiel](#) on Unsplash

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.

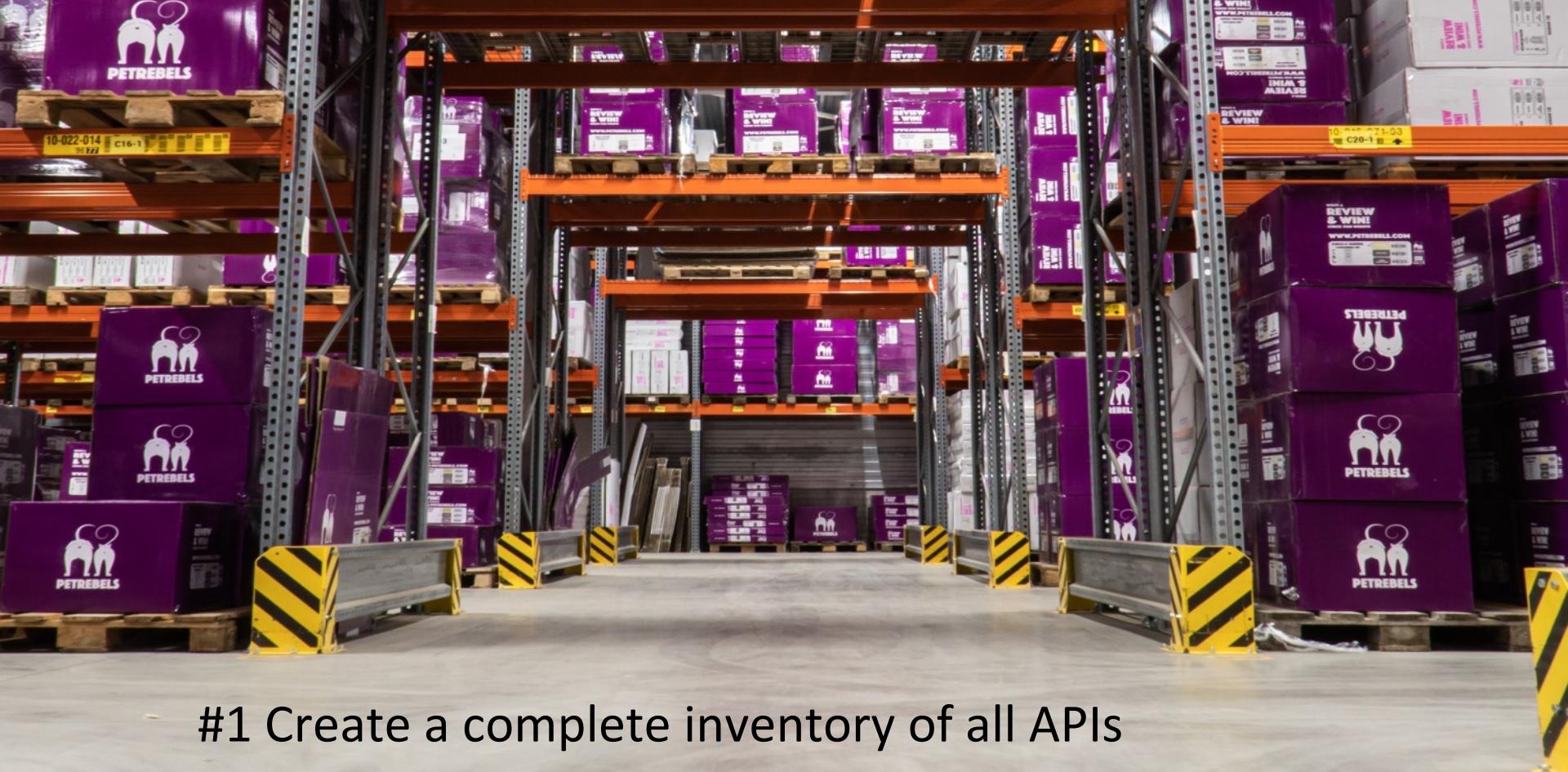
Sorry/not sorry.

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



Photo by [Laila Gebhard](#) on [Unsplash](#)

A close-up photograph of a motorcycle's handlebar. The handlebar is black with a textured grip. A chrome throttle grip is attached to the end of the bar. A small red plastic switch or indicator is mounted on the handlebar just above the grip. In the background, the blurred landscape of a field and trees is visible under a cloudy sky.

Throttling and Resource Quotas

Photo by [Donald Giannatti](#) on [Unsplash](#)

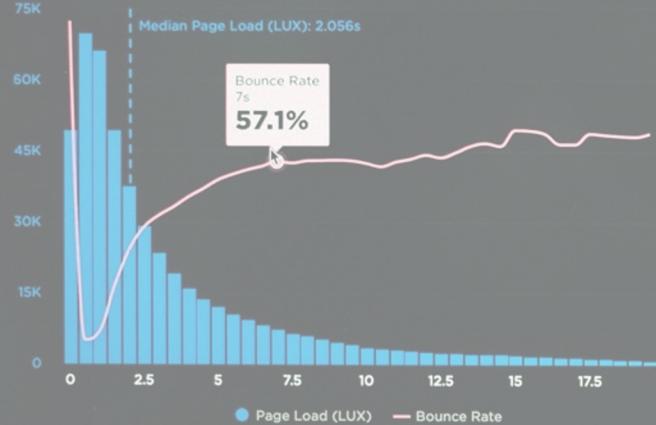
Logging, monitoring and alerting

The same as for Web Apps!

USERS: LAST 7 DAYS USING MEDIAN ▾



LOAD TIME VS BOUNCE RATE



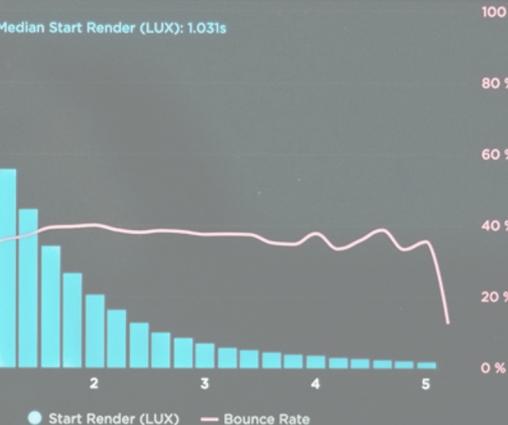
OPTIONS

100 %

START RENDER VS BOUNCE RATE

100 %

Median Start Render (LUX): 1.031s



OPTIONS

100 %

PAGE VIEWS VS ONLOAD

Page Load (LUX)

0.7s

Page Views (LUX)

2.7Mpv/s

Bounce Rate (LUX)

40.6%

OPTIONS

500K 100%

400K 80%

300K 60%

SESSIONS

Sessions (LUX)

479K

4 pvs

Session Length (LUX)

17min

2.4 pvs

OPTIONS

PVs Per Session (LUX)

2pvs

100K 40 min

80K 32 min

60K 24 min

Block all unused HTTP
methods/verbs



Use a service mesh for communication management



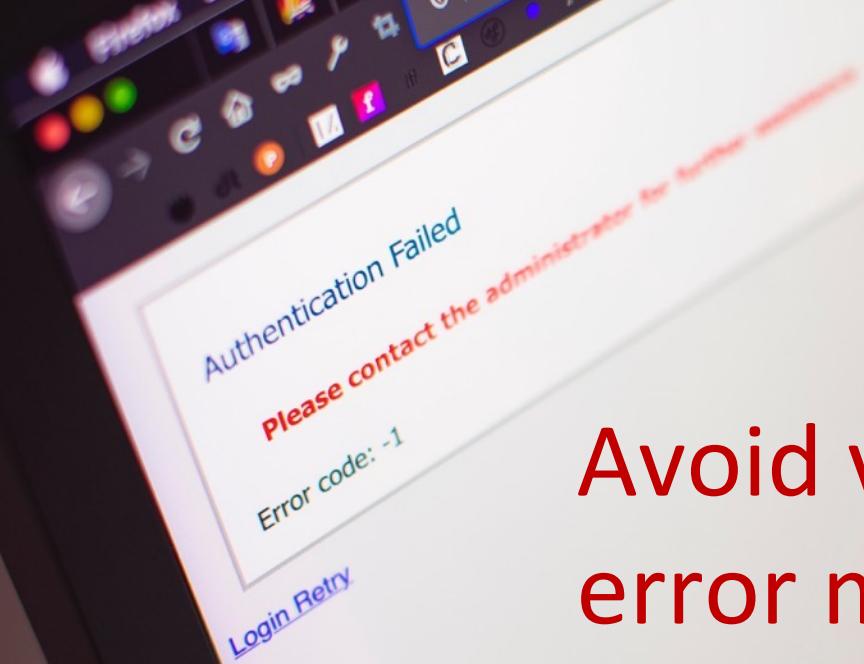
Implement
standards
for your org

Enforce Them.

Strict Linting

A close-up photograph of a fluffy orange tabby cat sleeping peacefully on a soft, white, textured surface, likely a bed or sofa. The cat's head is turned slightly to the right, eyes closed. In the background, there is a large window with a dark frame, through which some greenery and light are visible, creating a warm, cozy atmosphere.

Avoid verbose error messages



A close-up photograph of a weathered wooden door made of vertical planks. A metal strap with rivets runs horizontally across the middle. On the left side, there's a circular metal lock mechanism. A thick metal chain is attached to the top of the strap and hangs down, secured with several padlocks. One padlock is clearly visible, engraved with the word "Master".

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!

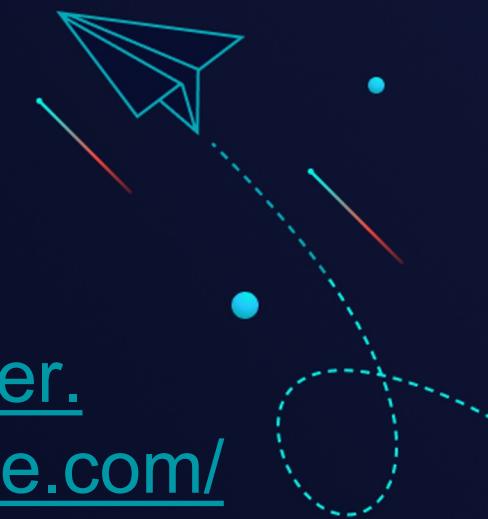
Secure SDLCs
produce secure
software





Resources

[newsletter.](#)
[wehackpurple.com/
api-security](http://wehackpurple.com/api-security)



Free PDF of This Talk!

newsletter.

wehackpurple.com/

api-security

Free API Security Mini Course!

[https://community.
wehackpurple.com/](https://community.wehackpurple.com/)

Go to 'courses' on the left!



THANK YOU

Tanya Janca
DevRel @ Bright
We Hack Purple

