



# Secure Coding Training & Awareness

Bjørnar Liberg | Security Engineer

DNB | Group Security | Security Knowledge & Advisory



# Why is training in secure coding important?



Increased pressure to deliver faster to stay competitive



Deploying 1-2 times a year vs multiple times in a week

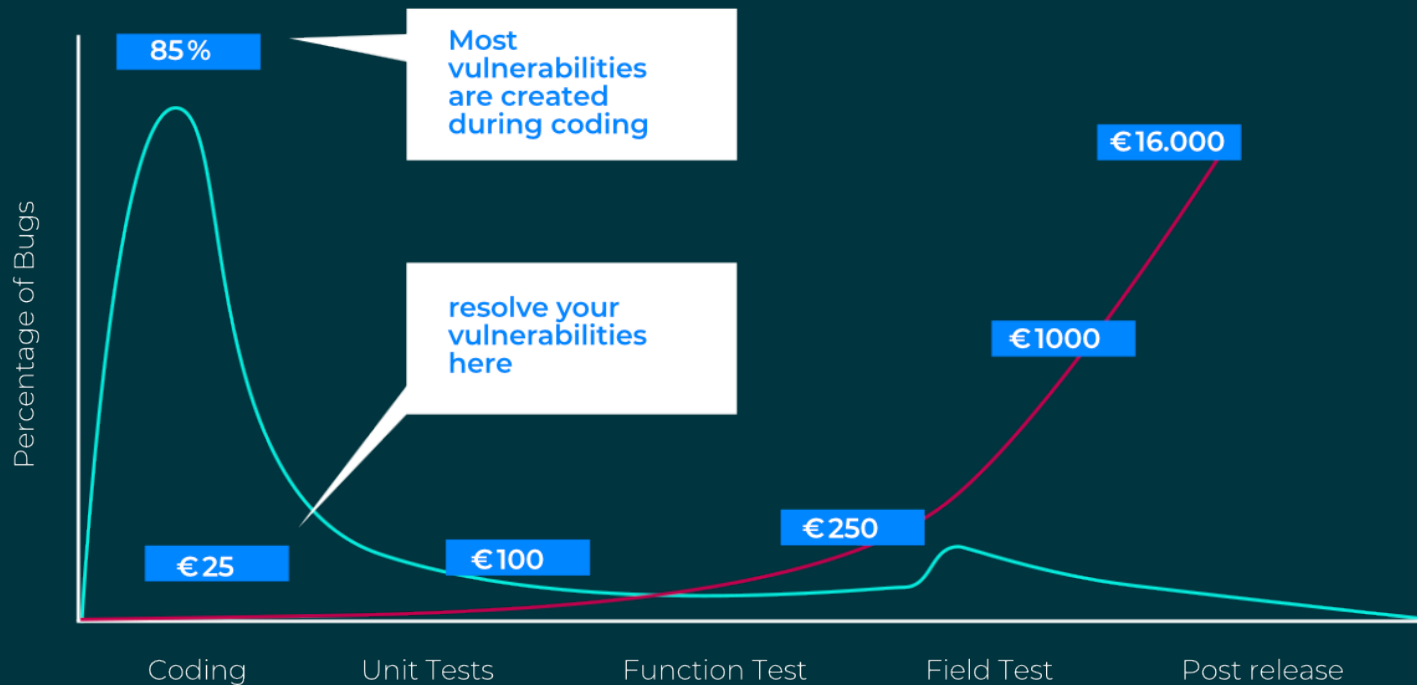


No time for comprehensive reviews that halt deployment



Security responsibility is shifting towards the developers themselves

# The cost of insecure code



■ Cost of repairing at this dev Phase    ■ Defects introduced at this dev Phase

# DNB's Training Program for Secure Coding

Promotional material

Tournaments



Bootcamps



Training material

Certification Program



Fundamental  
Learning Path

Advanced  
Learning Path

«Vulnerability of the Month» Courses



Self-Service Training



100/100

Licensed users

~250 hours

Used in the platform  
in Q2

~80%

became more confident in their ability  
to identify and fix vulnerabilities

5.6/6

Average rating of  
bootcamps

5.4/6

Average rating of  
tournaments

5.1/6

Average rating of  
certification program

*«Thanks for hosting.  
Very fun way to learn.»*

*«Awesome initiative!»*

*«Thank you for this! I am  
looking forward to  
practice with the tool»*

*«I participated in the last tournament  
and very much interested to improve  
my secure coding skills.»*

*«I very much appreciate the  
opportunities to attend the  
workshops like this, learning from  
security experts. I'm a developer and  
security is not my expertise, but I'm  
very interested to learn more.»*

*«Really enjoyed it and looking  
forward to the next one, great job!»*

*«Eye opening how much i have to learn!  
Look forward to further levels. One  
more point is that the platform is  
excellent in providing you knowledge  
and letting you see and test "real" world  
examples»*

# DNB's Training Program for Secure Coding

Promotional material

Tournaments



Bootcamps



Training material

Certification Program



Fundamental  
Learning Path

Advanced  
Learning Path

«Vulnerability of the Month» Courses



Self-Service Training



# Most important lessons learned



It needs to be relevant



It needs to be communicated



It needs to be interactive



# Relevance

- *What the developers learn needs to be directly applicable to their day-to-day work.*

## Why

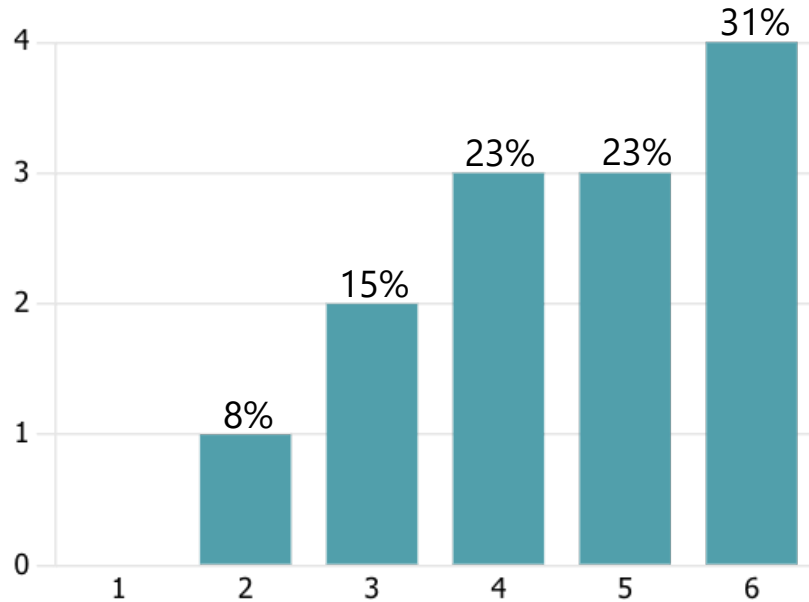
- Different programming languages and frameworks have different vulnerabilities that are more prevalent, and different ways of fixing them.

## What to do

- Start from industry best practice (such as OWASP Top 10)
- Tailor to your specific company
  - Ask your developers!
  - Use statistics from your SAST/vulnerability scanning tools. Are there any specific vulnerabilities that occur more often?
  - Triage and prioritize - you will not be able to create something that perfectly suits everyone.

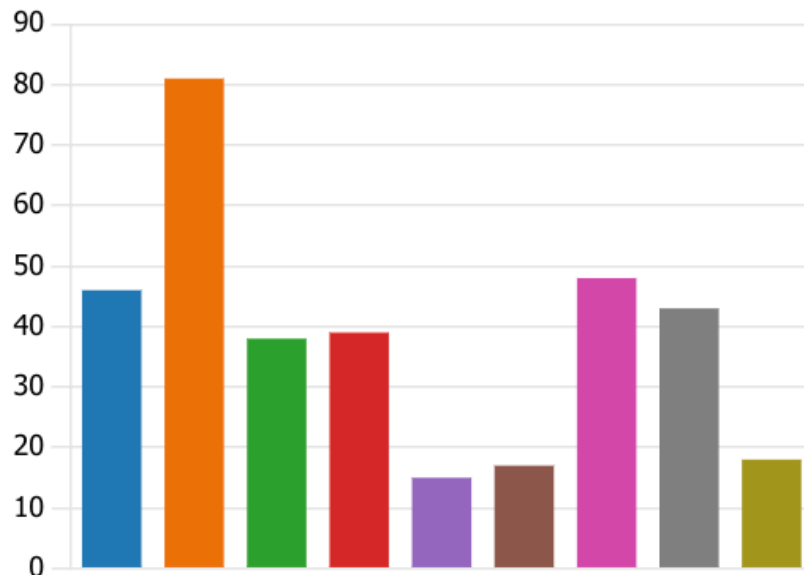
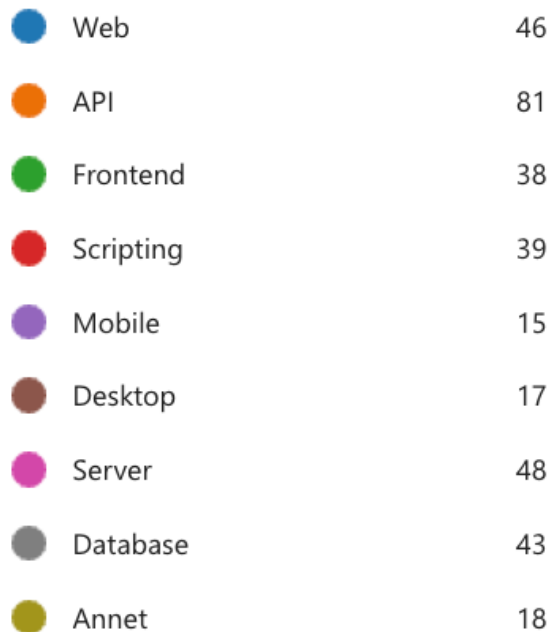


# "How would you rate the relevance of the challenges to your day-to-day work?"



- "A lot of exercises are focused on a web application (frontend). For people that work with just the backend (for example, development of APIs), some exercises are not so relevant. If possible somehow, it would be good to have the possibility to choose, for example, Java Spring (backend)."
- "Great platform especially those developing modern web apps / apis etc. Appears to not offer that much to people working on legacy applications eg WinForms desktop apps. However, for up skilling people very good»"
- "It would be great if we can include Typescript and javascript in the future"
- "Add Node.js :)"

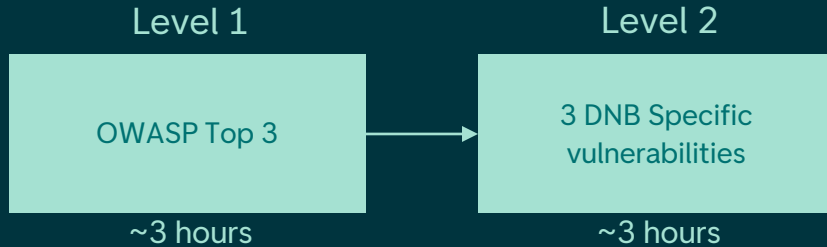
# What kind of development work do you do?



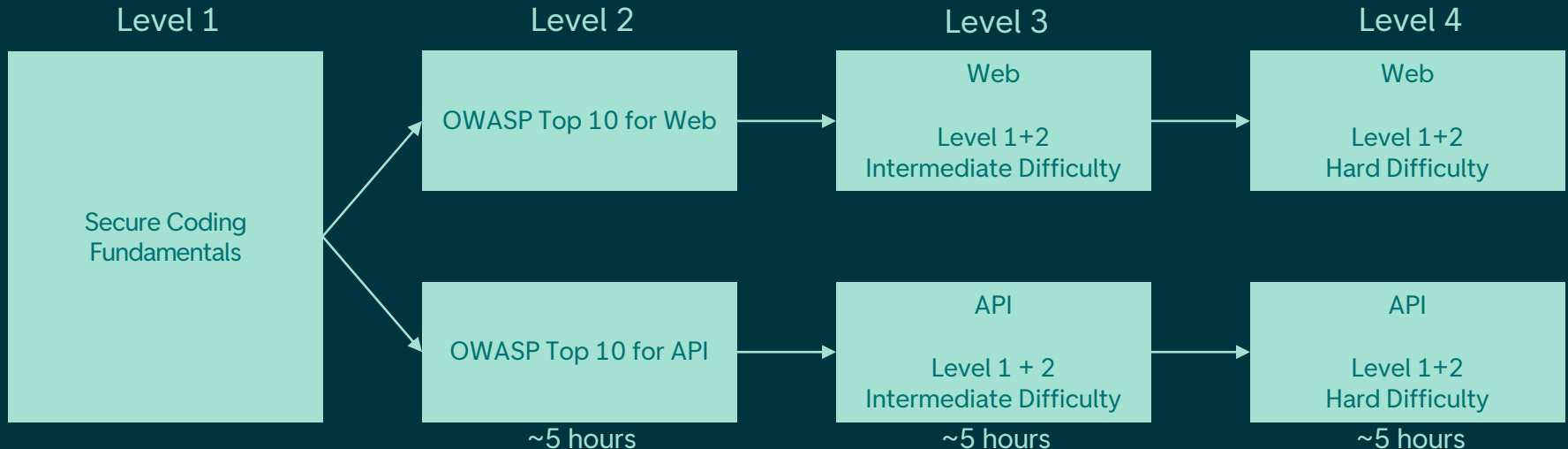
Progression: 1 level per quarter

Enrollment: Once per Quarter

## Secure Coding Fundamentals



## Secure Coding Advanced



# Communication

- *When was the last time you opened LinkedIn Learning? Was it because someone asked you to?*

## Why

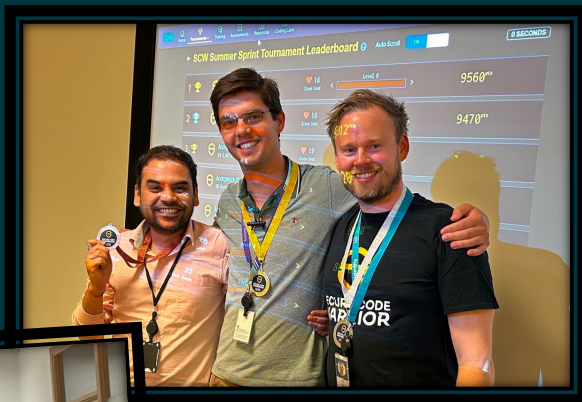
- Developers will not check for new material unless they are told to

## What to do

- Create a community for discussions and announcements
- Hold regular events to create FOMO
  - E.g. Tournaments, CTFs, «Lunch and learn», Workshops or Bootcamps
  - Reward (/bribe) participants with snacks, swag, or similar
- Try to get support from key personell to help spread the word (e.g. Security Champions, CISO, Managers)



# Tournaments



# Interactivity

- *Coding is as much in the hands as it is in the brain.*

## Why



- Interactive training is both more engaging and more effective than traditional «classroom» setups

## What to do

- Open Source lab/application (e.g. OWASP Juice Shop)
  - Pros: Easy to get started, good variety of challenges, cheap
  - Cons: Less focus on reading and writing code, more on exploiting
- Custom lab/application
  - Pros: Tailored to your business
  - Cons: Requires alot of time and expertise to set up
- Vendor-created learning platform
  - Pros: Support for multiple languages, fast to create new material
  - Cons: Cost




## STEPS


 Use raw parameterized queries Use Django's ORM filter

Great job! As we know, Django has an ORM (Object Relational Mapper) that automatically gives us a database abstraction API to interact with the database through its objects. Django's ORM queries are protected from SQL injection, as they are built using query parameterization. The SQL code of a query is defined separately from the query parameters. The input parameters are escaped by the database driver in the background.


## Task 1

All right, let's write the transaction query for the `get_context_data` method using Django's ORM filter. In the `if` statement:

- Replace the method call `self.get_owner_account_transactions(account, search_term)` with the `Transaction.objects` manager;
- Next,  **filter** the transactions. In SQL terms, a filter is a limiting clause such as `WHERE` or `LIMIT`.
  - Filter out all the transactions belonging to the account owner;
  - And, from those transactions, filter out the ones where the description contains the search term.

 Show step solution

Submit

 Changed number of methods views.py

Please don't add or remove methods. Change the

EXPLORER

PROJECT

&gt; accounts

&gt; assignment/accounts

views.py M

&gt; transactions

&gt; users

\_\_init\_\_.py

asgi.py

manage.py

settings.py

urls.py

wsgi.py

&gt; OUTLINE

&gt; TIMELINE

views.py M X

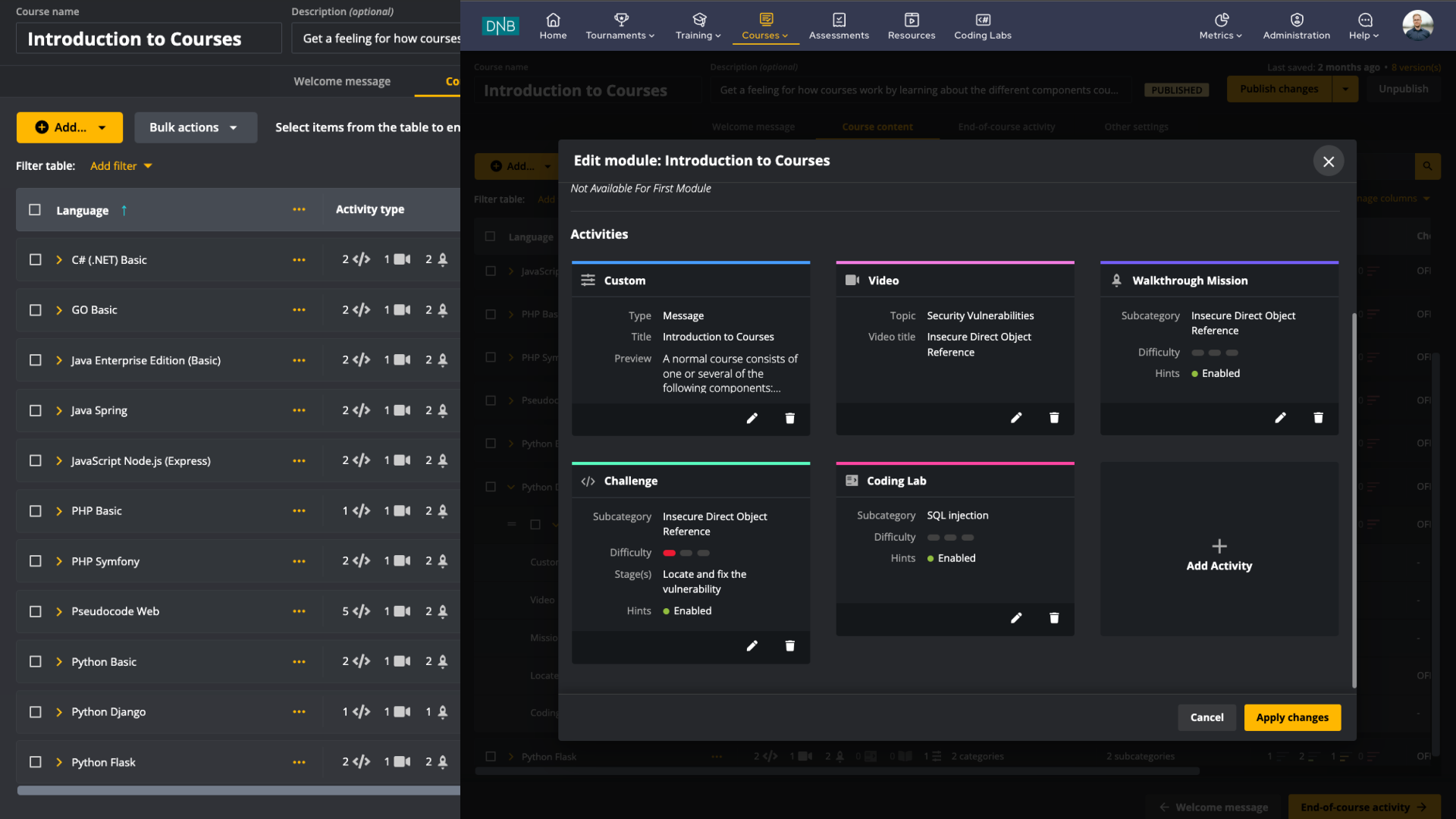
assignment &gt; accounts &gt; views.py &gt; AccountTemplateView &gt; get\_context\_data

```

1  from django.views.generic import TemplateView
2  from django.contrib.auth.mixins import LoginRequiredMixin
3  from django.shortcuts import get_object_or_404
4
5  from accounts.models import Account
6  from accounts.forms import SearchForm
7  from transactions.models import Transaction
8
9
10 class AccountTemplateView(LoginRequiredMixin, TemplateView):
11
12     template_name = 'account_detail.html'
13
14     def get_owner_account_transactions(self, account, search_term):
15         contains_search_term = f"%{search_term}%"
16         query = (
17             "SELECT id, timestamp, owner_account_id, foreign_account_id, "
18             "description, amount FROM transactions_transaction T "
19             "WHERE T.owner_account_id = %s "
20             "AND T.description LIKE %s"
21         )
22         return Transaction.objects.raw(query, (account.id, contains_search_term))
23
24     def get_context_data(self, **kwargs):
25         context = super().get_context_data(**kwargs)
26
27         account = get_object_or_404(Account, pk=self.kwargs.get('pk'))
28         context['form'] = SearchForm()
29         context['account'] = account
30         context['transactions'] = account.owner_account_set.all()
31
32         search_term = self.request.GET.get('searchterm')
33         if search_term and not search_term.isspace():
34             context['transactions'] = self.get_owner_account_transactions(
35                 account, search_term)
36
37         return context

```





# Introduction to Courses

Get a feeling for how courses

Welcome message

Introduction to Courses Get a feeling for how courses work by learning about the different components cou... PUBLISHED Publish changes Unpublish

+ Add... Bulk actions Select items from the table to en

Filter table: Add filter

| <input type="checkbox"/> Language ↑                        | ... | Activity type |
|--|-----|---------------|
| <input type="checkbox"/> > C# (.NET) Basic                 | ... | 2 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > GO Basic                        | ... | 2 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > Java Enterprise Edition (Basic) | ... | 2 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > Java Spring                     | ... | 2 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > JavaScript Node.js (Express)    | ... | 2 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > PHP Basic                       | ... | 1 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > PHP Symfony                     | ... | 2 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > Pseudocode Web                  | ... | 5 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > Python Basic                    | ... | 2 </> 1 🎥 2 👤 |
| <input type="checkbox"/> > Python Django                   | ... | 1 </> 1 🎥 1 👤 |
| <input type="checkbox"/> > Python Flask                    | ... | 2 </> 1 🎥 2 👤 |

## Edit module: Introduction to Courses

Not Available For First Module

### Activities

#### Custom

Type: Message  
Title: Introduction to Courses  
Preview: A normal course consists of one or several of the following components...

#### Video

Topic: Security Vulnerabilities  
Video title: Insecure Direct Object Reference

#### Walkthrough Mission

Subcategory: Insecure Direct Object Reference  
Difficulty: [Progress]  
Hints: Enabled

#### </> Challenge

Subcategory: Insecure Direct Object Reference  
Difficulty: [Progress]  
Stage(s): Locate and fix the vulnerability  
Hints: Enabled

#### Coding Lab

Subcategory: SQL injection  
Difficulty: [Progress]  
Hints: Enabled

+ Add Activity

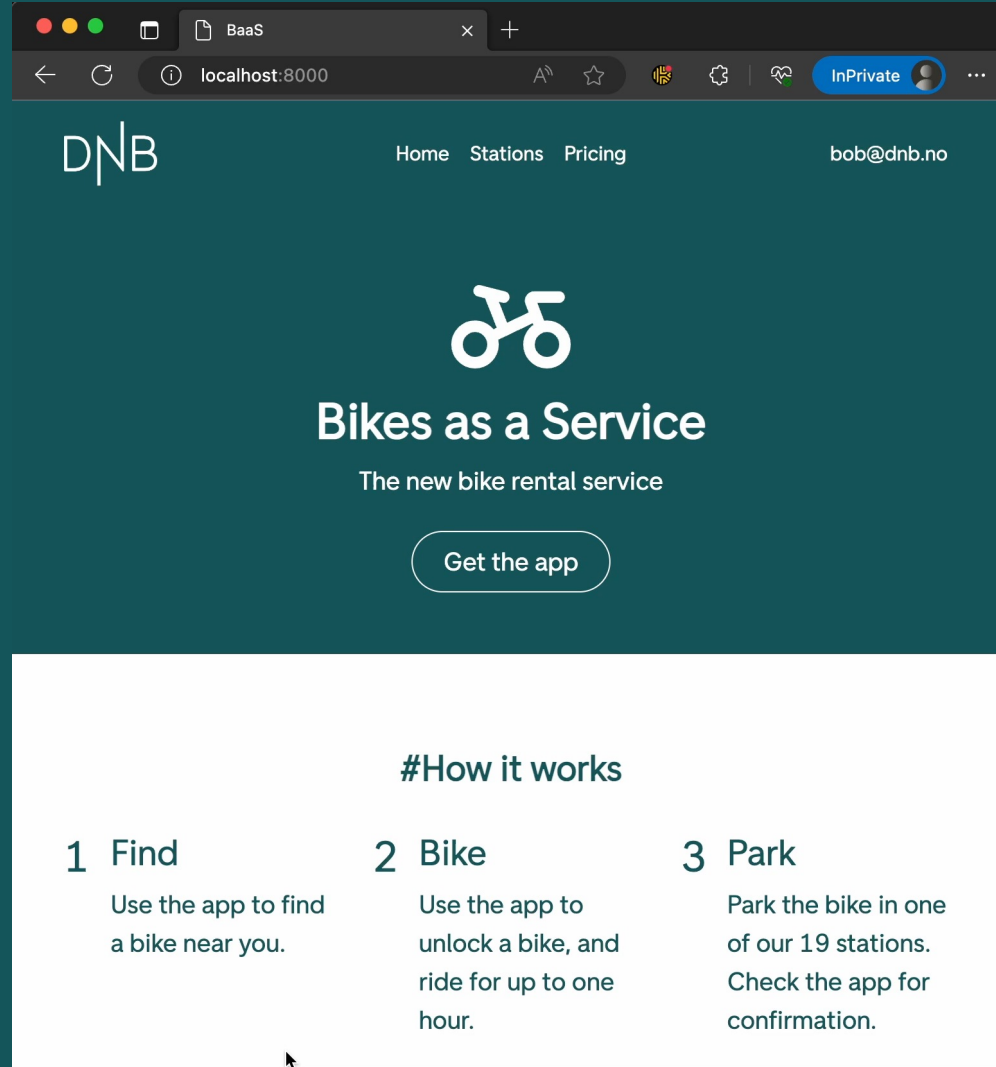
Cancel Apply changes

## The Case:

DNB has purchased a startup that offers easy-to-use bike rental across Oslo.

Your task is to review the security of their Web Portal. Using your knowledge of OWASP Top 10, can you find any vulnerabilities?

1. Find a way to see the information of another user  
(Hint: A01 Broken Access Control)
2. Using the trick from task 1, can you find any users of particular interest?
3. Log in on the account you found in task 2  
(Hint: A07 Identification and Authentication Failures)
4. You got access! But now what? Can you find anything new you have access to?
5. Give yourself a free lifetime subscription to the bike rental service



BaaS


localhost:8000

InPrivate

DNB

Home Stations Pricing

bob@dnb.no



# Bikes as a Service

The new bike rental service

Get the app

## #How it works

- 1 Find**  
Use the app to find a bike near you.
- 2 Bike**  
Use the app to unlock a bike, and ride for up to one hour.
- 3 Park**  
Park the bike in one of our 19 stations. Check the app for confirmation.

Try it yourself:

<https://github.com/bjornarfl/Secure-Coding-SF2023>

DNB

Thank you for listening!