Datagedreven webapplicatie getest voor high performance en security door Michelle Jolink, datum, Course NotS-WAPP

Ontwerpdocument Inside AirBnB Amsterdam

2019

Inhoudsopgave

[1. Inleiding 2](#_Toc10460856)

[2. Functioneel ontwerp 2](#_Toc10460857)

[3. Technisch ontwerp 2](#_Toc10460858)

[4. Performance 2](#_Toc10460859)

[4.1. AsNoTracking 3](#_Toc10460860)

[4.2. Async 5](#_Toc10460861)

[4.3. Caching 6](#_Toc10460862)

[4.4. Conclusie 7](#_Toc10460863)

[5. Security 7](#_Toc10460864)

[5.1. OWASP ZAP 7](#_Toc10460865)

[X-Frame-Options Header Not Set 7](#_Toc10460866)

[Cookie No HttpOnly Flag 7](#_Toc10460867)

[Cookie Without secure flag 8](#_Toc10460868)

[Incomplete or No Cache-control and Pragma http Header Set 8](#_Toc10460869)

[Web Browser XSS Protection Not Enabled 9](#_Toc10460870)

[X-Content-Type-Options Header Missing 9](#_Toc10460871)

[5.2. Conclusie 9](#_Toc10460872)

[Bijlages 10](#_Toc10460873)

[Bijlage “Caching load test” 10](#_Toc10460874)

[Bijlage: Literatuurlijst 11](#_Toc10460875)

# Inleiding

* Korte beschrijving casus

# Functioneel ontwerp

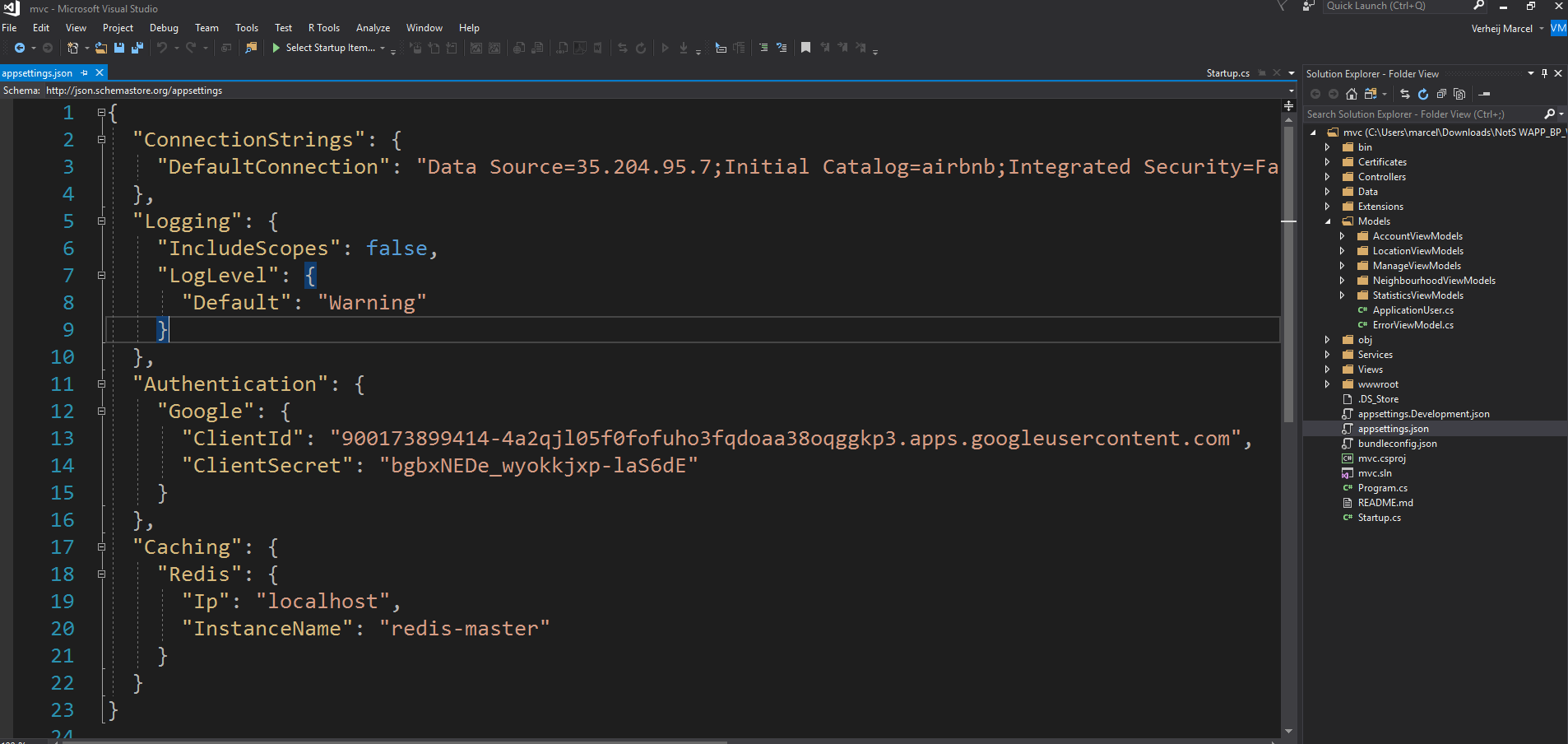
* Use Cases

|  |  |
| --- | --- |
| Use case | Prioriteit |
| Registeren en inloggen. | Must |
| Filter op prijs. | Must |
| Filter op buurt. | Must |
| Filter op review. | Must |
| Kaart is clickable, details rechts op pagina, maakt gebruik van de mapbox API. | Must |
| Details per item waarop gefiltered is: #overnachtingen, #opbrengst in de maand. | Must |
| Er moeten rollen toegevoegd en toegekend worden aan geregistreerde gebruikers. | Must |
| 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 |
| Layout idem als insideairbnb.com. | Could |
| Locaties van zoekresultaat zichtbaar op kaart. | Could |

# Technisch ontwerp

* Architectuur
* Overzicht gebruikte frameworks
* Overzicht gebruikte packages incl. versies

Configuratie externe services, etc.:



Figuur 1

# Performance

## Nulmeting listings

Om de verbeteringen in performance van de applicatie goed in beeld te krijgen op basis van de aanpassingen wordt er een nulmeting gedaan. Deze test zal gedaan worden met NBomber. Hierbij heb ik mijn laptop zo schoon mogelijk gehouden, hiermee bedoel ik dat ik geen andere programma’s open heb dan visual studio en mijn laptop voor de test heb herstart. Voor NBomber worden de volgende instellingen gebruikt:

Afbeelding met tekst, Lettertype, schermopname

Automatisch gegenereerde beschrijving

De nulmeting wordt gedaan op de API route die bij het opstarten van de applicatie alle 74.000+ listings ophaalt. Deze route haalt alleen de longitude, latitude en id op, maar ondanks dat is dit alsnog veeleisend.

De aangesproken endpoint voor het bepalen van de prestatie verbeteringen is:

* **GET /api/Listings/geoinfo**

Afbeelding met schermopname, Perceel, lijn, tekst

Automatisch gegenereerde beschrijving

Database queries voor non clustered index en na

Toevoegen van performance verbeteringen (performance powerpoint)

Zoals te zien is reageert de API in het begin erg snel, maar na 15 seconden zien we dat de vertragingen beginnen op te lopen.

Afbeelding met tekst, schermopname, lijn, Lettertype

Automatisch gegenereerde beschrijving

|  |  |  |
| --- | --- | --- |
| **Minimale responsetijd** | **Maximale responsetijd** | **Gemiddelde responsetijd** |
| 0.2129 seconden | 20.0492 seconden | 9.44228 seconden |

Er falen ook geen requests, dus dat is positief. Wel duren de meeste requests langer dan 1.2 seconden. Dit willen we natuurlijk verbeteren. Naar mate de tijd en requests toenemen is de zien dat de responsetijd boven de 10 seconden komt. Dit is wel erg hoog.

## AsNoTracking

Entity Framework biedt een aantal opties voor het verbeteren van de prestaties. Een van deze opties is AsNoTracking(). Met deze optimalisatie kan er aangeven worden dat Entity Framework de resultaten van een query niet moet bijhouden. Dit betekent dat Entity Framework geen aanvullende verwerking of opslag uitvoert van de entiteiten die door de query worden geretourneerd. Wat ervoor zorgt dat er minimaal verbruik gemaakt wordt van memory. (Bron)

AsNoTracking () moet alleen maar gebruikt worden wanneer de intentie is om data op te halen en wijzigingen niet bij te houden.

**Aangepaste code:**

**Afbeelding met tekst, schermopname, software, Lettertype

Automatisch gegenereerde beschrijving**

Zoals te zien is heb ik de AsNoTracking heel gemakkelijk toe kunnen voegen aan de pipeline. Laten we kijken wat dit voor de performance heeft gedaan:

### Resultaten AsNoTracking

### Afbeelding met schermopname, tekst, lijn, Perceel Automatisch gegenereerde beschrijving

Zoals we kunnen zien is de piek ongeveer 5 seconden verbeterd, want nu loopt de piek pas op na 20 seconden.

### Afbeelding met tekst, schermopname, lijn, Lettertype Automatisch gegenereerde beschrijving

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Minimale responsetijd** | **Maximale responsetijd** | **Gemiddelde responsetijd** |
| ***Nulmeting*** | 0.21290 seconden | 20.0492 seconden | 9.44228 seconden |
| ***Na asNoTracking*** | 0.20309 seconden | 16.8268 seconden | 7.34436 seconden |
| ***Verbetering*** | 0,00981 seconden | 3,2224 seconden | 2,09792 seconden |

### Ook zien we hier dat een deel van de requests die eerst in het gebied > 1.2s zaten nu in het gebied tussen 800ms en 1.2s zitten. De minimale responsetijd is minimaal afgenomen, maar bij de maximale en gemiddelde responsetijd is al zeker verbetering te zien. De maximale responsetijd is van 20.04 naar 16.8 gegaan en de gemiddelde responsetijd van 9.4s naar 7.3s. Al een stuk beter dus! Toch streven we naar meer!

## Nulmeting statestieken admin

Een endpoint om admin statestieken data op te halen voert een JOIN uit en is erg langzaam bij aanroepen. Hiervoor wil ik ook de performance verbeteren. Ik gebruik dezelfde NBomber isntellingen als bij nulmeting listings.

Code die wordt uitgevoerd voor performance verbeteringen:

Afbeelding met tekst, schermopname, software, Lettertype

Automatisch gegenereerde beschrijving

De aangesproken endpoint voor het bepalen van de prestatie verbeteringen is:

* **GET Listings/stats/revenue-per-neighbourhood-per-month?neighbourhood=Bourse**

## 4.4. Conclusie

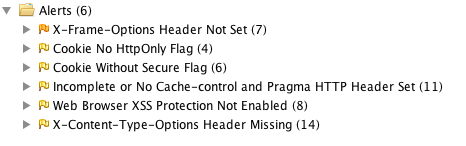
Als de hoogste aantal requests per seconde gepakt worden bestaat er een verbetering van 2122.22%. De grootste verbetering ontstaat door gebruik te maken van In-Memory caching, wat de latency omdat de applicatie niks van de database hoeft op te halen.

# 5. Security

In dit hoofdstuk wordt uitleg gegeven op de security issues die zijn gevonden met OWASP ZAP.

## 5.1. OWASP ZAP

De onderstaand Alerts zijn de issues die gevonden zijn binnen mijn webapplicatie. Deze issues worden stuk voor stuk verwerkt in dit hoofdstuk. Zie figuur 6.

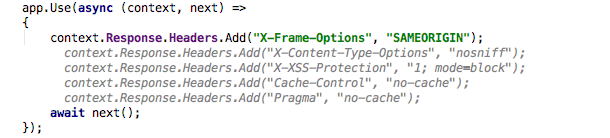


Figuur 6

### X-Frame-Options Header Not Set

X-Frame-Options header zorgt ervoor dat de browser het niet of wel toelaat om de content in een X-Frame te laten zien.

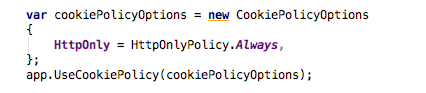
In dit geval is een X-Frame niet van toepassing en kan op de volgende manier opgelost worden. Zie figuur 7.



Figuur 7

### Cookie No HttpOnly Flag

Cookies mogen alleen maar gebruikt bij het http protocol. Dat betekent dat het niet mogelijk is om document.cookie te gebruiken vanuit een javascript bestand.

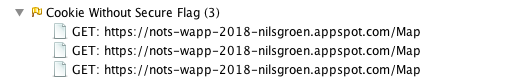


Figuur 8

### Cookie Without secure flag

Cookies met een secure kenmerk zijn een soort cookies die worden verzonden via gecodeerde http-verbindingen. Bij het instellen van de cookie geeft het secure kenmerk de browser de opdracht om de cookie alleen via geëncrypte verbindingen gebruikt moet worden.

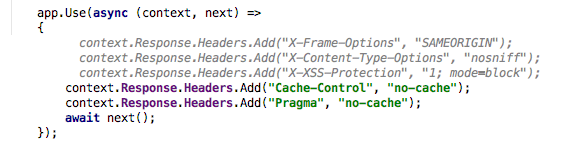
Aangezien het alleen maar te vinden is bij de Map pagina heb ik de aanname genomen dat mapbox de boosdoener is. Zie figuur 9.



Figuur 9

### Incomplete or No Cache-control and Pragma http Header Set

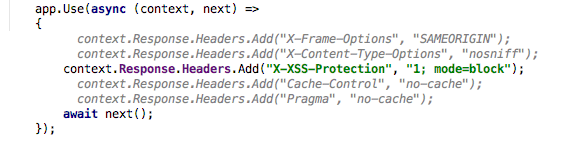
De “Incomplete or No Cache-control and Pragma” header zorgt ervoor dat de browser altijd checked bij de server of de gecachde response nog geldig is. Hierdoor is het onmogelijk dat een response te lang wordt gecached en wordt weergegeven wanneer dit niet de bedoeling is. Deze headers worden overschreven wanneer er in de code headers worden toegevoegd aan bepaalde endpoints, bijvoorbeeld wanneer ik in de code aangeef dat een response maximaal 120 seconde gecached mag worden. Zie figuur 10.



Figuur 10

### Web Browser XSS Protection Not Enabled

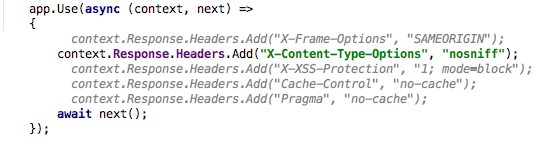
Deze header zorgt ervoor da een browser geen requests meer stuurt wanneer er XSS wordt herkend. Dit heb ik opgelost met de onderstaande code. Zie figuur 11.



Figuur 11

### X-Content-Type-Options Header Missing

Deze header zorgt ervoor dat de browser niet gaat proberen te raden wat de MIME type is van een bestand dat wordt opgehaald vanuit de server. Dit heb ik opgelost met de onderstaande code. Zie figuur 12.



Figuur 12

## 5.2. Conclusie

Zoals te zien in het bovenstaand voorbeeld zijn er door ZAP zes alerts gevonden. Hiervan heb ik vier kunnen oplossen. De rest van de alert komen de mapbox api. Daarnaast worden veel van de security issues al opgelost alleen door gebruik te maken van .Net core, identity en entity framework. Zie figuur 13 voor de overgebleven errors.

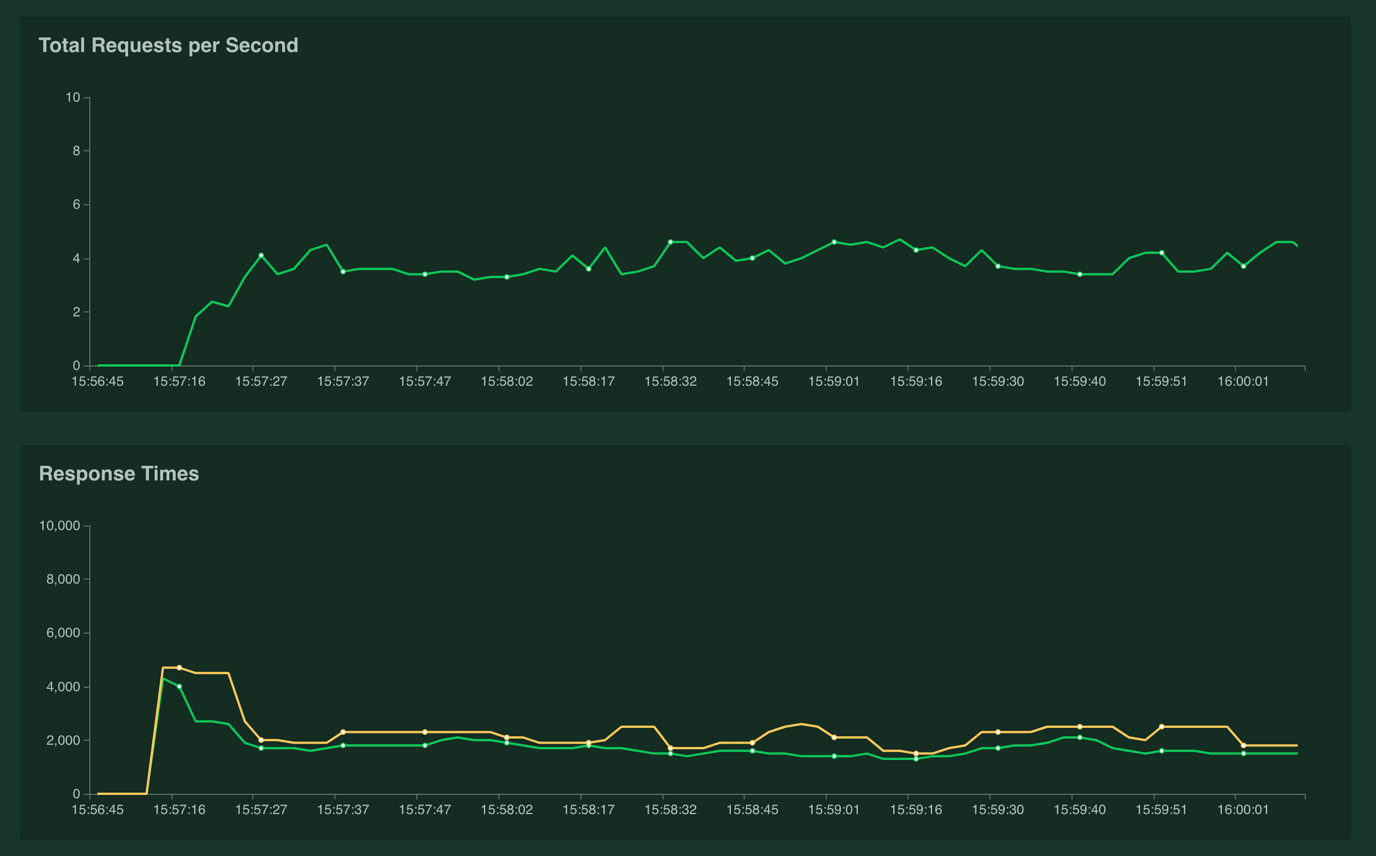


Figuur 13

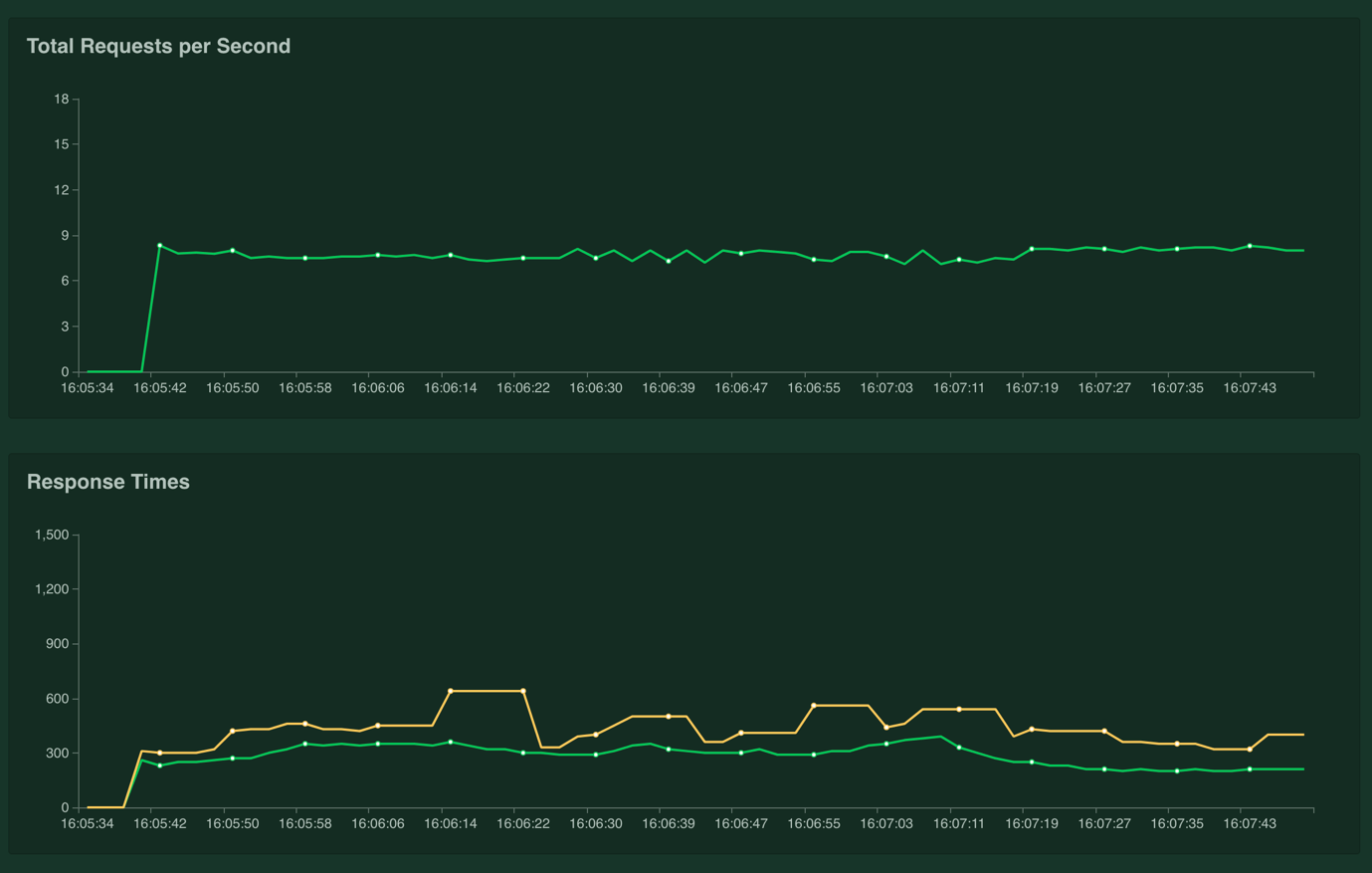
# Bijlages

## Bijlage “Caching load test”

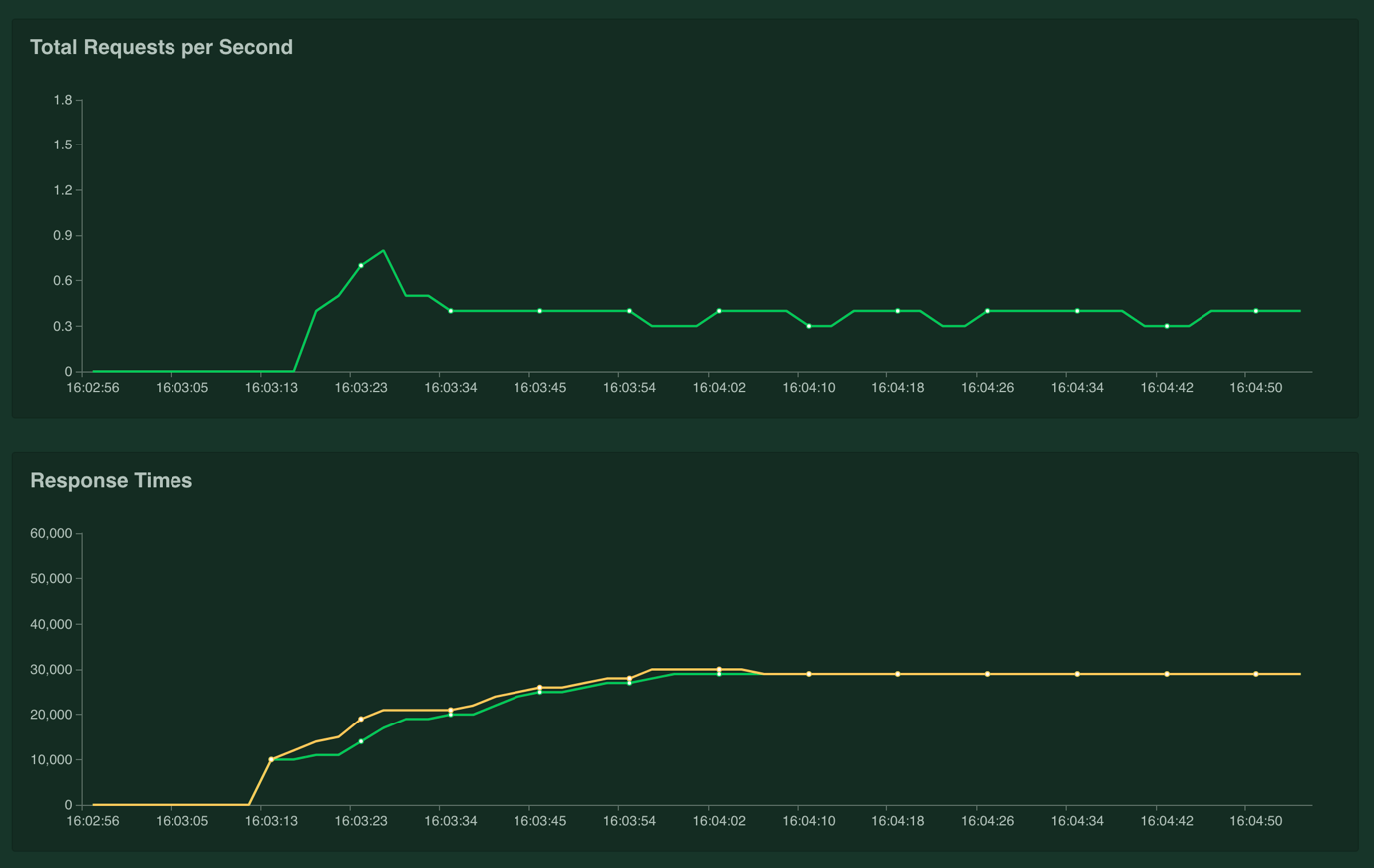
**Database**



**In-Memory**



**Redis**



## Bijlage: Literatuurlijst