Username enumeration via subtly different responses

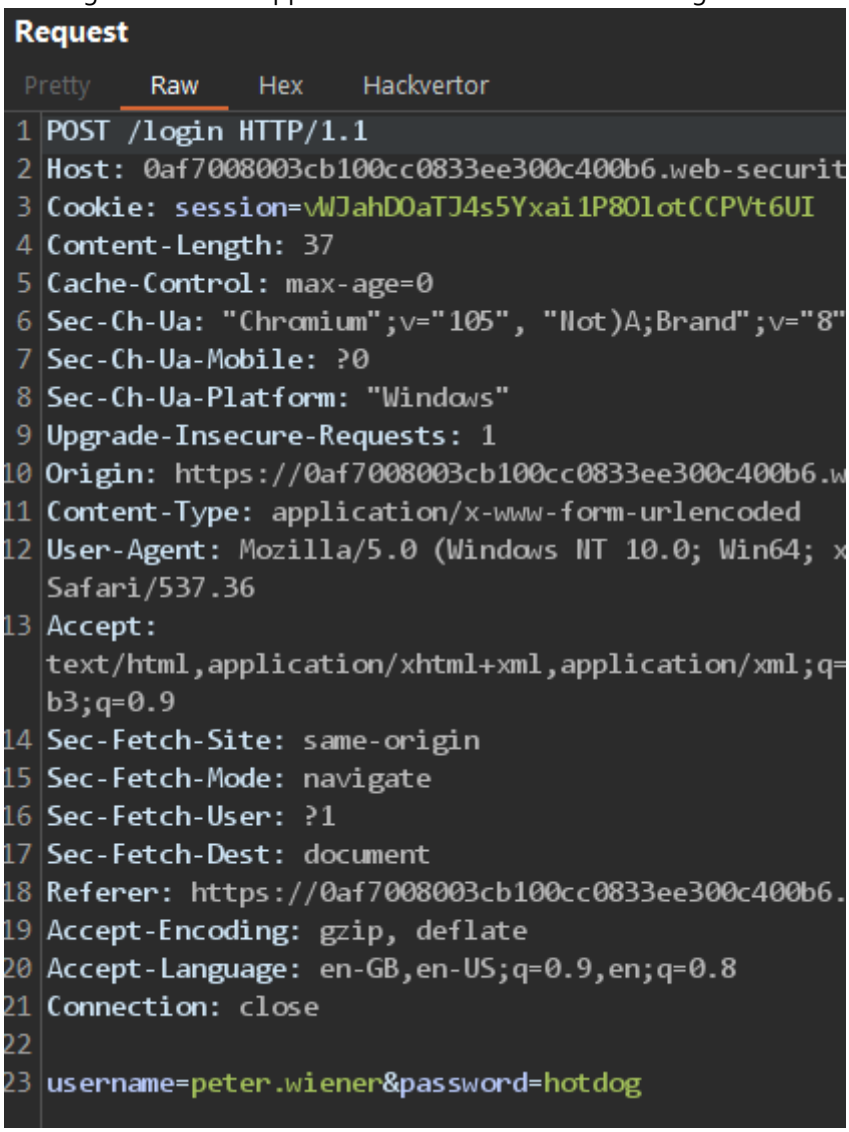
This lab is subtly vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- Candidate usernames
- Candidate passwords

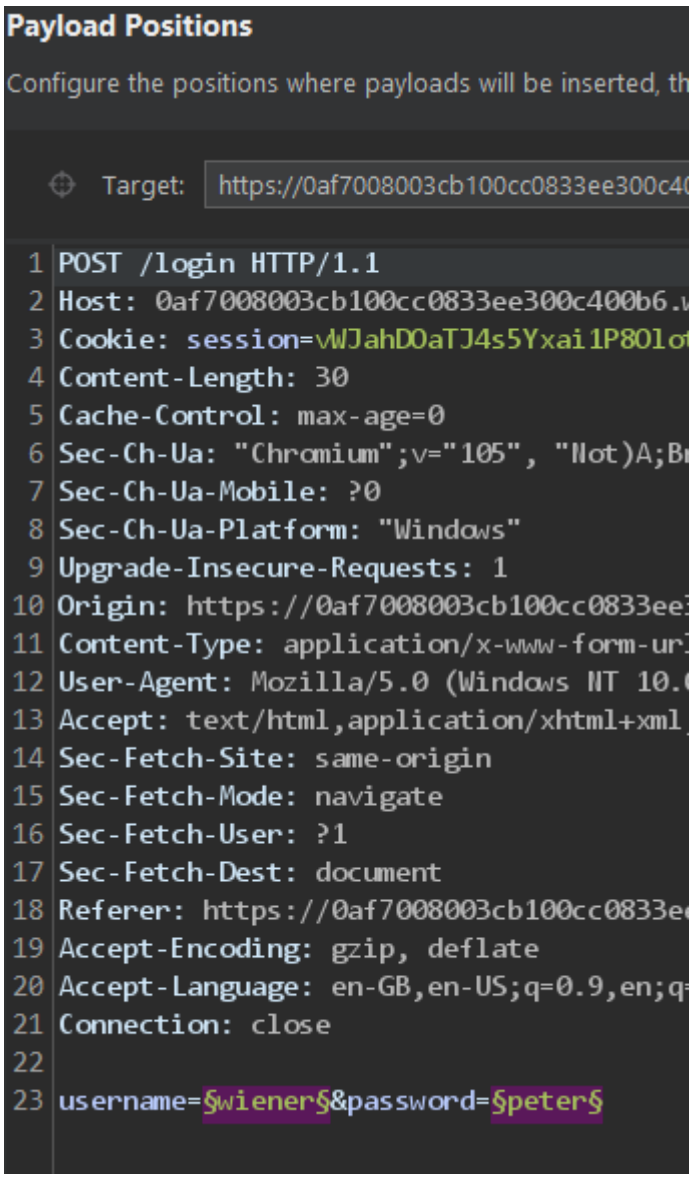
To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

Send login form to repeater to play around and find the subtle difference

Nothing from the webapp side is obvious in the error message so it must be in the backend

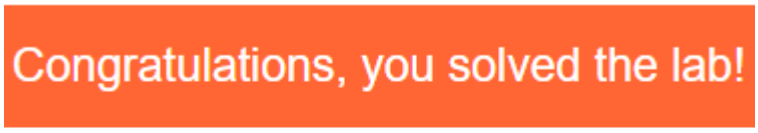


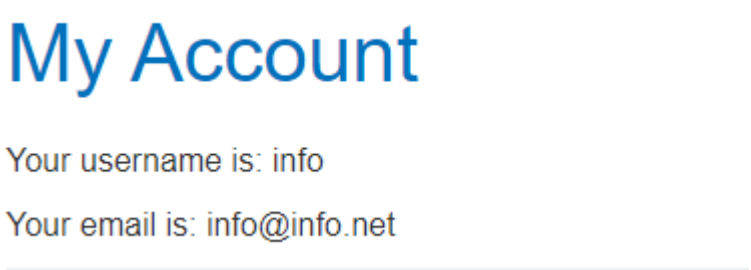
Not seeing much difference I went YOLO on clusterbomb



Username INFO generates a re-direct

Log in to complete

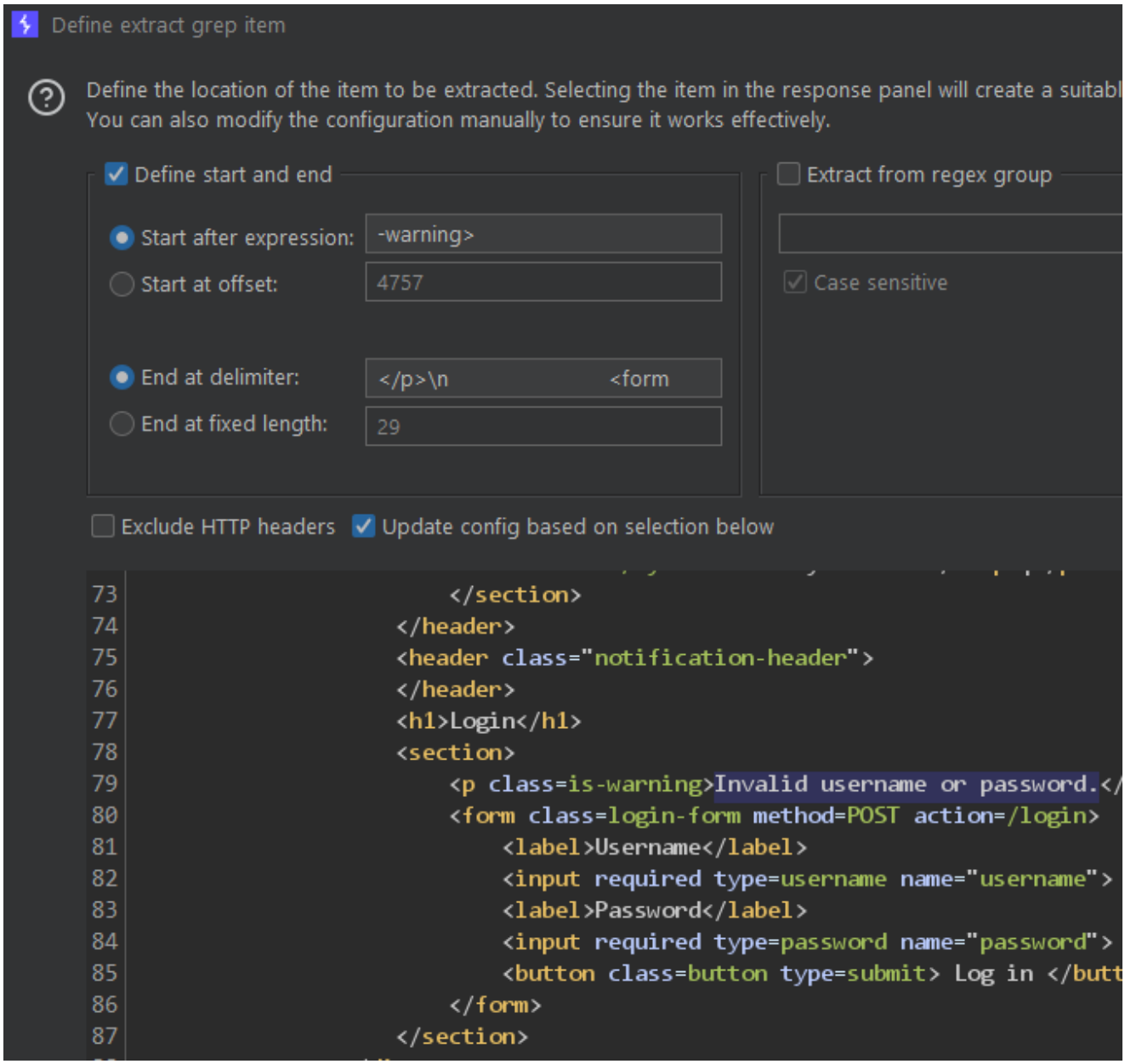




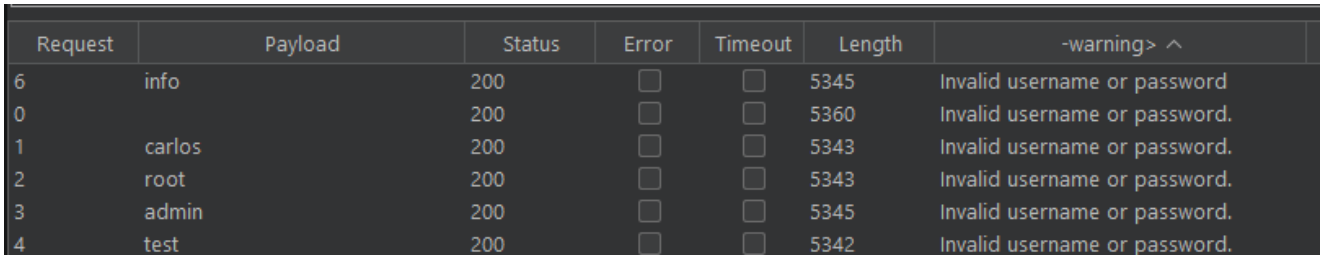
Following the guide

Obviously this lab is about subtely different response so working through the lab we get these steps.

Click fetch and highlight the error message

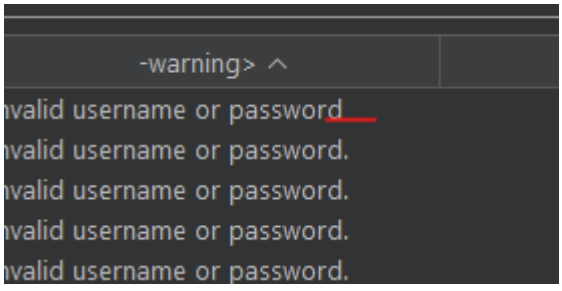


Start the attack and ascend the results to reveal the subtely



Request	Payload	Status	Error	Timeout	Length	-warning>
6	info	200			5345	Invalid username or password
0		200			5360	Invalid username or password.
1	carlos	200			5343	Invalid username or password.
2	root	200			5343	Invalid username or password.
3	admin	200			5345	Invalid username or password.
4	test	200			5342	Invalid username or password.

Looks like the subtlety is a full stop



You can see it clearly on the webapp login page