What I wish I knew about security when I started programming

Allon Mureinik
Senior Manager, Seeker Interactive Application Security Testing (IAST)
Synopsys, Inc.
allon.mureinik@synopsys.com / @mureinik / https://www.linkedin.com/in/mureinik/
FOSDEM 2022
My Goodness, Why Didn't I Think of That?

https://knowyourmeme.com/memes/my-goodness-why-didnt-i-think-of-that
But I have a firewall/WAF/RASP/other cool tech…

https://www.princessbrideforever.com/
It’s a matter of perception

https://www.dreamworks.com/movies/megamind
It’s a matter of perception (cont.)

https://www.hbo.com/game-of-thrones
Shifting left

https://www.thefastsaga.com/
A balancing act

https://www.marvel.com/movies/avengers-infinity-war
Perfection?

https://www.20thcenturystudios.com/movies/x-men-first-class
Reality check

https://thenounproject.com/term/check/1635221
Who really uses the system?

How will a reasonable person use it?

How will an unreasonable person abuse it?

https://thenounproject.com/term/theater/17128
Don’t reinvent the wheel

https://thenounproject.com/icon/wheel-118280/
Security through obscurity (alone) doesn’t work

https://thenounproject.com/icon/maze-316908/
Your code is just the tip of the iceberg

https://thenounproject.com/icon/iceberg-2258187/
Don’t trust your input

https://thenounproject.com/term/trust/2714631
You’re responsible for your user’s safety

https://thenounproject.com/icon/insurance-1635533/
Boring is good

https://thenounproject.com/term/yawn/3971467
Can we tool it away?

https://thenounproject.com/term/tools/943586
Harness the community

https://thenounproject.com/icon/community-3860455/
Takeaways

https://thenounproject.com/term/takeout/38140
Questions?

https://thenounproject.com/term/questions/1195076/
Thank You

Contact
allon.mureinik@synopsys.com
@mureinik
https://www.linkedin.com/in/mureinik/