The test case below describes the steps to conduct a brute force password cracking attack.

In the previous step (files/emailOnHomepage.pdf), I found user's logins, e.g. admin. Now, knowing the correct username, I will want to find his password. I will use the brute force attack to crack passwords using Burp Suite - Intruder.

Step	Expected behavior	Result (pass/fail)
Open https://juice-shop.herokuapp.com/#/search in the browser built into Burp Suite - Chromium	Page https://juice-shop.herokuapp.com/#/search is visible in Chromium	
Click on Account icon in Right top corner	Log in Menu appear	
Click on arrow near Log in	The login form is visible	
In e-mail field enter:admin@juice-sh.op	In e-mail field admin@juice-sh.op is entered	
In password field enter: 1234	In password field 1234 is entered	
Click „Log in" Button	„Invalid email or password" message is visible	
Go to Burp Suite - Proxy Tab - HTTP History Tab - search for Request POST /rest/user/login HTTP/1.1	POST /rest/user/login HTTP/1.1 Is visible on list	
Right-click on this request and select „Send to Intruder"	POST /rest/user/login HTTP/1.1 is visible in Intruder Tab	
Select the value of the password key (in our case 1234) and click the button „Add §"	The value of the password key (in our case 1234) is highlighted	
Select „Sniper attack"	„Sniper attack" is selected	
In Payloads Tab - Payload type - choose „Simple list"	„Simple list" is selected	
Copy the contents of the dictionary attached to this task and paste it using the "paste" button in the Payloads tab. *When I tested the juice shop, I used a more extensive dictionary. To speed up the tests, I reduced the content of the dictionary*	The content of the dictionary is visible in the list	

Step	Expected behavior	Result (pass/fail)
Click „Start attack”	A window with the message that the Community Edition of Burb Suite contains a demo version of Intruder appeared.	
Click „Ok” on window and go to New Open Window with Intruder attack	List of Results with Status code is visible.	
Search for status code = 200	One password have status code 200 - admin123	
Go to Chromium - login window Enter correct Login (admin@juice-sh.op) and Password (admin123)	Correct Login (admin@juice-sh.op) and Password (admin123) are entered	
Click „Log in” Button	You are correctly logged in as administrator	

Dictionary:

123456
password
12345678
qwerty
111111
qwertyuiop
1234567890
Admin
Admin12
Admin123
Admin1234
Admin1245
Administrator
superman
1qaz2wsx
121212
000000
qazwsx
123qwe
zxcvbnm
asdfgh
computer

To protect applications against password cracking using the brute force attack, I would suggest the following Improvement:

Title: Add a temporary login lock after 3 failed login attempts
Priority: Medium

ENVIRONMENT:
https://juice-shop.herokuapp.com/#/search
Production

BROWSER / Mobile OS Version:
Chromium Wersja 132.0.6834.84
Windows 11

STEPS TO REPRODUCE:
Crack the administrator password using Burp Suite Intruder (steps in tabele above)

CURRENT BEHAVIOR:
You can break a password using the brute force attack - by sending many requests and checking a popular entry from the dictionary as a password.

EXPECTED BEHAVIOR:
Add a temporary login lock after 3 failed login attempts (Block a given IP address).
This will make the attack longer and more difficult.

ADDITIONAL INFORMATIONS: