Opdracht 1 – Jentse Vander Hulst

Opdracht : Account registeren op juiceshop met een reguliere username die geen email is.

Graphical user interface, text

Description automatically generatedTools : Burp suite  
  
Testen van het registeren met een gewone naam zonder email:

Dit blijkt niet te werken want er is effectief validatie op het form dat ons verplicht een soort van email in de username te zetten. We weten dus al dat er client validatie is.

Als we wel een geldig email invoeren dan kunnen we ons gaan registeren.

Graphical user interface, application

Description automatically generated

Als we op de registratie knop klikken en dit pakketje gaan intercepten met Burp suite zien we onze POST request naar de website. Hierin zien we ook de gegevens die we hebben ingevoerd in plain tekst vanonder.

Text

Description automatically generated

A screenshot of a computer

Description automatically generatedWe zouden nu de waarde van onze “email” kunnen aanpassen naar een naam die we willen en dit doorsturen naar de server en kijken of dit effectief registreert. Ik pas voor mijn voorbeeld nu de email aan naar JentseVanderHulst en forward dit pakketje naar de server om te kijken of het lukt.

Als we na het sturen van ons pakketje nog blijven intercepten en wat door klikken op de antwoorden van de server zien we uiteindelijk ook een antwoord met een UserID tevoorschijn komen.

A screenshot of a computer

Description automatically generated with medium confidence

We hebben als UserID 24 gekregen we zien hier ook het antwoord van onze security question, onze user zou dus moeten geregistreerd zijn met de naam JentseVanderHulst.

Ik probeer vervolgens dus aan te melden met de username JentseVanderHulst om te testen of het effectief gelukt is de user te registeren met een “foute” naam.

Graphical user interface, application

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidenceEn dit is ook gelukt, onze username is JentseVanderHulst zonder iets van email in de naam, er is dus blijkbaar geen server side validatie op de usernames die binnenkomen. Enkel client side is er een validatie die checkt of de username op een email lijkt.