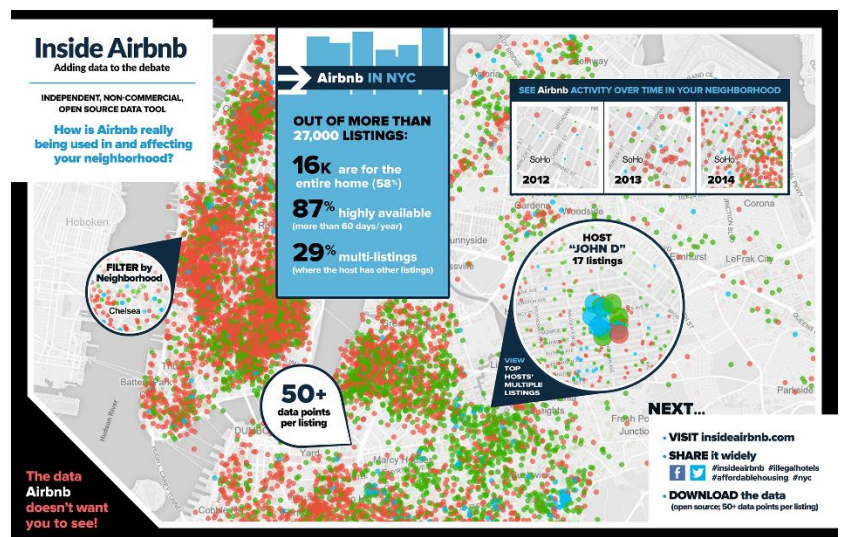


# Casus NoTS-WAPP: InsideAirbnb Amsterdam

Datum: 12-04-2022

Auteur: Marcel Verheij



Inside Airbnb © 2018

## Inhoudsopgave

Inhoudsopgave .....	2
1. Businesscase .....	3
2. Opdracht : Ontwikkel een webapplicatie .....	3
2.1. De applicatie moet voldoen aan de volgende technische eisen: .....	3
2.2. Use Case's: .....	4
3. Opdracht: Voer een onderzoek uit volgens de ICA onderzoeksmethodieken: .....	4
3.1. Onderzoeksopdracht .....	4
3.2. Onderzoeksvragen, uitgaande van/op basis van de casus, eisen en ontwikkel- hostingomgeving: .....	5
4. Opdracht : De resultaten van het onderzoek worden in de weken 3 t/m 7 van de course gepresenteerd .....	5
5. Ontwikkelomgeving .....	6
6. Gegevens AZURE .....	7
a. Tutorials & documentatie AZURE .....	7
b. Azure met Visual Studio .....	7
c. BUDGET .....	7
d. Belangrijk voor HERKANSERS: Azure Pay-As-You-Go .....	7
7. MAPBOX .....	8
8. Criteria .....	8
9. Toetsrooster WAPP P4/2021-2022 .....	10
Bijlage A : Voorbeeld frontend InsideAirBnB.com .....	13
Bijlage B: Bronnen .....	14

## 1. Businesscase

Het management van InsideAirbnb wil inzicht in het gebruik van Airbnb locaties in Amsterdam. Zij willen weten wat het gemiddelde aantal overnachtingen is in een maand, wat de opbrengsten zijn per buurt, en wat de gemiddelde reviews zijn in een buurt. Zij willen ook graag andere stuurinformatie die tijdens het ontwikkeltraject naar boven kan komen en laten zich daarvoor graag adviseren met behulp van een prototype. De site is bedoeld voor medewerkers van InsideAirBnB gebruik maar het management vindt het belangrijk dat de look-and-feel hetzelfde is als voor externe gebruikers. Inspiratiebron voor het front-end ontwerp is de site van [insideairbnb.com](https://insideairbnb.com).

## 2. Opdracht : Ontwikkel een webapplicatie

Ontwikkel een webapplicatie op basis van de allernieuwste ASP.NET CORE technologie die gehost wordt op MS AZURE. Er moet gebruik worden gemaakt van de publieke data die beschikbaar is via [insideairbnb.com](https://insideairbnb.com) van de stad Amsterdam. De webapplicatie moet een oplossing bieden voor de businesscase van InsideAirbnb.

### 2.1. De applicatie moet voldoen aan de volgende technische eisen:

- Ontwikkelt met de laatste Microsoft ASP.Net Core versie. (must)
- Wordt gehost op het Azure Cloud Platform. (must)
- Maakt gebruik van ASP.Net Razor pages of MVC. Alleen in overleg met docent als er goede redenen zijn om hiervan af te wijken. (must)
- Maakt gebruik van MSSQL Server (versie van Azure). (must)
- De applicatie moet veilig zijn. Gebruik de OWASP top 5 om de meest voorkomende onveiligheden op te sporen en af te dichten. (must)
- De applicatie is aantoonbaar highly-scalable. Er worden daarvoor performance tests als bewijsmateriaal opgeleverd (voor de performance-verbeteringen en daarna). (must)
- Authenticatie en autorisatie via Azure AD of IdentityServer4 (Authentication As A Service) of Auth0. (must)
- Caching service via Redis. (must)
- Microservice architectuur. (would)
- Microservice orchestration met Kubernetes. (would)
- Blazor applicatie met SignalR (would)

## 2.2. Use Case's:

1. Registeren en inloggen. (must)
2. Filter op prijs. (must)
3. Filter op buurt. (must)
4. Filter op review. (must)
5. Locaties van zoekresultaat zichtbaar op kaart. (could)
6. Kaart is clickable, details rechts op pagina, maakt gebruik van de mapbox API. (must)
7. Layout idem als insideairbnb.com. (could)
8. Details per item waarop gefilterd is: #overnachtingen, #opbrengst in de maand. (must)
9. Er moeten rollen toegevoegd en toegekend worden aan geregistreerde gebruikers. (must)
10. Resultaten zoals trends, totalen, gemiddelden, etc. worden weergegeven in charts, alleen te bekijken voor ADMINS. Denk daarbij aan bv. Gemiddelde beschikbaarheid per maand, gemiddelde beschikbaarheid per buurt, overzicht van gemiddelde huurprijs per buurt. Andere managementoverzichten zijn ook mogelijk, ga daarvoor op zoek naar online voorbeelden (must)

## 3. Opdracht: Voer een onderzoek uit volgens de ICA onderzoeksmethodieken:

### 3.1. Onderzoeksopdracht

Elke groep van studenten doet een onderzoek en presenteren de resultaten in twee kennissessies. Elke groep kiest twee onderwerpen waarvan er in ieder geval één over of een Security onderwerp of een Performance onderwerp gaat.

Voor de kennissessie: **Workshop Performance en Security** moet dus een performance en security onderwerp behandeld worden EN een algemeen onderwerp.

Performance onderwerpen:

- Performance improvements (DATABASE, AZURE, WEBAPP)
  - Storage Locking
  - Caching
  - Asynchrony
  - Queuing & Isolation
  - Redundancy & Fault Tolerance

Security onderwerpen:

- Een Top-5 security issue uit de OWASP lijst van 2017

Algemene onderwerpen:

- IAM via Azure B2C / Identity Server
- Entity Framework

- Repository pattern
- Displaying GeoData in ASP.NET CORE via Mapbox
- Displaying Charts in ASP.NET CORE
- Caching via Redis op Azure
- Azure deployment
- LINQ
- Of een ander relevant onderwerp die van belang is in de requirements/Use Cases.

Als een groep afvalt of niet in staat is om voldoende invulling te geven aan een gekozen onderzoek moet dit door anderen overgenomen worden. Het is dus de verantwoordelijkheid van alle deelnemers om de voortgang te monitoren en indien nodig bij te sturen.

### 3.2. Onderzoeksvragen, uitgaande van/op basis van de casus, eisen en ontwikkel- hostingomgeving:

Kies één van de OWASP Top 5 security issues.

- Wat is het?
- Hoe werkt het?
- Hoe merk je het?
- Hoe voorkom je het?
- Hoe implementeer je het?

Kies een performance onderwerp

- Wat is het?
- Hoe werkt het?
- Hoe implementeer je het?

Kies één van de andere onderwerpen nodig voor deze opdracht

- Wat is het?
- Hoe werkt het?
- Hoe merk je het?
- Hoe implementeer je het?

## 4. Opdracht : De resultaten van het onderzoek worden in de weken 3 t/m 7 van de course gepresenteerd

Bereid een presentatie inclusief workshop van minimaal 30 en maximaal 90 minuten voor met de hele groep. Het doel van de presentatie is:

- Een duidelijke presentatie geven van het gekozen onderwerp: duidelijke intro, doel, kern, einde.

- Kennisdeling over de gekozen onderwerpen: Heldere uiteenzetting van de gekozen onderwerpen zodat medestudenten dit kunnen toepassen in hun implementatie.
- Oefeningen/Workshop waarbij de resultaten geïmplementeerd worden samen met alle aanwezigen.
- Q&A.

## 5. Ontwikkelomgeving

Het doel van dit semester is dat er met de nieuwste versies gewerkt wordt van het .NET CORE ecosysteem. Dit betekent dat er veel zelf onderzocht, geëxperimenteerd en getest moet worden.

We gaan deze course in een volledig Microsoft Ecosysteem werken, voor Apple gebruikers het advies: zorg dat je systeem een volledig Microsoft omgeving kan draaien.

Daarvoor moet het volgende geïnstalleerd zijn om de lessen goed te kunnen volgen (advies: geen ryder, geen VS code of andere IDE vanwege preview DOTNET versies):

- Visual Studio Enterprise 2022 Preview via <https://visualstudio.microsoft.com/vs/preview/>
- Installeer de laatste .NET 7.0 preview release van de SDK via: [Download .NET 7.0 \(Linux, macOS, and Windows\) \(microsoft.com\)](https://dotnet.microsoft.com/en-us/download/dotnet/7.0)
- Zorg dat je SQL Server 2016 geïnstalleerd hebt inclusief SQL Server Management Studio (SSMS).

## 6. Gegevens AZURE

Het project moet uiteindelijk gedeployed en gepubliched worden op het MS-Azure platform. Op <https://azure.microsoft.com/nl-nl/> kun je een gratis 30-dagen account maken.

Toegang tot het project krijg je via de portal: <https://portal.azure.com/#home>

### a. Tutorials & documentatie AZURE

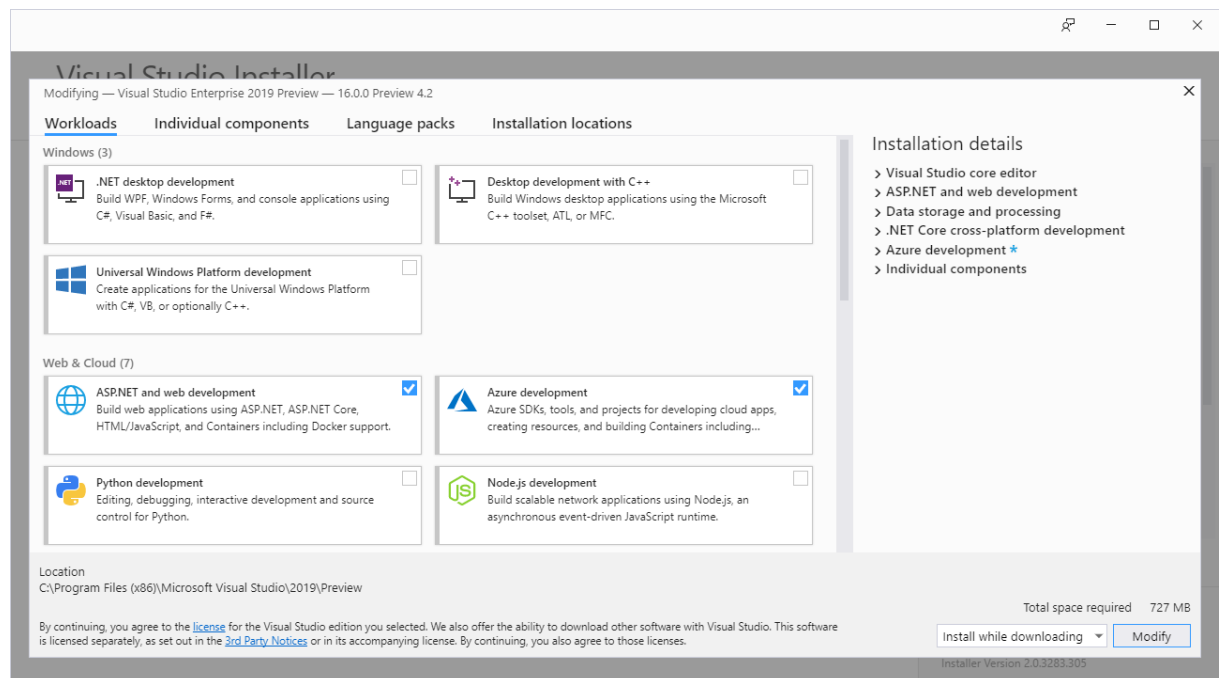
Er zijn diverse tutorials en documentatie beschikbaar via:

- <https://docs.microsoft.com/nl-nl/azure/app-service/app-service-web-get-started-dotnet>

### b. Azure met Visual Studio

De volgende zaken zijn van belang voor het gebruik van Azure met VS:

- In Visual Studio Installer kies je 'Modify' voor je Visual Studio product en zorg je dat de 'Azure Development' component aangevinkt is.



### c. BUDGET

Je hebt een beperkt **budget** om te spenderen aan dit project aan Azure diensten en moet dit zelf goed monitoren en managen. Als je over je budget gaat loop je dus kans dat je het project niet succesvol op Azure kunt deployen en publiceren en daardoor WAPP niet succesvol kunt afronden.

### d. Belangrijk voor HERKANSERS: Azure Pay-As-You-Go

Als je moet herkansen en je 30-dagen proefperiode is verlopen kun je gebruik maken van Azure Pay-As-You-Go via: [Betalen per gebruik : rechtstreeks betalen | Microsoft Azure](#)

De diensten die je nodig hebt voor het maken van de opdracht zijn gratis dus je zult niets te hoeven betalen (mits je zelf diensten inschakelt waarvoor je moet betalen). Zorg dat je geen diensten gebruikt die je niet nodig hebt, schakel diensten uit als je ze niet gebruikt (bv. de SQL server) want je hebt beperkt budget.

## 7. MAPBOX

Via MAPBOX kun je kaarten aanmaken met geolocation bestanden. Voor de airbnb casus kan het .geojson bestand gebruikt worden voor mapbox (account maken, mapstyle kiezen en via mapbox studio kan deze ingelezen, geedit en gebruikt worden via de mapbox API.

## 8. Criteria

De presentatie van de resultaten wordt beoordeeld op de volgende punten:

- Doel/Inleiding
- Inhoud:
  - Relevantie
  - Actualiteit
  - Nut
  - Uitleg
  - Toepasbaarheid
  - Begeleiding workshop
- Einde: Koppeling aan doel.

Het tussentijdse demo beroepsproduct wordt beoordeeld op de volgende inhoudelijke punten:

- Minimaal een basisstructuur van de app. (middleware, services via DI, EF)
- Hoeft nog niet gedeployed te zijn op Azure
- AIRBNB DB in MS SQLServer
- Identity mgmt (via google/fb door Azure B2C of identityserver)
- Enkele must have requirements geïmplementeerd.
- EF Core geïmplementeerd MET repository pattern
- Performance zaken uit workshops toegepast (async, queueing, linq, caching) of in ieder geval kunnen uitleggen waar deze toegepast moeten worden.
- Profiling geconfigureerd en werkend
- Profiling DB werkend en gevuld met eerste metingen



De producten van WAPP worden beoordeeld volgens onderstaande rubric:

	Onvoldoende	Matig - Voldoende	Voldoende - Goed	Uitstekend
<b>Oplossen van OWASP Security issues uit de top 5 lijst 2017</b>	Heeft minder dan drie Top-10 OWASP issues opgelost. Uit de PenTest blijkt dat er nog meerdere kritische vulnerabilites bestaan	Heeft de eerste drie Top-5 OWASP issues opgelost maar uit de PenTest blijkt dat er nog none critical issues bestaan	Heeft de eerste drie Top-5 OWASP issues opgelost, uit de PenTest zijn nog warnings gegeven, alles is gedocumenteerd en onderbouwd.	Heeft de Top-5 OWASP issues opgelost, uit de PenTest komen geen warnings, alles is gedocumenteerd en onderbouwd.
<b>Oplossen van Performance issues m.b.t. Database en Webapplicatie</b>	Er is nauwelijks geprobeerd performance-issues op te lossen en de beschrijving is te karig	Het is duidelijk dat er serieus is geprobeerd met onderbouwde acties het groepsproduct en/of -proces te verbeteren op het gebied van performance	Het is duidelijk dat de resultaten het groepsproduct en/of -proces sterk verbeterd zijn op het gebied van performance	Alle bottlenecks zijn duidelijk in kaart gebracht, gedocumenteerd, onderbouwd en aangepakt in de applicatie. De applicatie is gestroomlijnd en er zijn duidelijk bovengemiddelde activiteiten ondernomen om op prestatiegebied het uiterste uit de applicatie te halen.
<b>Implementeren van technische eisen en UseCases uit de gegeven Casus</b>	Er zijn geen must-have UC's geïmplementeerd	Niet alle must-haves zijn geïmplementeerd, er zijn een aantal UC's met lagere prioriteit geïmplementeerd.	Alle must-haves zijn geïmplementeerd plus een aantal UC's met lagere prioriteit	Alle eisen zijn geïmplementeerd en er zijn extra UC's die de functionaliteit van de applicatie ten goede komen toegevoegd.
<b>Ontwerpdocumentatie up-to-date.</b>	Er is geen documentatie opgesteld	Er is een document opgesteld echter keuzes en resultaten zijn summier verantwoord.	Alle keuzes, resultaten van performancetests en pentests zijn beschreven en verantwoord met relevante technieken (UML, Functioneel ontwerp, technisch ontwerp, testrapport).	Bovenop het ontwerpdocument is er een onderzoek gedocumenteerd, onderbouwd met de methodekaart, Proof of Concepts/Prototypes zijn beschreven, de resultaten zoals ze in de webapplicatie zijn opgenomen zijn beschreven.
<b>Demonstratie van Webapplicatie</b>	De kwaliteit van de architectuur voldoet niet aan de gestelde eisen. Er is nauwelijks geprobeerd om aan de eisen te voldoen	Er is duidelijk geprobeerd om alle architectuureisen te implementeren, niet alles is gelukt ondanks pogingen daartoe.	De ASP.NET CORE request pipeline is correct geïmplementeerd, de architectuur is correct toegepast (Entity Framework, Authentication as a Service, Caching as a service, SQL Server en Webapplicatie gepubliceerd in de Cloud)	Er is bovenop de ge-eiste architectuurimplementaties onderzoek uitgevoerd naar nieuwe ontwikkelingen op architectuurgebied en de uitkomsten zijn geheel of gedeeltelijk geïmplementeerd.
<b>Kennisessies</b>	De structuur van de presentatie en workshop is onduidelijk. Er is weinig moeite gedaan om een kwalitatief goede kennissessie voor te bereiden en uit te voeren.	Er is duidelijk geprobeerd om een onderzoek uit te voeren naar de gekozen onderwerpen. De resultaten blijven oppervlakkig, er is weinig concrete informatie voor medestudenten	Er is een goed onderzoek uitgevoerd, de resultaten zijn helder gepresenteerd, Er is concrete informatie gegeven voor medestudenten om te gebruiken in het beroepsproduct.	Er is een uitvoerig onderzoek uitgevoerd met concrete resultaten en duidelijke instructies voor medestudenten. Er zijn nieuwe inzichten, ontwikkelingen en implementaties gevonden, toegepast en meegegeven aan medestudenten.

De ontwerpdocumentatie moet aan het volgende voldoen:

- De vorm en layout van het document voldoet aan de ICA controlekaart (titelpagina, inhoudsopgave, genummerde hoofdstukken/paragrafen en paginanummers).
- Er zijn twee hoofdstukken, 1 over performance en 1 over security
- In het hoofdstuk performance wordt uitleg gegeven welke performance issues zijn opgelost met een verantwoording en bewijsvoering (screenshots van performancemetingen met VS2017 OF Apache JMeter, bewijs van Sweetspot en Operational Ceiling, screenshots profiling van start development tot eind, uitleg en voorbeelden wat er gewijzigd is in code, settings, configuratie)
- In het hoofdstuk security wordt uitleg gegeven welke security issues zijn opgelost met een verantwoording en bewijsvoering (idem als bij performance).

## 9. Toetsrooster WAPP P4/2021-2022

### ***Deadlines:***

Inleverdata beroepsproducten ISAS:

Toetsen WAPP ISAS

Nieuwe inleverdata BP's

- |          |   |
|----------|---|
| <b>1</b> | <b>week 5 Onderzoek Performance</b>                   |
| <b>2</b> | <b>week 6 ASP.Net Infra/Performancetest Simulatie</b> |
| <b>3</b> | <b>Week 7 Onderzoek Security</b>                      |
| <b>4</b> | <b>Week 8 Datagedreven WebApp</b>                     |
| <b>5</b> | <b>Week 9 Hertentamens</b>                            |

**Gastcolleges:**

Datum	Onderwerp	Gastdocent	Lokaal
22/4 09.30	Sessie 1: Identity, AuthN & AuthZ with Azure AD	Sander van den Hoven Technical Strategist	R26 / C102a
29/4 09.30	Sessie 2: .NET Blazor	Sander van den Hoven Technical Strategist	R26 / C102a
13/5 09.30	Sessie 3: Azure Cloud	Bodgan Grozoiu Cloud Solution Architect	R26 / C102a
20/5 09.30	Sessie 4: Modern Applications & Serverless	Bodgan Grozoiu Cloud Solution Architect	R26 / C102a
03/6 09.30	Sessie 5: Cloud Security.	Olivier van der Kruijf Cloud Solution Architect	R26 / C102a

**Assesments:**

- Week 3 t/m 7, woensdagen presentaties Performance/Algemene onderwerpen en Security (Top 10 OWASP issues)
- Week 4, Assessment Infrastructuur AirBNB applicatie en performancetest
- Week 8, Assessment AirBNB applicatie incl. Security en alle UseCases

Eisen inhoud presentaties:

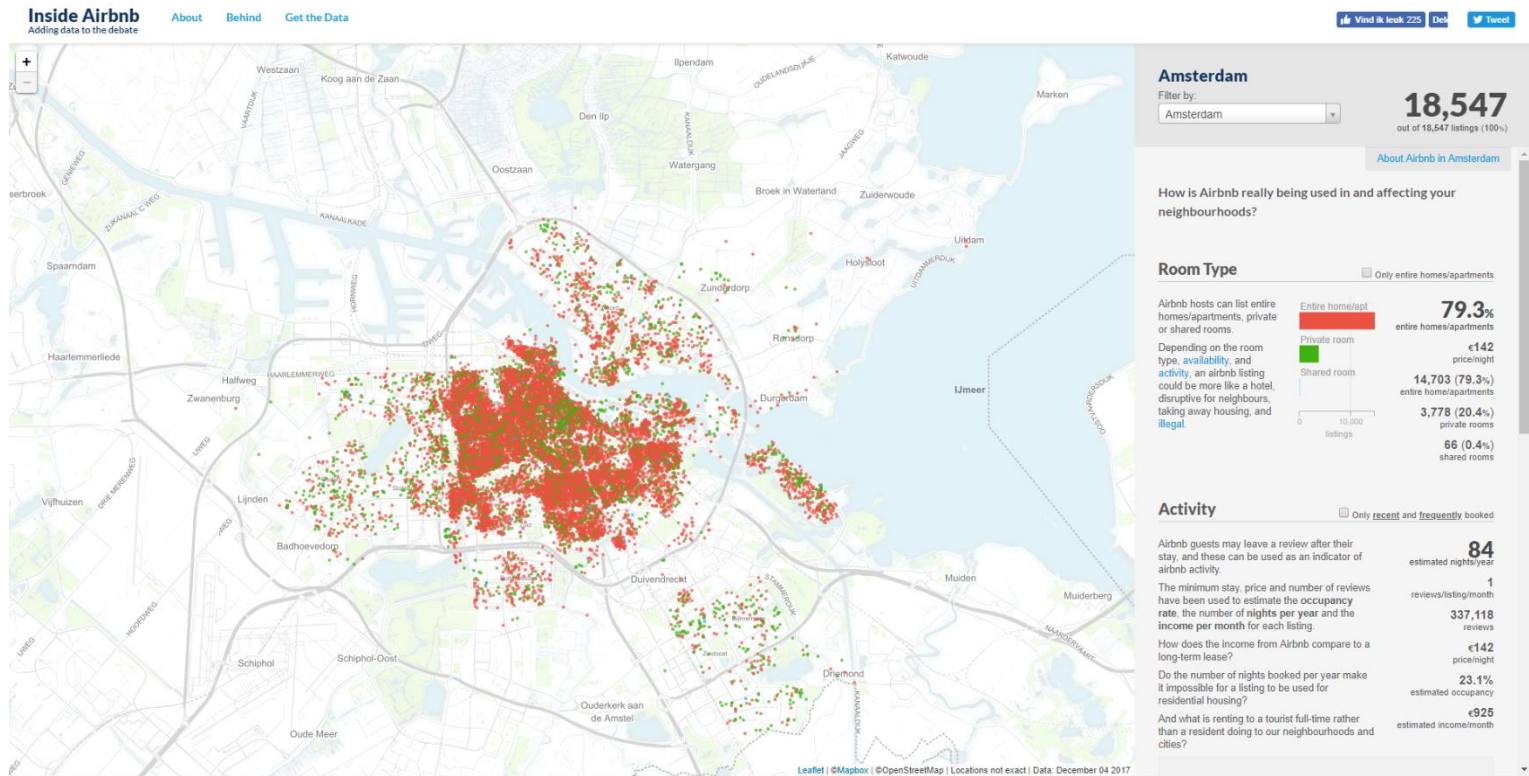
- Goede uitleg van het onderwerp
- Hoe te implementeren in DOTNET CORE
- Goede kennisoverdracht en workshops
- Max 45 minuten.

- Iedereen bedenkt een vraag per onderwerp voor zowel Security als Performance, deze moeten in de workshops behandeld/beantwoord worden

Planning presentaties/workshops:

P4-2021/2022	Workshops WAPP				
Vul per groep de studentnummers en namen in. Max. 4 studenten per groep.					
Studentnummer	Achternaam		Voornaam	Presentatiedatum	Onderwerp
Groep 1				Week 3 Donderdag 28 April	Identity Server/Azure Identity A1-Injection
Groep 2				Week 4 Woensdag 11 Mei	Entity Framework/Repository pattern A3-Sensitive Data Exposure
Groep 3				Week 5 Woensdag 18 Mei	Mapbox A6- Security Misconfiguration
Groep 4				Week 6 Donderdag 25 Mei	Charts A2 - Broken Authentication
Groep 5				Week 7 Woensdag 1 Juni	A1 Injection Response headers
Groep 6				Week 7 Woensdag 1 Juni	SQL SRV -> Azure Deployment A5 - Broken Access Control

## Bijlage A : Voorbeeld frontend InsideAirBnB.com



## Bijlage B: Bronnen

Airbnb. (z.d.). <https://www.airbnb.nl>. geraadpleegd op 12 April 2022

InsideAirbnb. (z.d.). <http://insideairbnb.com/get-the-data.html>. geraadpleegd op 12 April 2022

OWASP (27-03-2018). *Top 10 Security issues*. geraadpleegd op 12 April 2022, van [https://www.owasp.org/index.php/Top\\_10-2017\\_Top\\_10](https://www.owasp.org/index.php/Top_10-2017_Top_10).