# Processen en functies

## Rolsysteem

Niet alle rollen hebben dezelfde rechten, om te voorkomen dat iemand zonder rechten iets kan doen met rechten, moet er overal gecontroleerd worden of de rol gelijk is aan de rol die toegang heeft.

Dit om te voorkomen dat een gebruiker acties kan doen die eigenlijk alleen de administrator hoort te kunnen doen.

## Inloggen

Gebruikers hebben de mogelijkheid om in te loggen op de applicatie. Bij het inloggen worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Beveiliging van het formulier(SQL Injection, Brute force, cross-site-scripting).
* Controleren of de ingevulde gegevens gelijk staan aan een record in de database.
* Foutmelding, bijvoorbeeld: U heeft bepaalde gegevens niet ingevuld.
* Status boodschap doorgeven, bijvoorbeeld (0 niet ingelogd, 1 wel ingelogd).

## Registreren

Mensen die nog niet geregistreerd staan kunnen een account aanmaken om vervolgens in te kunnen loggen in de webapplicatie. Bij het registreren worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Beveiliging van het formulier(SQL Injection, Brute force, cross-site-scripting).
* Controleren of de ingevulde gegevens niet gelijk staan aan een record in de database.
* Foutmelding, bijvoorbeeld: U heeft bepaalde gegevens niet ingevuld.
* Een formulier met de velden als volgt: Voornaam, achternaam, geboortedatum, woonplaats, postcode, telefoonnummer, email-adres, wachtwoord, bevestig wachtwoord, gebruikersnaam.
* De ingevulde gegevens van de gebruiker worden in de database opgeslagen.

## Wachtwoord vergeten

Gebruikers die hun wachtwoord vergeten zijn kunnen deze opnieuw opvragen. Deze opvraging word via de mail verzonden naar het geregistreerde e-mailadres van het account. Hierbij worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Beveiliging van de invoer(SQL Injection, Brute force, cross-site-scripting).
* Een invoer met het veld: E-mailadres.
* Bevestigingspop-up, om zeker te weten dat een persoon zijn of haar e-mail correct heeft ingevuld. (dit alsnog vergelijken met e-mail uit de database, of deze mail bestaat). Als niemand bijvoorbeeld een e-mailadres heeft geregistreerd heeft met bijvoorbeeld @gmail.com, dan komt er een foutmelding waarin staat, controleer uw e-mailadres.
* Een niet spambare knop, zodat een persoon niet iemand zijn/haar mailbox vol kan gooien met wachtwoord vergeten mailtjes.
* Er word een mail verzonden naar het geregistreerde account met het opgegeven e-mailadres waarbij de ontvanger zijn of haar wachtwoord kan resetten.

## Een product toevoegen

De verkoper kan een product op de webapplicatie zetten. Hierbij worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Beveiliging van het formulier(SQL Injection, Brute force, cross-site-scripting).
* Een formulier met de velden als volgt: Naam, beschrijving, minimum bod, status, einddatum, foto.
* Ingevoerde product gegevens in de database opslaan.
* De invoervelden worden gecontroleerd op illegale tekens, denk hierbij aan letters bij het veld: €prijs

## Een product verwijderen

De verkoper en de administrator kunnen een product verwijderen. Hierbij worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Het product word verwijderd uit de database.
* Er komt een pop-up met een vraag naar bevestiging.

## Een product wijzigen

De verkoper en de administrator kunnen een product wijzigen. Hierbij worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Een formulier met de velden als volgt: Naam, beschrijving, minimum bod, status, einddatum, foto, deze velden worden automatisch ingevuld als de huidige velden, zodat deze velden niet ALLEMAAL opnieuw moeten worden getypt als bijvoorbeeld alleen de prijs aangepast hoeft te worden.
* Beveiliging van het formulier(SQL Injection, Brute force, cross-site-scripting).
* De oude gegevens in de database worden overschreven met de nieuwe gegevens uit de ingevulde invoer.
* Er komt een pop-up met een vraag naar bevestiging.
* De invoervelden worden gecontroleerd op illegale tekens, denk hierbij aan letters bij het veld: €prijs

## Op een product bieden

De gebruiker kan op een product bieden. Hierbij worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Beveiliging van de invoer(SQL Injection, Brute force, cross-site-scripting).
* Een invoer met een prijsveld.
* Er worden bieding gegevens in de database opgeslagen(gebruiker id, product id).
* De invoervelden worden gecontroleerd, denk hierbij aan een foutmelding die voorkomt wanneer er €999999 geboden word op een product.
* De gebruiker krijgt een mailbevestiging waarin word gezegd dat de bieding is geplaats.
* Zodra de gebruiker niet meer het hoogste bod heeft, word er een mailtje gestuurd waarin staat dat de gebruiker niet meer het hoogste bod heeft.

## Een bieding wijzigen

De verkoper en de administrator kunnen een bieding wijzigen via het overzicht biedingen. Stel dat er contact opgenomen word omdat er per ongeluk een verkeerd bedrag is ingevoerd. Kan deze informatie gewijzigd worden. Bij het wijzigen van biedingen worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Beveiliging van de invoer(SQL Injection, Brute force, cross-site-scripting).
* Een invoer met het veld: Prijs.
* De oude prijs in de database worden overschreven met de nieuwe prijs uit de ingevulde invoer.
* Er komt een pop-up met een vraag naar bevestiging.
* Het invoerveld moet worden gecontroleerd op illegale tekens, denk hierbij aan letters bij het veld: €prijs.
* De gebruiker krijgt een mailbevestiging waarin word gezegd dat de bieding is gewijzigd.

## Een bieding verwijderen

De verkoper en de administrator kunnen een bieding verwijderen via het overzicht biedingen. Stel dat een gebruiker per ongeluk op het verkeerde product heeft geboden of zijn bieding wil annuleren kan dat. Hierbij worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Een pop-up met vraag naar bevestiging.
* De bieding gegevens worden verwijderd uit de database.
* De gebruiker krijgt een mailbevestiging waarin word gezegd dat de bieding is geannuleerd.

## Een bieding winnen

Als een gebruiker heeft geboden op een product en het biedbedrag is de hoogste zodra de timer op 00:00 staat. Heeft deze gebruiker gewonnen bij het winnen van een bieding worden meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* De gebruiker krijgt een mailbevestiging waarin word gezegd dat deze gebruiker de bieding heeft gewonnen, hierbij word ook een link naar de betaling gestuurd.
* Het product wordt verwijderd uit de database.
* De bieding gegevens van de winnaar van de bieding blijft opgeslagen totdat de betaling is voldaan. Dan worden de gegevens verwijderd.

## Betaling

Zodra een gebruiker een bod heeft gewonnen krijgt deze persoon een mail, in deze mail staat een link naar de betaling, als deze gebruiker gaat betalen worden er meerdere functionaliteiten uitgevoerd, deze zijn als volgt:

* Er word een nieuwe pagina geopend met de betalingsmogelijkheden.
* Zodra de betaling is gelukt komt worden de bieding gegevens verwijderd, het product word voor het gebruikersoverzicht op onzichtbaar gezet, maar voor de verkoper staat het product nog steeds in het overzicht. Stel de verkoper heeft nog een product zoals deze hoeft er bijvoorbeeld niet vier keer hetzelfde product worden aangemaakt.