JANINE VAN SAAZE

SECURITY RESEARCH

SEMESTER 3

Table of contents

Chapter 1: Introduction

When thinking about a good subject to do a security research about, the first thing that came to mind was a research about JWT tokens, although interesting I already had a lot of classmates around me do that research. Instead of doing the same research but with a new coat of paint, I decided to do something different.

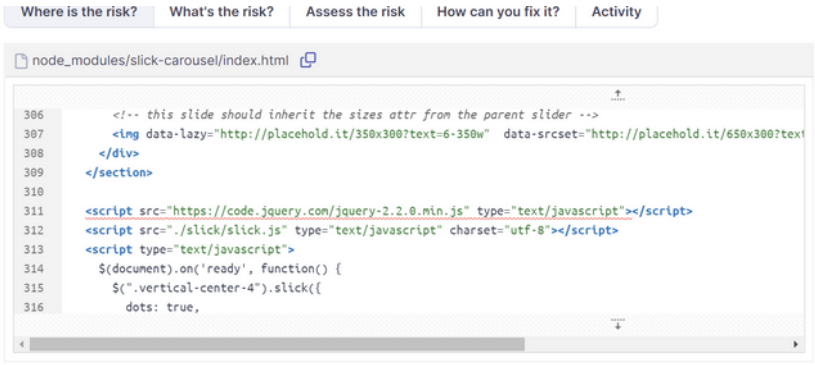
When I checked my code on code quality, it came back with a few security vulnerabilities. My research will be about:

"Which security vulnerabilities my project has and how I can protect them against breaches"

Chapter 2:
Which security vulnerabilities does my project have

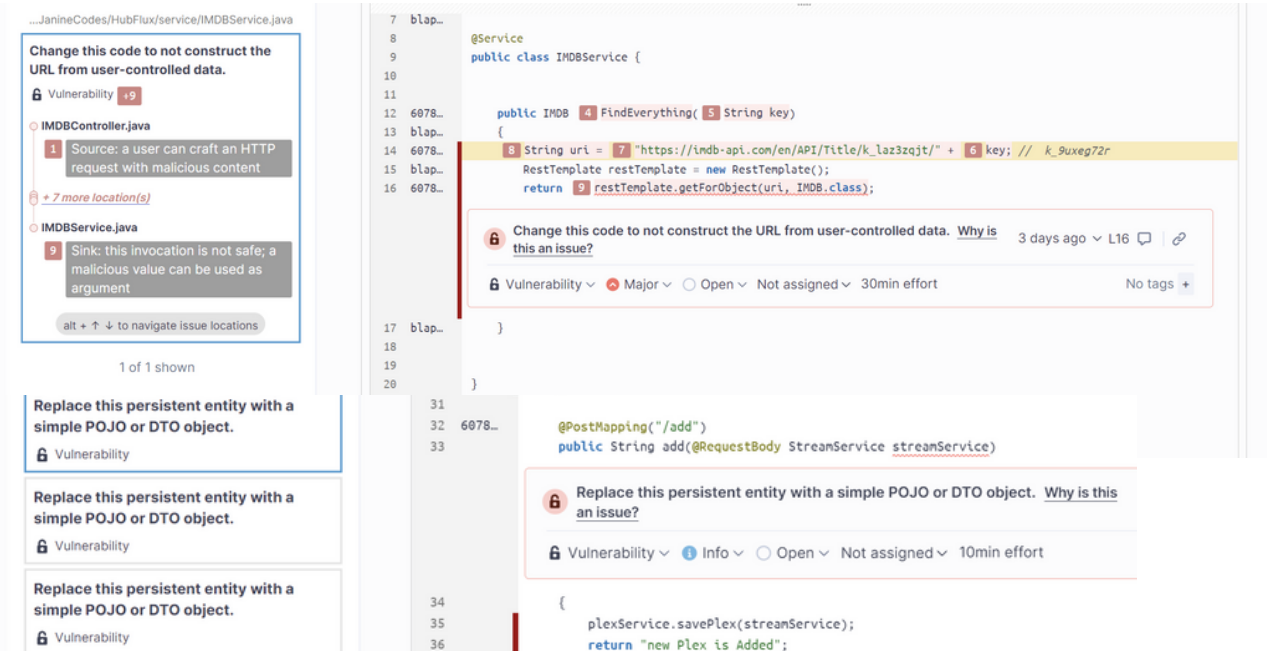
My project has a seperate front- en backend, they both have different security vulnerabilities.

Frontend
When looking at the front-end you will see that I have one security hotspot, the error says "Make sure not using resource integrity feature is safe here"



Backend

In the backend I have a security issue that shows my API key, and that I should replace the entity with a DTO object



And also the hardcoded database login

```
spring.jpa.hibernate.ddl-auto=update
spring.datasource.url=jdbc:mysql://hubfluxdb.mysql.database.azure.com:3306/plex
spring.datasource.username=hubflux
spring.datasource.password=5R24!O1uY!cJ
spring.jpa.properties.hibernate.enable_lazy_load_no_trans=true
spring.datasource.driver-class-name=com.mysql.cj.jdbc.Driver
server.port = 8090
```

Chapter 3:
Why are these security vulnerabilities?

Frontend

SonarCloud says I should a "integrity" inside my script code, but what even is that and why is this an issue?

On W3Schools it says "The integrity attribute allows a browser to check the fetched script to ensure that the code is never loaded if the source has been manipulated." *(HTML script integrity Attribute, z.d.)*

So to put it simply it basically checks the scripts before it actually loads to sure there are no vunerabilities inside it.

Backend

For my backend it says I need to add a DTO object, but what even is a DTO object?

DTO object stands for a Data Transfer Object, so it encapsulates data and sends it from one to another.

When using a DTO you can slit specifically which data you want to send where, or even make two different classes with data come together before sending it.

(What is a Data Transfer Object (DTO)?, 2009)

I don't think I really need to explain why hardcoding your database login data is a bad practice. But just in case, when saving sensitive data and pushing your project online, everyone can easily find that data and even change it.

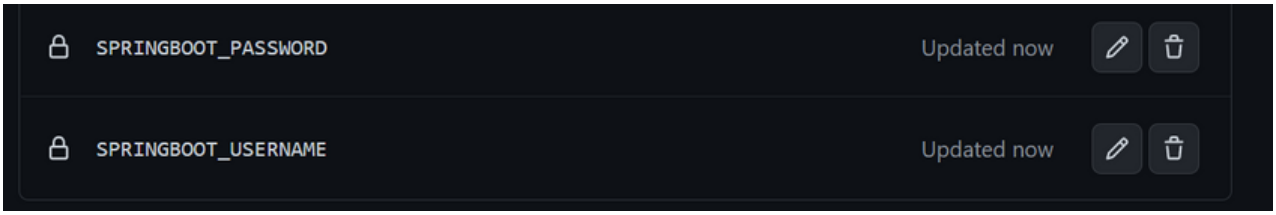
Chapter 4:
How can I protect them against breaches?

Backend

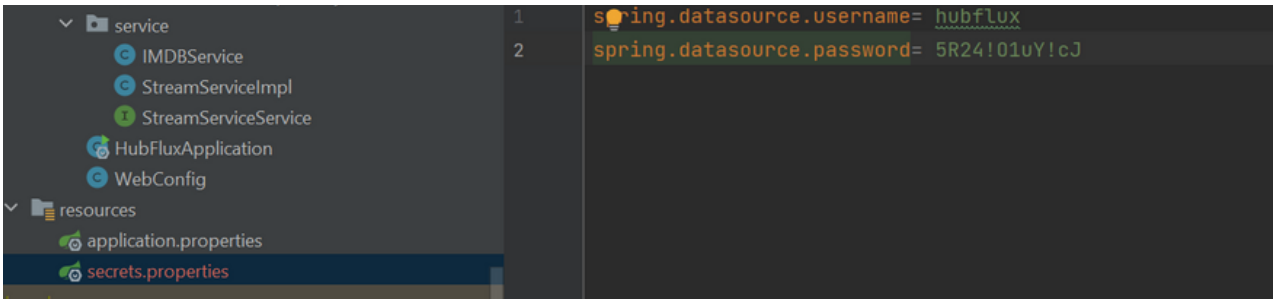
Although you could argue that using a DTO is more SOLID, it does depend on the use case. In my case I won't do that, when looking at this forum post you will find this "What is somewhat outdated is the notion of having DTOs that contain no logic at all...In simple applications, the domain objects can often be directly reused as DTOs and passed through directly to the display layer" (What is the point of using DTO *(What is a Data Transfer Object (DTO)?, 2009)*

And I think this is true for my case, my whole page already is a DTO, it has zero logic and is only used as a transfer bucket. So for my project I will not add a DTO.

For the hardcoded login data, I made two github secrets.



In my project I made a new properties file that contains the username and password, this only gets used when running my project locally and WON'T be pushed to github



After pushing my project it will build my docker container with the username and password added from the github secrets

```
with:
  username: ${{ secrets.DOCKER_HUB_USERNAME }}
  password:  ${{ secrets.DOCKER_HUB_PASSWORD }}
  repository: plunku/hubflux
  tags: latest
  environment:
    spring.datasource.username= ${{ secrets.SPRINGBOOT_USERNAME }}
    spring.datasource.password= ${{ secrets.SPRINGBOOT_PASSWORD }}
```

In reality this doesn't really work because Docker finds it hard to add envionment variables. But this would be a way to make it more secure.

Chapter 5:
Conclusion

When researching for vulnerabilities I found a lot of usefull things like a DTO and how much the community is split between if you should use it yes or no.

For my project I decided not to make a seperate DTO because one of my classes basically already is a DTO because it contains zero logic

My frontend didn't contain many security risks, that is because he will only send and receive data to the backend that has most of the security vulnerabilities

Sadly I didn't get the database security fixed, but the idea would still be the same if you would do it for a different project.

Literature list

HTML script integrity Attribute. (z.d.).
https://www.w3schools.com/tags/att_script_integrity.asp

What is a Data Transfer Object (DTO)? (2009, 26 juni). Stack Overflow.
https://stackoverflow.com/questions/1051182/what-is-a-data-transfer-object-dto

What is the point of using DTO (Data Transfer Objects)? (2012, 26 oktober). Software Engineering Stack Exchange.
https://softwareengineering.stackexchange.com/questions/171457/what-is-the-point-of-using-dto-data-transfer-objects