Juvan Thavalingam, Christian Graber

Task 2:

1. Download txt with usernames in a file
2. Open Login Screen and Start Burp
3. Give random username and password
4. Go to Burp and send the login request to Intruder
5. By Positions: Set the Attack Type to: Cluster bomb
6. Mark the username and password like this: username=§astro-officer§&password=§DarkSide2021§, you can achieve this with the button add
7. Go to payloads: Set the payload to 2
8. Payload 1: Set the simple list with the txt file, you downloaded in point 1
9. Payload 2: Set the simple list with the single input “DarkSide2021”
   So we have 46 iterations because we have 46 different username and only one password
10. Click on Start attack!
11. Watch on the length, if you see an outlier, then this might the username!
    The outliers are vader, jabba, tarkin! Vader has a length of 341 and a Status code: 302!
    Jabba and tarkin have a length of 2752.
    The rest has a length of 2750.
12. Test this by login: Username = ‘vader’ / Passwort = ‘DarkSide2021’ -> Welcome to the Dark Side, vader!
13. The response I got by ‘jabba’ and ‘tarkin’ with the password DarkSide2021 is: “Wrong password.”
14. The response by the other “users” is: “Unknown username.”

So: Jabba and tarkin are valid usernames but their password isn’t ‘DarkSide2021’!
vader has the password ‘DarkSide2021’!