



TECHNISCH RAPPORT

Webprogrammeren en Databases

29 januari 2016

Student:

Sander Hansen
10995080

Jens Kalshoven
11026243

Pim Hordijk
10468528

Rico Hoegee
10707301

Frederick Kreuk
11020997

Practicumgroep:
Assembly

Docent:
Stephen Swatman, Robert Belleman

1 Introductie

Wij hebben als groep de opdracht gekregen om een webwinkel te bouwen die gemakkelijk te gebruiken en te beheren is en daarnaast ook veilig is. Dit betekent dat er een website gecreëerd moet worden waarop klanten producten van het bedrijf moeten kunnen kopen die aan een aantal eisen moet voldoen. Zo moet de website intuïtief in gebruik zijn voor zowel de klant als de beheerder.

Verder moet een klant gemakkelijk alle producten kunnen vinden. Dit hebben wij geprobeerd te bereiken door ten eerste zowel een zoekbalk voor producten, als een indeling per categorie te maken. Hierdoor kan de klant op meerdere manieren bij een bepaald product terecht komen. Verder worden op de hoofdpagina een aantal producten getoond om klanten naar deze producten te trekken.

Om het bestellen van producten voor de klant zo gemakkelijk mogelijk te maken zijn de volgende maatregelen getroffen. Als je op een product klikt krijg je bijvoorbeeld naast de beschrijving, prijs, voorraad en specificaties een bestelknop te zien. Door op deze bestelknop te drukken wordt een product aan je winkelwagen toegevoegd en bij elke druk op de knop wordt het product nogmaals toegevoegd aan de winkelwagen.

Verder kan de klant makkelijk zien welke producten hij in zijn winkelwagen heeft zonder dat hij echt naar de winkelwagenpagina gaat. Dit gebeurt via een knop in de menubalk. Als je uiteindelijk wel naar de winkelwagen gaat kan je nogmaals zien welke producten erin zitten en per product het aantal keer dat deze zich in de winkelwagen bevindt. Ook kan het aantal keer dat je een product besteld hier nog gewijzigd worden en kan een product geheel uit de winkelwagen verwijderd worden. Daarnaast kan er natuurlijk ook verder gewinkeld worden.

Als de klant wel besluit om te gaan bestellen kan hij uit twee opties kiezen, namelijk bezorgen of ophalen. Als er gekozen wordt voor ophalen kan dit gebeuren op het adres van UvA Science Park 904 en als er gekozen wordt voor bezorgen krijgt de klant weer twee opties, namelijk thuis bezorgen of op een ander adres laten bezorgen. Daarna komt de klant bij de afrekenpagina waar hij nog één maal zijn winkelwagen inhoud kan zien. Vervolgens kan de klant kiezen om te betalen of om de bestelling alsnog te annuleren.

Als de klant wel heeft betaald wordt hij geleid naar de orderpagina, waar hij zijn order kan inzien en alsnog kan kiezen om de bestelling te annuleren, mits de producten nog niet verzonden zijn. Daarnaast kan de klant hier een factuur van zijn order downloaden.

Verder is er voor de klant voldoende feedback op input die hij geeft in velden waar hij wat kan invoeren, zoals bij het wijzigen van gegevens en bij het registreren.

Ook wilden wij dat de website makkelijk was te gebruiken voor beheerders. Dit is geprobeerd door een aparte pagina te maken voor beheerders. Hier heeft hij verschillende mogelijkheden. Zo kan hij bijvoorbeeld de gegevens van alle geregistreerden bekijken en aanpassen en de gegevens van alle producten bekijken en wijzigen. Daarnaast heeft een beheerder ook de mogelijkheid om nieuwe producten toe te voegen, alle orders te bekijken en de status van elk order aan te passen.

2 Ontwerp

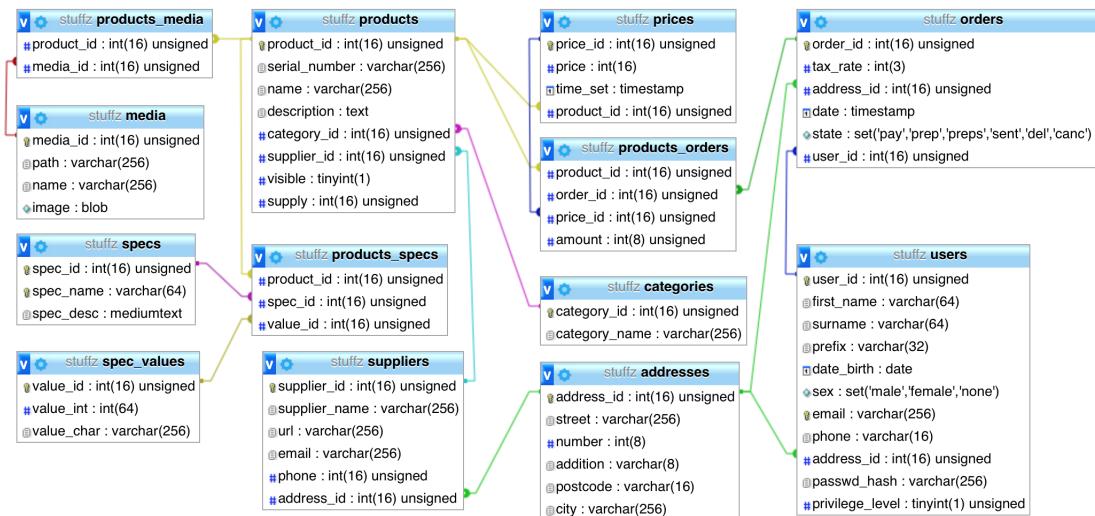
2.1 Gebruikers

In de webwinkel zijn drie gebruikersgroepen te onderscheiden:

- Niet-geregistreerde gebruikers kunnen door de producten bladeren en ze toevoegen aan de winkelwagen.
- Geregistreerde gebruikers kunnen naast het bovenstaande de artikelen in hun winkelwagen afrekenen, hun bestelgeschiedenis zien en hun gegevens aanpassen.
- Administrators kunnen naast het bovenstaande artikelen toevoegen en wijzigen, bestellingen van klanten inzien en wijzigen en gegevens van andere gebruikers inzien en wijzigen.

Bij een webwinkel is het belangrijk dat klanten en administrators goed van elkaar gescheiden zijn. Het aanpassen van de prijzen door klanten is immers enerzijds wel zeer klantvriendelijk, anderzijds ook uitermate onwenselijk. Om ervoor te zorgen dat alleen administrators toegang hebben tot de voor hen gereserveerde functionaliteiten, wordt er in de database bij de gebruikersgegevens een privilege level opgeslagen. Wanneer door een gebruiker een alleen voor administrators bedoelde pagina wordt benaderd, wordt direct vastgesteld of de gebruiker hier de benodigde rechten voor heeft door de privilege level direct uit de database op te halen en te vergelijken met het benodigde niveau voor de betreffende functionaliteit. Indien de bevoegdheden van de gebruiker niet toereikend zijn, wordt deze weggeleid van de pagina.

2.2 Databaseontwerp



Het datamodel voor een webwinkel is vrij complex. Naast tabellen voor de gebruikers zijn er ook in ieder geval tabellen nodig voor de producten en bestellingen. Dit zou echter tot veel onwenselijke niet-unieke rijsegmenten hebben geleid. Daarom zijn de tabellen zo veel mogelijk opgedeeld in kleinere tabellen.

De adressen zijn, omdat zij zowel in orders als users voorkomen afgesplitst en met een relatie aan die tabellen gelinkt.

Omdat een product gedurende zijn leven meerdere prijzen kan hebben, maar de prijzen in de bestelgeschiedenis niet mogen veranderen, is er een aparte tabel met prijzen in een

veel-op-een relatie met producten en een een-op-veel relatie met orders via linktabel products_orders. Zo blijft bij een prijswijziging de geschiedenis onaangetast.

In de tabel orders zelf wordt niets over de producten binnen de order opgeslagen, deze worden opgeslagen in de linktabel products_orders omdat het hier om een veel-op-veel relatie gaat.

Specificaties zijn vrij complex: om herhaling van specificatiedefinities te voorkomen, wordt informatie over specificaties in een aparte tabel opgeslagen van de specifikatiewaarden.

Ook de paden van de plaatjes bij producten worden niet in de productentabel opgeslagen, maar in een aparte media tabel in een veel-op-veel relatie met products. Hierdoor is het mogelijk om twee producten hetzelfde plaatje te geven, en in theorie ook om een product meerdere plaatjes te geven.

Het datamodel voldoet bijna volledig aan de derde normaalvorm, behalve bij de adressen, waarin de straatnaam en stad afgeleid zouden kunnen worden van de postcode. Verder kunnen er meerdere identieke adressen voorkomen in addresses, maar is besloten dit niet verder aan te passen, omdat de oplossing vrij veel werk zou betekenen voor een probleem dat zich in de realiteit niet snel voor zal doen.

3 Implementatie

Om code onderhoudbaar en uitbreidbaar te maken is het noodzakelijk code en de gehele codebase een structuur mee te geven waaruit valt af te lezen hoe deze is opgebouwd. Dit geldt zowel voor de structuur van individuele bestanden als voor de structuur van de bestanden samen.

3.1 Algemene bestandsstructuur

In de file tree van de source-bestanden is een structuur te vinden die als volgt valt te lezen:

Alle html die uiteindelijk geserveerd wordt aan de eindgebruiker is ingekapseld in PHP-bestanden.

Er is daarbij een scheiding aangebracht tussen PHP-bestanden die pagina's vertegenwoordigen die bezocht kunnen worden door de internetgebruiker, en PHP-bestanden die content aanleveren voor deze te bezoeken pagina's. Het verschil in de pagina's kan herkend worden aan de bestandsnaam. Internetpagina's hebben een bestandsnaam in kleine kapitalen en de bestanden die content aanleveren maken gebruik van camelCase.

De geserveerde HTML uit de PHP-bestanden aan de internetgebruiker, wordt opgemaakt middels CSS. Alle CSS-bestanden bevinden zich in een aparte map zodat deze op één plek toegankelijk zijn. Locatie: /style.

Naast HTML, bevatten sommige PHP-bestanden scripts. Ook alle scripts zijn te vinden in een aparte map, te weten: /scripts.

Queries die gedaan worden richting de database middels SQL, bevinden zich soms in de PHP-bestanden van de internetpagina's zelf, en soms in aparte bestanden. Alle queries die uniek zijn voor een internetpagina, zijn te vinden in de bestanden zelf. Alle queries die meervoudig benodigd zijn, zoals het serveren van producten uit de database bij het weergeven van categorieën en bij het weergeven van zoekresultaten, bevinden zich in aparte bestanden. De door ons ingestelde locatie hiervoor is /stools. Hetzelfde geldt voor PHP-functies die meermaals gebruikt worden.

De header en footer op elke pagina wordt aangeroepen vanuit /globalUI. Ook bevindt zich hier een bestand om een connectie op te zetten met de database en een bestand die de meest benodigde CSS-bestanden aanroeft.

De zojuist behandelde bestandsindeling voorkomt het onnodig herhalen van dezelfde code. En maakt de code beter onderhoudbaar en uitbreidbaar.

3.2 Algemene individuele bestandsstructuur

In de individuele bestanden is gekozen om zoveel mogelijk indentatie toe te passen. Dit om de leesbaarheid en toegankelijkheid te verhogen.

Om de voorgenoemde functionaliteiten in bestanden aan te roepen vanuit de internetpagina's, wordt gebruik gemaakt van het PHP include statement.

3.3 Functionaliteiten

Zoals gezegd bevinden meervoudig benodigde PHP-functies zich in bestanden te vinden in de map /stools. Middels deze logica valt dan te bepalen wat de belangrijkste queries zijn.

De belangrijkste queries bevinden zich in /stools/cartTools en /stools/orderTools. Beiden bestaan uit meerdere functies om alle benodigde informatie uit de database op te halen wanneer deze geserveerd dient te worden aan de eindgebruiker, de bezoeker van de website, of moet manipuleren om producten aan het winkelmandje toe te voegen of te bestellen.

3.4 Gebruiksgemak

Om de website gebruiksvriendelijk te maken is er een onderscheid gemaakt tussen desktopgebruikers en mobiele gebruikers. De site past zich automatisch aan wanneer deze detecteert met één van hen te maken te hebben; Vooral de grootte en uitlijning van HTML-elementen speel hierin en rol. Zo zal bijvoorbeeld de rastering van producten zich aanpassen naar een steeds meer verticale weergave naarmate het aantal verticaal beschikbare pixels minder wordt. De rastering kent verschillende niveaus dus ook een groter en kleiner wordend browserscherm op de desktop kent een optimale weergave.

Aangezien niet iedereen de beschikking heeft tot JavaScript, of JavaScript wil gebruiken, is het mogelijk om de site te bezoeken en producten te bestellen zonder JavaScript. Ook dit wordt automatisch gedetecteerd. Zo zal de header, waarin categorieën bekijken kunnen worden, gezocht kan worden op producten, of toegang kan worden verkregen tot functionaliteit betreffende de account, terugvallen op een header zonder Javascript als het niet aanwezig is. Helaas is het niet mogelijk dezelfde gebruiksvriendelijkheid te bieden zonder JavaScript. Alle functionaliteit blijft echter wel behouden.

3.5 Beveiliging

De beveiliging dient op orde te zijn om te voorkomen dat de database gemanipuleerd kan worden door derden, of dat gebruikers de dupe worden van kwaadwillenden. Wij hebben er zorg voor gedragen de volgende zaken af te dekken:

Voor alle SQL-queries wordt gebruik gemaakt van de PHP Data Objects (PDO) interface. Potentieel gevaarlijke input van de gebruiker wordt zo automatisch afgevangen door PHP en voorkomt SQL-injection.

Daar waar redirects plaatsvinden en GETs worden gedaan wordt foute input afgevangen middels de htmlspecialchars() functie. Dit voorkomt Cross-Site Scripting (XSS) aanvallen.

Om Session Hijacking te voorkomen wordt vanuit de server voor iedere bezoeker een SSL-verbinding afgedwongen. Daarmee is de communicatie tussen de client en server altijd versleuteld.

Wachtwoorden worden in de database opgeslagen middels de password_hash functie. Een cryptografische hashfunctie. Als de database ooit in verkeerde handen komt, kunnen de wachtwoorden niet uitgelezen worden. Om te voorkomen dat dezelfde wachtwoorden dezelfde hash krijgen, wordt er een salt toegevoegd. De standaard is om wachtwoorden altijd op te slaan als hash met een salt. Onze implementatie doet dit dus.

Als laatste dient vermeld te worden dat het nu voor iedereen mogelijk is om de facturen van orders op te vragen. Wanneer iemand de volgende URL in de adresbalk intypt:

`stuffz.nl/factuur.php?order_id=xx`

Waar xx een bestaande id is, wordt ongeacht of deze factuur voor de opvrager bedoeld is, de factuur weergegeven.

Dit is niet de bedoeling en daar zijn wij ons van bewust. Wij zijn echter niet in staat geweest om dit probleem voor de deadline op te lossen. Benadrukt dient te worden, dat het geen noodzakelijke functionaliteit betreft en dus uitgezet kan worden. Zie ook het hoofdstuk discussie.

3.6 Gebruikers en login

In een website voor een webwinkel is het belangrijk om een goede scheiding te hebben tussen klant en administrator. Dit is bereikt door het opslaan van een privilege level bij de gebruikersgegevens. Een reguliere klant heeft hierbij privilege level 0, administrators hebben hogere privileige levels. In totaal zijn er 9 niveaus

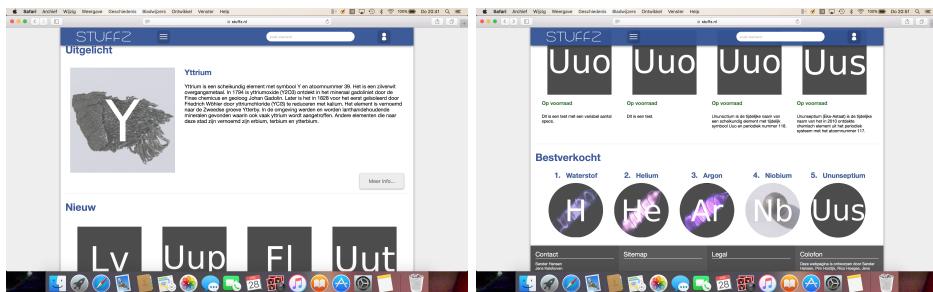
4 Resultaten

Na weken hard gewerkt te hebben, is het ons uiteindelijk gelukt om een mooi resultaat neer te zetten.

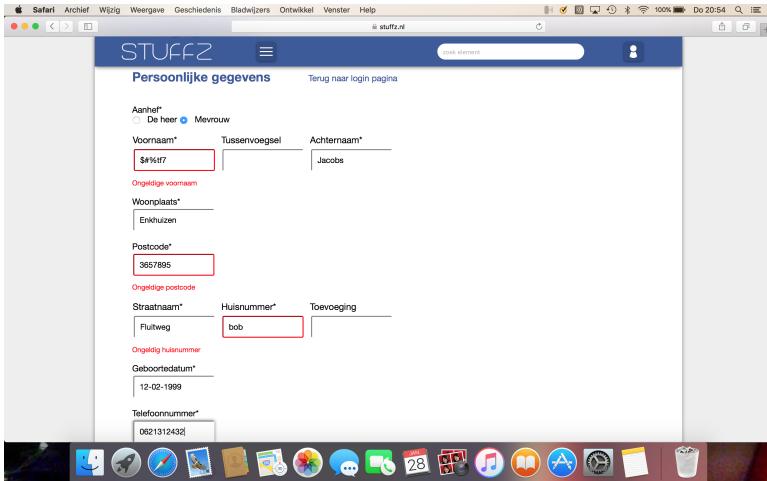
Elke pagina is voorzien van een mooie header die meebeekt als de gebruiker door de pagina scrollt. Deze header bevat een zoekbalk, een knop (het logo) waar als de gebruiker erop drukt de gebruiker naar de hoofdpagina gaat en twee knoppen die uitklappen in menus.



De hoofdpagina bestaat uit drie delen: Een uitgelicht artikel, de nieuwste artikelen in het assortiment en de 5 populairste artikelen. Al deze artikelen en hun gegevens worden uit de database gehaald.



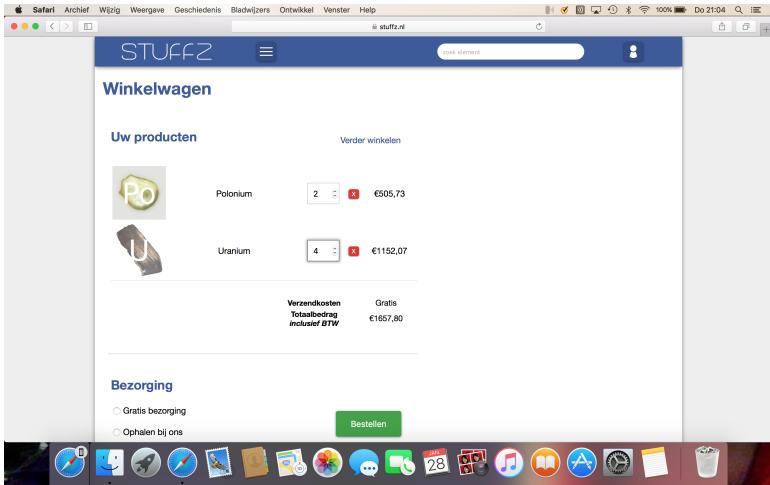
Bij het registreren staat duidelijk vermeld welke gegevens verplicht zijn en welke niet. Als een gegeven fout is ingevuld, wordt dit vermeld. Als alle gegevens goed zijn, wordt de gebruiker met gegevens in de database gestopt. Als de gebruiker zijn gegevens wil wijzigen, zal de pagina vrijwel hetzelfde zijn, alleen zijn dan de gegevens al ingevuld waarmee de gebruiker zich heeft geregistreerd.



Op de productpagina kan de gebruiker lezen wat voor product het is. Hier staat ook bij of het product op voorraad is en hoeveel het kost. Ook kan hier het product aan het winkelwagentje worden toegevoegd. Als het product niet op voorraad is, dan is de "Voeg toe" niet meer aanwezig.

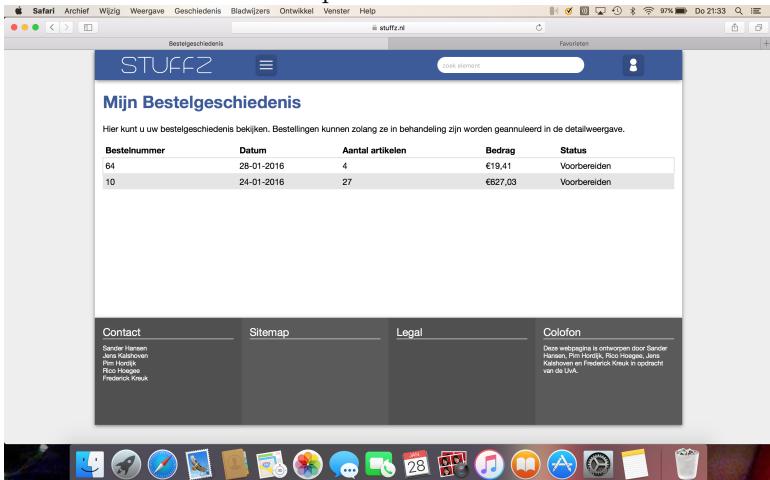


In de winkelwagen is overzichtelijk te zien welke artikelen aan de winkelwagen zijn toegevoegd, ook zijn het subtotaal en eindtotaal te zien. Verder kan de gebruiker het aantal per artikel aanpassen. Als dit gebeurt, worden automatisch het betreffende subtotaal en eindtotaal aangepast. Als de gebruiker tevreden is met de bestelling, kan hij de bestelling afronden. Tussendoor heeft de gebruiker nog de mogelijkheid om een alternatief afleveradres aan te geven.



The screenshot shows a shopping cart page for 'Stuff2'. At the top, there's a navigation bar with links like 'Safari', 'Archief', 'Wijzig', 'Weergave', 'Geschiedenis', 'Bladwijzers', 'Ontwikkel', 'Venster', and 'Help'. The main content area has a blue header 'Winkelwagen' (Shopping Cart). Below it, under 'Uw producten', there are two items: 'Polonium' (2 units, €505,73) and 'Uranium' (4 units, €1192,07). A summary row shows 'Verzendkosten' (Shipping costs) as 'Gratis' (Free), 'Totaalbedrag' (Total amount) as '€1657,80', and 'inclusief BTW' (including VAT). Under 'Bezorging' (Delivery), there are two options: 'Gratis bezorging' (Free delivery) and 'Ophalen bij ons' (Pick up at our location). A green 'Bestellen' (Order) button is located at the bottom right of this section.

De gebruiker kan ook zijn bestelgeschiedenis bekijken. Hier is overzichtelijk te zien wat de gebruiker wanneer heeft besteld. Ook kan vanaf hier de factuur van de bestelling bekijken worden. Deze factuur is in pdf formaat.

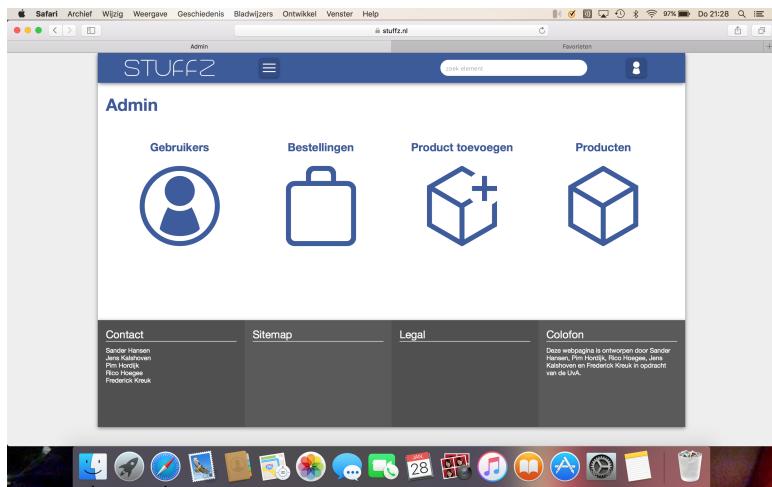


The screenshot shows the 'Bestelgeschiedenis' (Order History) page for 'Stuff2'. The top navigation bar is identical to the shopping cart page. The main content area has a blue header 'Mijn Bestelgeschiedenis'. Below it, a message says: 'Hier kunt u uw bestelgeschiedenis bekijken. Bestellingen kunnen zolang ze in behandeling zijn worden getoond in de detailweergave.' (Here you can view your order history. Orders that are still being processed will be shown in detail view.) A table lists two recent orders:

Bestellenummer	Datum	Aantal artikelen	Bedrag	Status
64	28-01-2016	4	€19,41	Voorbereiden
10	24-01-2016	27	€627,03	Voorbereiden

At the bottom of the page, there are links for 'Contact', 'Sitemap', 'Legal', and 'Colofon'. The footer contains copyright information: 'Dit werk is uitgevoerd door Sander Hansen, Jens Kalshoven, Pim Hordijk, Rico Hoegee, Jeroen Kuijper en Frederick Kreuk in opdracht van de UvA.'

De adminpagina is alleen beschikbaar voor gebruikers met een hoog genoeg privilege level (dit level is opgeslagen in de database). Voor een gebruiker met een te laag privilege level is de admin knop niet zichtbaar. In de adminpagina kan de gebruiker kiezen om gebruikergegevens te wijzigen, bestellingen aan te passen en producten toe te voegen of aan te passen. Het aanpassen van gebruikergegevens ziet er vrijwel hetzelfde uit als de pagina waarop een gebruiker zijn eigen gegevens kan aanpassen. Ook kan de admin de bestellingen per gebruiker zien en kan hij de facturen van deze bestellingen bekijken.



Op de product-toevoegen-pagina kan de admin een product toevoegen. Net als bij het registreren wordt er bij elke input gekeken of het van het juiste formaat is en een foutmelding gegeven als dit niet zo is. De admin kan ook een variabel aantal specificaties aan het product toevoegen. Deze functie is zo geïmplementeerd zodat dit geen lege specificatie rijen oplevert in de database. Ook kan vanaf hier als dat gewenst is een nieuwe categorie worden aangemaakt waarin het nieuwe product zal komen. Het categoriemenu zal hierop dan automatisch worden aangepast, aangezien de categorieën (net zoals alle andere gegevens) uit de database worden gehaald.

The screenshot shows the 'Producten toevoegen' (Add Product) form. The page title is 'STUFFZ Admin'. The form fields include 'Naam' (Name) with an input field, 'Beschrijving' (Description) with a text area, and 'Specificaties' (Specifications) with three input fields for density values: 'Dichtheid kg*m^-3' with value '12,55', 'Dichtheid kg*m^-3' with value '12,55', and 'Dichtheid kg*m^-3' with value '12,55'. There are also green '+' and red '-' buttons for adding or removing specification rows.

5 Bronvermelding

Voor het maken van de factuur hebben we gebruik gemaakt van wkhtmltopdf dit is een command line tool to html pagina's om kan zetten naar pdf. Deze command line tool hebben we geïnstalleerd op onze server en is te verkrijgen via;
<http://wkhtmltopdf.org>.

Verder hebben we een random string generator gebruikt die we van internet hebben gehaald. Deze bron staat ook in de code vermeld;
<http://stackoverflow.com/questions/4356289/php-random-string-generator>

Daarnaast hebben voor enkele regexen gebruik gemaakt van:
<http://molenaar-technologies.nl/regex-op-zn-nederlands/>

En voor het uploaden van afbeeldingen hebben we gebruik gemaakt van:
http://www.w3schools.com/php/php_file_upload.asp

Verder hebben we wel veel inspiratie en hulp gehad van het 'internet'. Dit waren echter geen grote belangrijke stukken die we letterlijk hebben overgenomen.

6 Discussie

De functionaliteit die we van te voren gepland hadden voor onze webshop is in principe volledig geïmplementeerd. Een klant kan registreren, producten toevoegen aan zijn of haar winkelmandje en deze vervolgens bestellen. Een admin kan producten toevoegen, bestellingen wijzigen en gebruikersgegevens bekijken en aanpassen.

Alle functies die we voor ogen hadden hebben we dus werkend gekregen en verder hebben we veel extra functionaliteit toegevoegd. Zo hebben we de specificaties flink uitgebreid en kunnen we pdf facturen aanmaken.

Als we achteraf terugkijken naar het project hadden we wel een aantal dingen anders kunnen doen. De manier waarop we het ontwerp van de website aangepakt hebben was ideaal. Ieder heeft zijn eigen html geschreven en de styling is in principe centraal gedaan. Doordat vervolgens door iedereen de stijl op door hen geschreven pagina's aangepaste om overeen te komen met het basis design, kregen we uiteindelijk een uniforme stijl. Toen we met databases aan de slag gegaan zijn heeft iedereen in principe zijn eigen queries geschreven.

Een aantal van ons deden dit in de bestanden zelf en het andere deel deed dit in aparte PHP bestanden met functies die aangeroepen konden worden. Als we dit van te voren hadden geweten hadden met elkaar af kunnen spreken om slechts een van deze implementatie vormen toe te passen, waardoor de code wellicht wat overzichtelijker was geworden. Toch is dit op dit moment redelijk opgelost door commentaar toe te voegen.

Doordat een groot deel van de queries in functies zijn geschreven is de functionaliteit gemakkelijk uit te breiden. In de ideale situatie zouden we alle queries in functies plaatsen zodat functionaliteitRt nog gemakkelijker uit te breiden is, helaas kwamen we hier pas laat achter omdat we niet genoeg voorkennis hadden om dit te voorzien.

Toen we praktisch klaar waren met de basis functies zijn we extra functies gaan implementeren. Helaas hebben we deze niet allemaal volledig afgekregen. Toch hebben we er bewust voor gekozen om bijvoorbeeld de factuur wel aan de master branch toe te voegen. De beveiliging hiervan is op dit moment verre van ideaal maar buiten dat om werkt het PDF factureringsysteem wel.