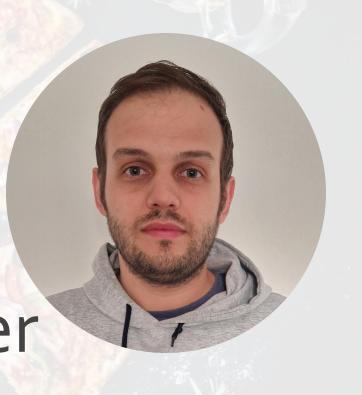
Spring Security basics

Sprinkle of Security (and Spring)

A passionate and enthusiastic web software developer



Help wanted and greatly appreciated



Our software is safe... as long as nobody breaks it

Even if people like Andres Freund exist

https://www.youtube.com/watch?v=FpT_cYUaxkU

https://xkcd.com/2347/

Where to start? Meet our new friend OWASP

https://www.owasp.org

Where to continue? Meet our new friends Let's Encrypt, Snyk, SecurityHeaders

Spring Boot

- Opinionated version of the Spring Framework
- The web support has an integrated web server
- Easily configurable and well documented
- Let's see a basic *unsecured* web application

Spring Security

- Exploit prevention
- Integrates with the Servlet API
- Authentication & authorization
- Let's see how our app changes by adding it

Sh*t happens...

XSS Cross-site scripting

Sh*t happens...

CSRF Cross-site request forgery

The keywork is authentication

The keywork is authorization

OAuth₂

- An open standard protocol for authorization
- Typical "Sign up with Google" button
- OpenID Connect extends it for authentication
- Let's see how we can work with it

JWT JSON Web Token

- A web standard
- Supports many signature algorithms
- Some claims are registered (sub, iss, exp, ...), some are not
- DO NOT PUT SENSITIVE INFORMATION IN IT

That's a lot! Key takeaway: think about security

Thank you!



lb.luca.bonetti@gmail.com



https://github.com/LBLucaBonetti/Spring-Security-basics



https://linkedin.com/in/lb-luca-bonetti