

Opdracht 1 – Jentse Vander Hulst

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

Tools : Burp suite

Testen van het registreren met een gewone naam zonder email:

The screenshot shows a 'User Registration' form with the following fields and elements:

- Email ***: Contains the text 'jentse'. A red border highlights the field, and a red error message 'Email address is not valid.' is displayed below it.
- Password ***: Contains masked characters '.....'. A mouse cursor is hovering over the field. Below the field, a hint says 'Password must be 5-40 characters long.' and a character count '9/20' is shown.
- Repeat Password ***: Contains masked characters '.....'. A character count '9/40' is shown.
- Show password advice**: A toggle switch is turned on, revealing a list of requirements:
 - ✓ contains at least one lower character
 - ✓ contains at least one upper character
 - ✓ contains at least one digit
 - ✓ contains at least one special character
 - ✓ contains at least 8 characters
- Security Question ***: A dropdown menu with the selected option 'Name of your favorite pet?' and a downward arrow.
- Answer ***: Contains the text 'Rusty'. A hint below the field says 'This cannot be changed later!'.
- Register**: A button with a user icon and the text 'Register'.
- Already a customer?**: A link at the bottom of the form.

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 registreren.

User Registration

Email *
jentse@randomemail.com

Password *
.....

🔔 Password must be 5-40 characters long. 9/20

Repeat Password *
.....

9/40


☒ Show password advice

- ✓ contains at least one lower character
- ✓ contains at least one upper character
- ✓ contains at least one digit
- ✓ contains at least one special character
- ✓ contains at least 8 characters

Security Question *
Name of your favorite pet? ▼

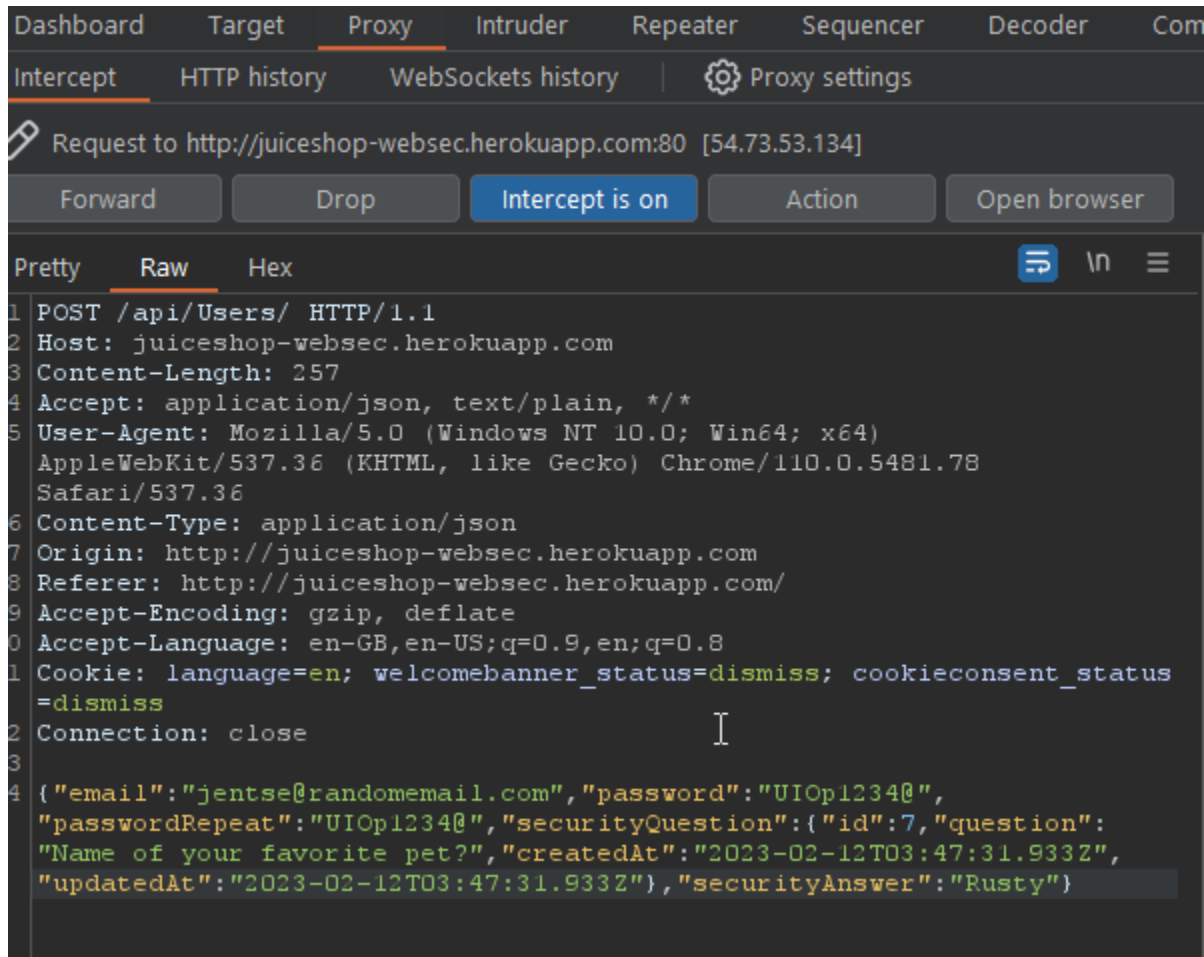
🔔 This cannot be changed later!

Answer *
Rusty

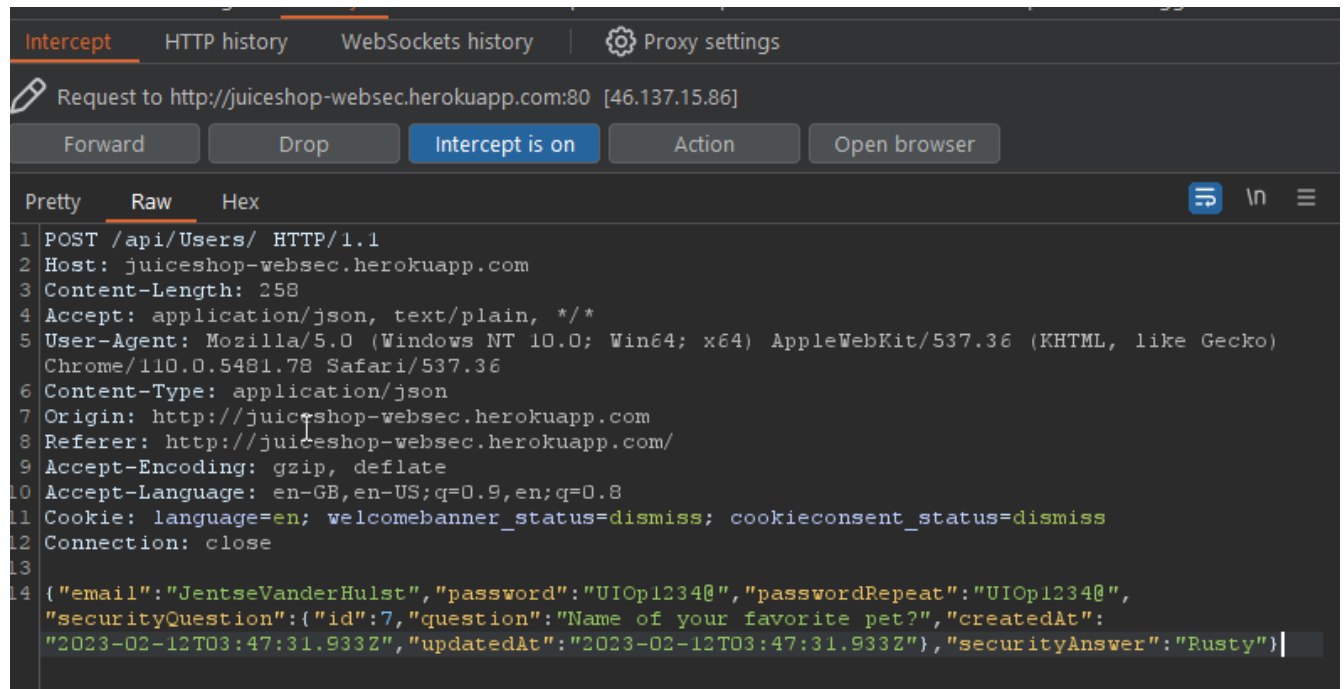
 Register

[Already a customer?](#)

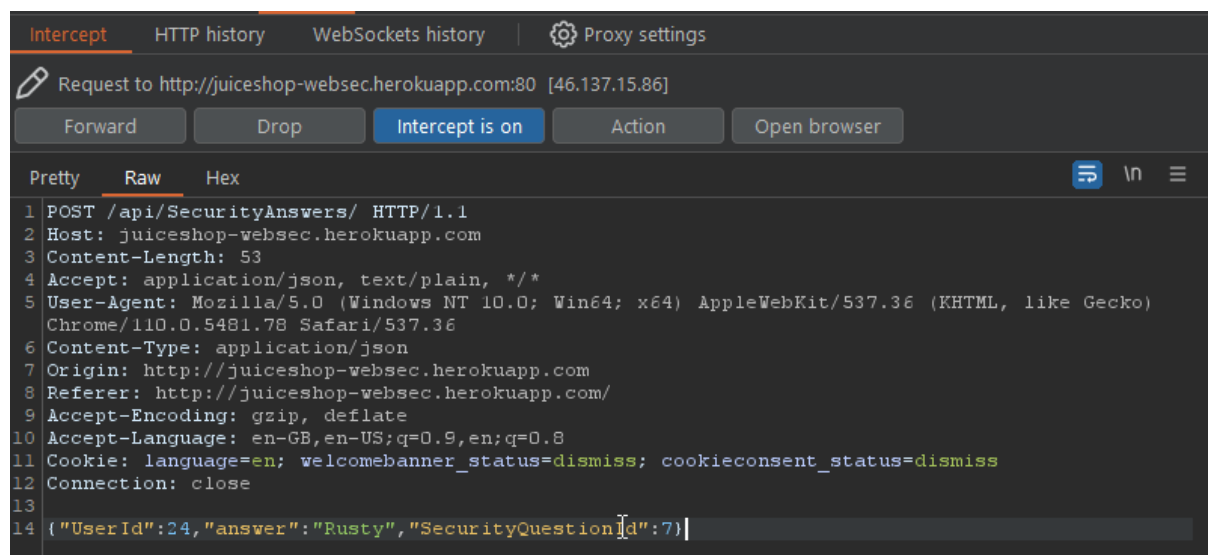
Als we op de registratie knop klikken en dit pakketje gaan intercepten met Burp suite zien we onze POST request naar de website. Hierin zien we ook de gegevens die we hebben ingevoerd in plain tekst vanonder.



We 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.

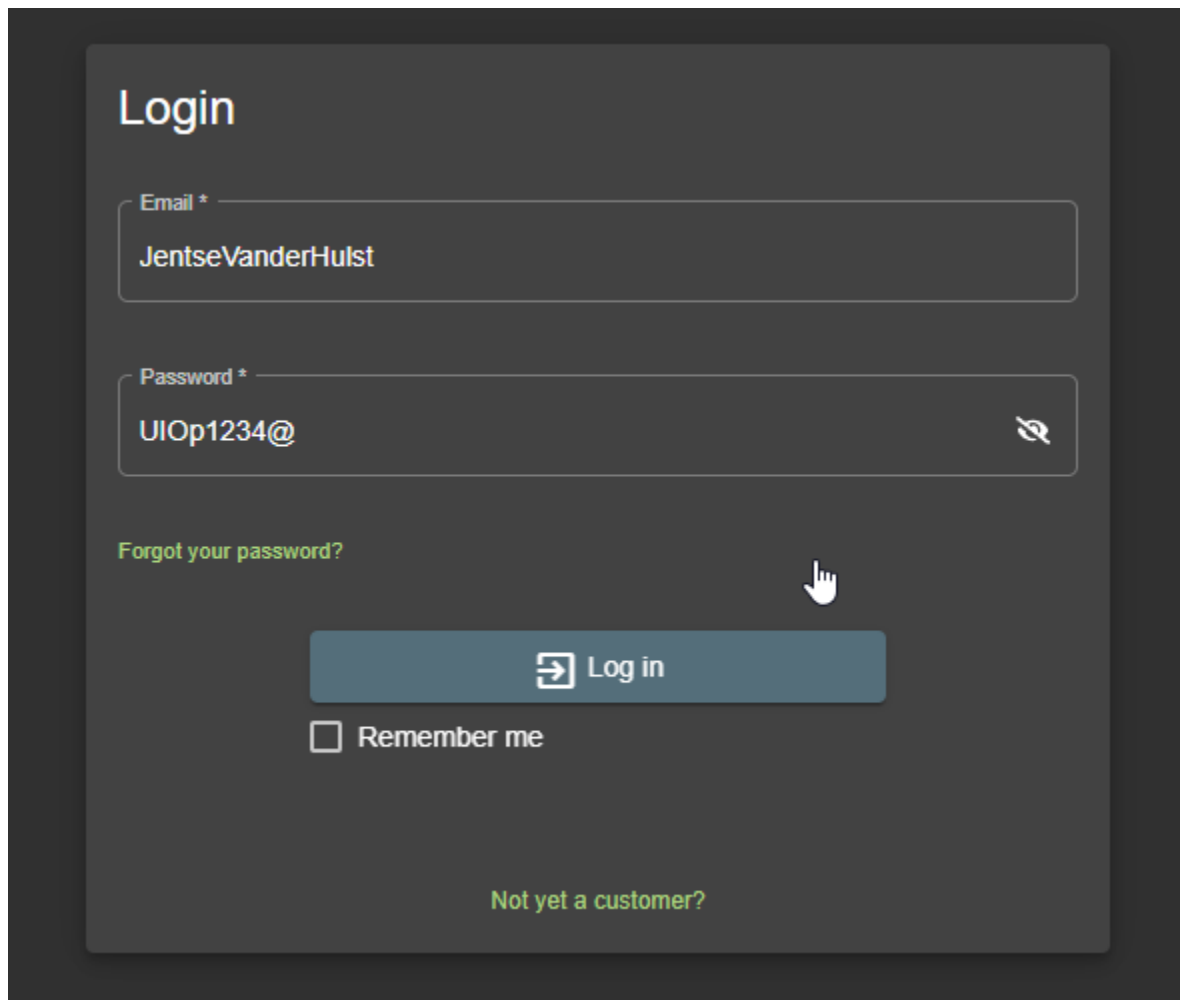


Als we na het sturen van ons pakketje nog blijven intercepten en wat door klikken op de antwoorden van de server zien we uiteindelijk ook een antwoord met een UserID tevoorschijn komen.



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 registreren met een “foute” naam.


A login form on a dark background. The form has a title 'Login' in white. Below it are two input fields: 'Email *' containing 'JentseVanderHulst' and 'Password *' containing 'UIOp1234@'. The password field has a toggle icon on the right. Below the password field is a link 'Forgot your password?' in green. A white hand cursor is pointing at the 'Log in' button, which is a teal rectangle with a white arrow icon and the text 'Log in'. Below the button is a checkbox labeled 'Remember me'. At the bottom of the form is a link 'Not yet a customer?' in green.

Login

Email *
JentseVanderHulst

Password *
UIOp1234@

[Forgot your password?](#)


 Log in

☐ Remember me

[Not yet a customer?](#)

En 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.

User Profile



Email:
JentseVanderHulst

Username:
e.g. SuperUser

Set Username

File Upload:

Choose file No file chosen

Upload Picture

or

Image URL:
e.g. https://www.gravatar.com/avatar/7e98d1a4abc11c780bd4c39137e5fee

Link Image