Aantekeningen

Inhoud

[27-11-2020 3](#_Toc58485579)

[01-12-2020 4](#_Toc58485580)

[3-12-2020 5](#_Toc58485581)

[4-12-2020 6](#_Toc58485582)

[Feedback: 6](#_Toc58485583)

[2 type kortingscodes die de klant wilt: 6](#_Toc58485584)

[Features in de volgende sprint: 6](#_Toc58485585)

[Verbeterpunten komende sprint: 6](#_Toc58485586)

[Verbeterpunten presentatie: 6](#_Toc58485587)

[Testrapport 7](#_Toc58485588)

[Testrapportage sprint 2: 7](#_Toc58485589)

[Activiteiten: 7](#_Toc58485590)

[Trello bord aanpassen onderwerpen: 7](#_Toc58485591)

[Onderwerpen: 7](#_Toc58485592)

[07-12-2020 8](#_Toc58485593)

[Securityscan 8](#_Toc58485594)

[Technisch Ontwerp 8](#_Toc58485595)

[8-12-2020 9](#_Toc58485596)

# 27-11-2020

Aanwezig: Ivar, Jan Willem, Roy, Jasper, Ana  
Notaris: Jasper

Activity diagram voor bezoeker en videoportaal gemaakt

Wisten niet precies hoe dat moest omdat het ons best weinig leek. Bezoeker klikt of klikt niet op het filmpje als hij het wilt bekijken.

Docent binnengekomen en gevraagd hoe het ging. Ging voor iedereen wel goed. Vraag over taakverdeling: we kunnen maar 2 rollen verzinnen.

Misschien iemand aanstellen om documenten na te kijken (aan het einde van een sprint) zodat alles er ongeveer hetzelfde uit ziet. Nu gebruiken we Engels en Nederlands door elkaar etc.

Opmerking over mailserver van Ivar voor docent. Kan via localhost. Voor security niet handig want het wachtwoord staat er letterlijk in. Voor dit project niet handig maar wel goed om mee te nemen in het securityverslag. Verslag gaat (o.a.?) over problemen waarvoor je een oplossing hebt geïmplementeerd en andere problemen waarvan je weet dat ze niet veilig zijn maar je het niet veiliger hebt gemaakt.

Activity diagram voor contentbeheerder en videoportaal gemaakt

Besloten in de inleiding uit te leggen wat het filmpje in dit activity diagram betekent.

Deze bleek ook best wel klein te zijn.

Begonnen met de inleiding. Besloten dit niet af te maken want dit was nog best wel lastig. Pas afmaken als we alles van het document afhebben

Jan Willem’s stukje code: Veel uitleg over het stukje code, lastig te begrijpen. Besloten waar de session\_destroy moet komen te staan: op een plek waar het niet wordt gehinderd door iets en waar de bedragen op pay.php kloppen.

Besloten de header uit confirmation.php te halen zodat je de check of de bedragen kloppen op dezelfe pagina kan doen.

Het stukje van de loginpagina foutmeldingen zit nu op dezelfde manier verwerkt in confirmation.php. Daarna weer terugveranderd omdat het nog niet zo makkelijk werkte als gewenst en wegens tijdgebrek wordt je nu bij een fout bedrag teruggestuurd naar de vorige pagina (invullen). Jasper of Ivar gaat wanneer hij klaar is met het inloggen waarschijnlijk bezig met het goedmaken van confirmation.php.

# 01-12-2020

Aanwezig: Jasper, Ivar, Jan Willem  
Notaris: Jan Willem

IT architectuur maken voor het programma eisen en wensen wat valt onder het vak pakketselectie en wat meetelt voor de KBS.

Wij gaan eisen stellen over wat wij willen in het videoportaal en wat niet.

Dit doen we met behulp van de architectuurprincipes die we hebben gekregen op de meegegeven site.

De principes vormen de “spelregels” van ons systeem ze geven aan wat wel en niet mag in ons videoportaal, het is aan ons om uit te zoeken wat wij belangrijk vinden.

De docent heeft ons geholpen met ons op gang helpen.

Verslag is voor een groot deel in de les gemaakt, na de les is het verslag afgerond.

# 3-12-2020

Aanwezig: Jasper, Ivar, Jan Willem, Ana  
Notaris: Jasper

*Wat heeft Jasper gedaan deze sprint? Jasper heeft het inloggen en aanmelden gemaakt, en het automatisch invullen bij order.php wanneer ingelogd.*

*Wat heeft Jan Willem gedaan deze sprint? Jan Willem heeft het confirmatie scherm voor het betalen gemaakt. Ook heeft Jan Willem de klantenservice gemaakt.*

*Wat heeft Ivar gedaan deze sprint? Ivar heeft een mailserver opgezet, waardoor de klant en wij een factuur krijgen van de bestelling. Ook krijgt de customerservice een mail wanneer de klant een vraag heeft bij de klantenservice.*

*Wat heeft Ana gedaan deze sprint? Ana heeft het kortingscode systeem gemaakt en het optimaliseren van het betalen.*

*Wat heeft Roy gedaan deze sprint? Roy heeft het factuur gemaakt en gegenereerd in pdf formaat.*

Vandaag zijn we begonnen met het security verslag

Ivar, Jan Willem en Jasper waren op school aanwezig, Ana was ongeveer een uurtje via teams aanwezig.

Het was best lastig om een begin te maken maar na een tijdje wisten we wel het één en ander te noemen voor risicoanalyse.

We zijn hierna verder gegaan met het beschrijven van het ingebouwd veiligheidsniveau. We zijn erachter gekomen dat we niet heel veel voor security hebben gedaan, alleen hashed wachtwoorden en sql injection.

Vraag of inloggen bij security hoort aangezien het gaat over identificatie etc. op de elo.

Alles nagekeken of er security bij is gemaakt.

Cart uitgelegd gekregen

Demo 2 powerpoint gemaakt, alleen uurdistributie moet nog

Security verslag nog niet af

Wat problemen (mail customer service) en extra functionaliteiten (uitloggen) voor site gemaakt.

# 4-12-2020

Aanwezig: Jasper, Roy, Ana, Jan Willem, Ivar

Notaris: Ivar

Bij deze aantekening hebben we een demo die we gaan uitvoeren. In de ochtend hebben we de PowerPoint nog goed doorgenomen en kleine css deeltjes opgepakt. De website ziet er nu redelijk acceptabel uit.

Jasper en Jan-Willem voeren de demo uit. Jasper doet de demo en Jan-Willem doet de presentatie.

## Feedback:

Wachtwoord policy  
Consistente voorraad notatie

### 2 type kortingscodes die de klant wilt:

* Hallo code Met geldigheid. Voor iedereen. Voor een bepaalde tijd
* Individuele codes. Eenmalig.

### Features in de volgende sprint:

* Automatisch aanvullen van Strong-Search-Form.
* Kleine fouten eruit halen
* 2 Decimalen van prijs
* Raspberry Temp.
* Database optimalisatie
* Korting in het factuur opnemen
* Gender Onzijdig
* Alles in het Nederlands
* Stijling Buttons

### Verbeterpunten komende sprint:

* Meerdere items in backlog
* Betere (en tijdige) documentatie
* Proces beter in controle houden, En laten zien

### Verbeterpunten presentatie:

* Conversie verhogende punten benoemen tijdens de demo.
* Backup als demo niet werkt
* Wellicht opnemen voor review en zelfreflectie

## Testrapport

Aanwezig: Jasper, Roy, Ana, Jan Willem, Ivar

Notaris: Roy

Bij deze aantekeningen hebben we het testrapport aangepast voor het einde van de sprint. Na de demo hebben we een pauze genomen en hier zijn we mee bezig gegaan in de KBS les.

### Testrapportage sprint 2:

* Factuur mist nog korting.
* Overleg over orders opslaan in een database en zo ordernummers toewijzen aan orders.
* Op het moment geeft een onjuiste kortingscode nog geen melding terug.

### Activiteiten:

* Overleg over urenregistratie.
* Voortgangsrapportage ingevuld.
* Trello bord aanpassen.

### Trello bord aanpassen onderwerpen:

* Taalgebruik en code rechttrekken, alles naar één taal verwerken.
* Persoonlijke kortingscode, een code die eenmalig te gebruiken is.
* Voorraad notatie rechttrekken, grote getallen moeten veranderd worden naar iets als ‘ruim op voorraad’.
* Password policy, er moet een bedacht worden die ook gecheckt kan worden.
* Raspberry Pi

### Onderwerpen:

* Raspberry Pi moet de live temperatuur in een database zetten die gelinkt gaat worden aan de producten database, de temperatuur moet uit het database gehaald worden en live op de site worden geplaatst onder de *chilled products* (bijvoorbeeld chocolade).
* Vragen m.b.t. aanstaande donderdag, aangezien het rooster een klein beetje is aangepast.

# 07-12-2020

Aanwezigen: Roy, Ana, Jasper, Jan Willem, Ivar  
Notaris: Ivar

Ana heeft veel kleine taken gedaan om tijd recht te trekken. Is redelijk goed gegaan. Roy heeft niet getracht tijd in te halen.

## Securityscan

14-12-2020 inleveren

## Technisch Ontwerp

14-12-2020 inleveren

Losstaande tabellen invoeren.

Besloten om bestelling wel in de database te plaatsen. De manier om een bestelling aan de klant te koppelen is e-mailadres en voor -achternaam.

Database vinden wij allen erg ingewikkeld.

# 8-12-2020

Aanwezigen: Roy, Ana, Jasper, Jan Willem, Ivar  
Notaris: Jasper

Pakketselectie requirements t.a.v. functionaliteiten gemaakt.

Uitleg gekregen over waarom heb je bron nodig en waar kan je deze vinden.

In kbs les opdracht sprint 3 bekeken (zonder Ivar)

Voor autorisatie: account bezoeker/klant maken. Permissies zijn select, update en insert van de tabellen beschreven bij de bijbehorende queries in de betreffende php code

Engine tabje: gebruik van archive engine op alle archieftabellen. De FK gaat dan weg maar we weten niet waarom dat uit zou maken.

Tabel people heeft al een trigger voor correcte\_email.

Gedragsregels: trigger of php controle voor sowieso correcte postcode

Transactie: SQL commando na betalen moet 1 commando zijn, dus waarschijnlijk met procedure

Temperatuursensor: alle isChillerStock = 1 moeten de temperatuur gemeten worden dmv de raspberry pi. CodeRoomSensorNumber = 5. Data van pi niet lokaal opslaan maar naar nerdygadgetsdatabase (die wel lokaal staat maar op pc/laptop). Elke 3 seconden wordt de temperatuur geupdate. Oude temperaturen worden in de coldroomtemperatures\_archive geschreven.

Voor de database mogen we onze eigen selectie tabellen gebruiken en toevoegen. TO, Pakketselectie en Security scan af voor vroegtijdige review en feedback. TO moet af zijn, maar we moeten proberen zo veel mogelijk te doen (niet maken zonder ontwerp, wel niet maken met ontwerp).

# 11-12-2020

Aanwezigen: Jasper, Jan Willem, Ivar  
Notaris: Jasper

Security verslag verder gemaakt

Bronvermelding: kleine uitleg met verdere verwijzing naar de bronnen

Weten niet zeker of php hash wel secure is

Password policy: heeft nerdy gadgets waarschijnlijk niet. Gekeken op de referentie architectuur van nerdy gadgets maar niet echt een policy gevonden. Dachten dat dat voor de leverancier zou gelden (die moeten het leveren)

Gekeken hoe je sessies nou het beste kan beveiligen

DDoS aanval niet tegen te gaan

# 12-12-2020

Aanwezigen: Jasper, Ivar  
Notaris: Jasper

TO verder gemaakt

Besloten een gebruiker administrator te maken ipv root, omdat dit beter is voor de beveiliging. Dit moet ook in het securityverslag komen.

Onderzocht wat views zijn. Dachten dat dit best goed zou werken voor security. Blijkt uiteindelijk niks uit te maken omdat je met SQL injectie nog steeds alle tabellen van de database kan laten zien met bijvoorbeeld joins. We hebben besloten dit uiteindelijk wel te gaan implementeren, omdat het ondanks dat het niet veilig is toch een stuk langer duurt om te kraken. Dit is ook een extra punt voor in het security verslag.

We willen views gaan maken voor elk apart stukje SELECT SQL in de code van de website.

Function geeft iets terug, procedure voert iets uit, trigger roept ze aan. Voor de database willen wij een trigger maken, die vóór de UPDATE in de coldroomtemperatures tabel een procedure aanroept. Deze procedure INSERT de oude temperatuurdata in de archive tabel.

Eerste sessie: 2 uur aan gewerkt

Verschil triggers en constraints/check: constraints/check definieer je voordat je de tabel maakt. Deze gelden ook altijd wanneer er data in de tabel gezet wordt. Lijkt meer op PHP code en lijkt geen SQL te kunnen bevatten (zie voorbeeld email TO). Ook gelden deze alleen voor de rij die geINSERT wordt.

Triggers gelden alleen voor de bijbehorende regel {BEFORE/AFTER} {UPDATE/INSERT/DELETE}. Hierbij kun je ook oude data erbij halen.

We gebruiken geen transacties omdat we niks met geldoverdracht doen. Transactie: 2 of meer queries die tegelijkertijd uitgevoerd worden omdat deze niet apart uitgevoerd kunnen/mogen worden.

We waren van plan een trigger voor de postcode te maken, maar dit bleek uiteindelijk helemaal niet te kunnen. Na ongeveer 1.5 uur is het gelukt met een check constraint. De postalcode kolom in de accounttabel in hiervoor veranderd naar VARCHAR(7) vanwege de spatie.

Iets later zijn we erachter gekomen dat het nog steeds niet werkt. De constraint wordt niet aan de tabel toegevoegd (gechecked in information\_schema database). Dit komt waarschijnlijk door dat MySQL checks niet ondersteund.

Zijn er niet uitgekomen, willen dit nog na gaan vragen.

Problemen bij de andere triggers/procedures: je mag geen 2 triggers op 1 tabel hebben van mysql. Je mag geen 2 procedures callen in 1 trigger. Je mag geen 2 verschillende statements hebben in 1 procedure (INSERT en DELETE). Conclusie: we zijn nog geen stap verder. Mogelijke oplossing: voer het DELETE statement uit op de Pi. Deze moet dan wel 2 queries uitvoeren maar dan werkt hij wel.

Het inserten in de archive tabel werkt namelijk.

# 14-12-2020

Aanwezigen: Jasper, Ivar, Ana, Roy, Jan Willem  
Notaris: Jasper

Coldroomtemperatures is heel slecht gemaakt (database).

Review Securityverslag:

* Tabellen zo compleet mogelijk te maken: voeg maatregel en restrisico toe.
* Soms kost een maatregel meer dan de schade dus is het voor lief nemen ook een optie
* Meer tekst bij de maatregelen: leg het uit, wat is het?, wat is het risico? Welke maatregelen tref je?

Verder gegaan met securityverslag

* Bij alle tabellen maatregel en restrisico toegevoegd

Moeten de rest nog toevoegen

Tonen temperatuur op website: proberen het live te laten updaten zonder de website te herladen. Anders haal temperatuur op uit database en wordt pas herladen wanneer je de pagina refresht.