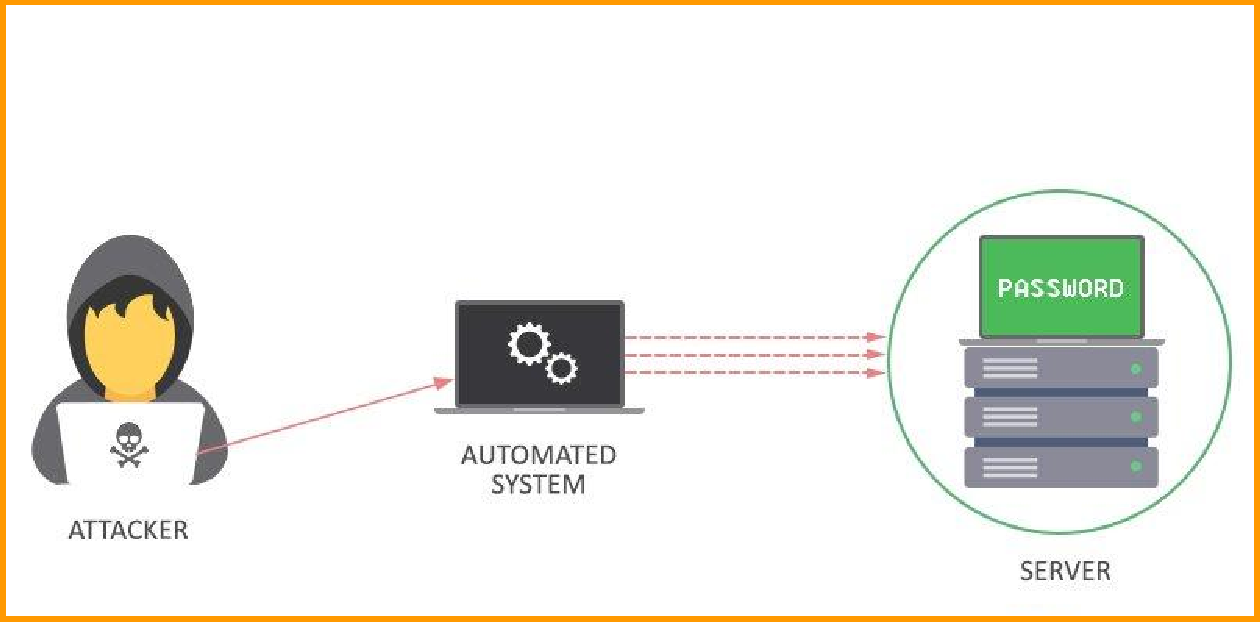
# Brute-Force Attack



* **What is a Brute-Force Attack?**

# Brute Force Attack Types

* + *Dictionary Attack*
  + *Reverse Brute Force Attack*
  + *Credential Stuffing*

# How To Prevent Brute Force Attacks

* + *Require Use of Strong, Unique Passwords*
  + *Require the Use of Multi-Factor Authentication*
  + *Adopt Network Security and Threat Detection Tools*
  + *Use a Whitelist to Limit Access to Specific Pages*

# [Brute - Force Lab Practical Link](https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses)

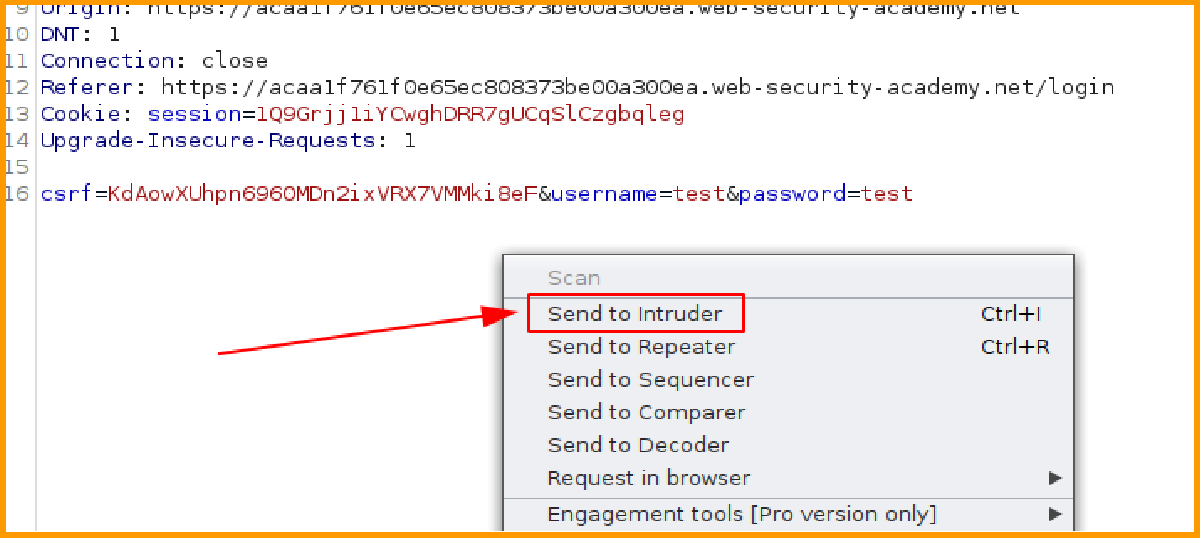
## Step 01

Navigate to the ‘Account login’ page of the website**.**



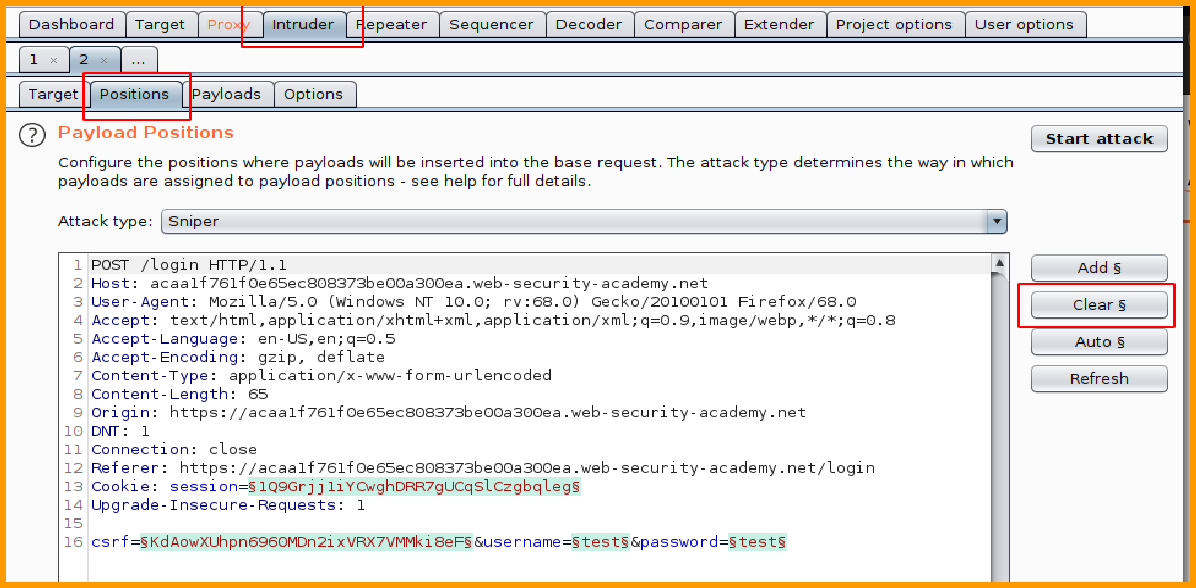
**Step 02**

* With Burp running, investigate the login page and submit an invalid username and password.
* In Burp, go to "Proxy" > "HTTP history" and find the POST /login request. Send this to Burp Intruder.



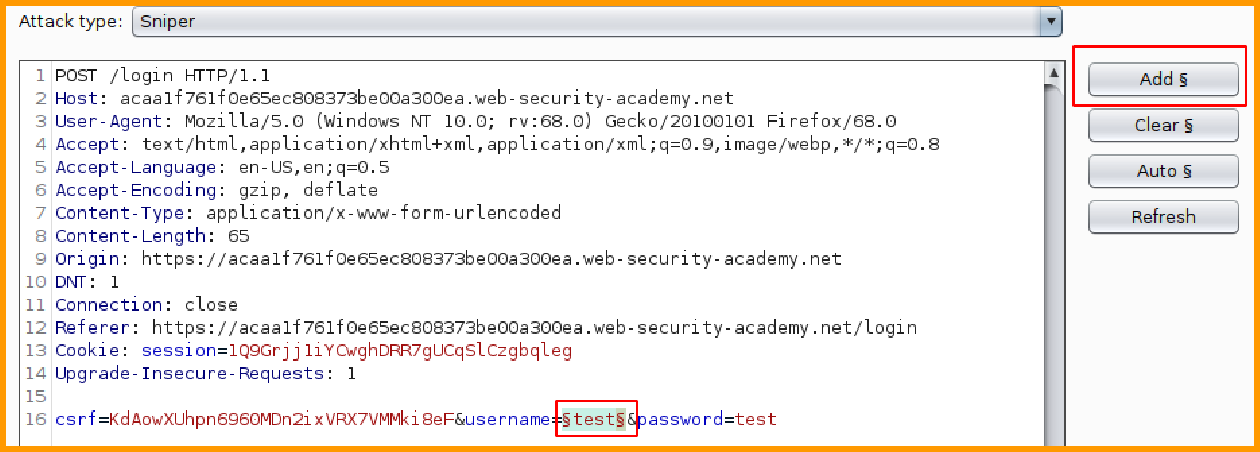
**Step 03**

* In Burp Intruder, go to the "Positions" tab. Make sure that the "Sniper" attack type is selected.
* Click "Clear" to remove any automatically assigned payload positions.



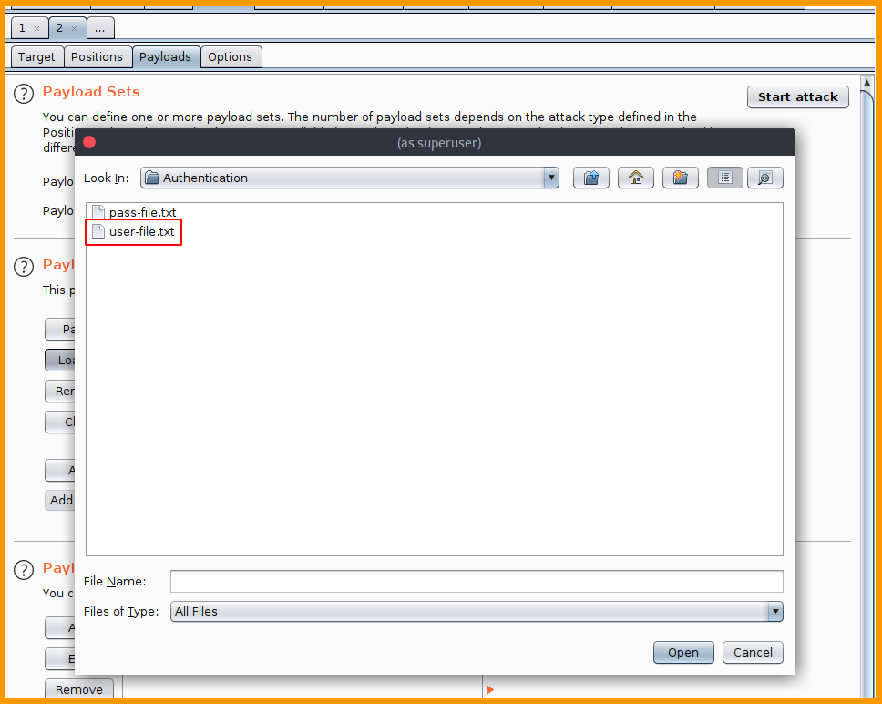
**Step 04**

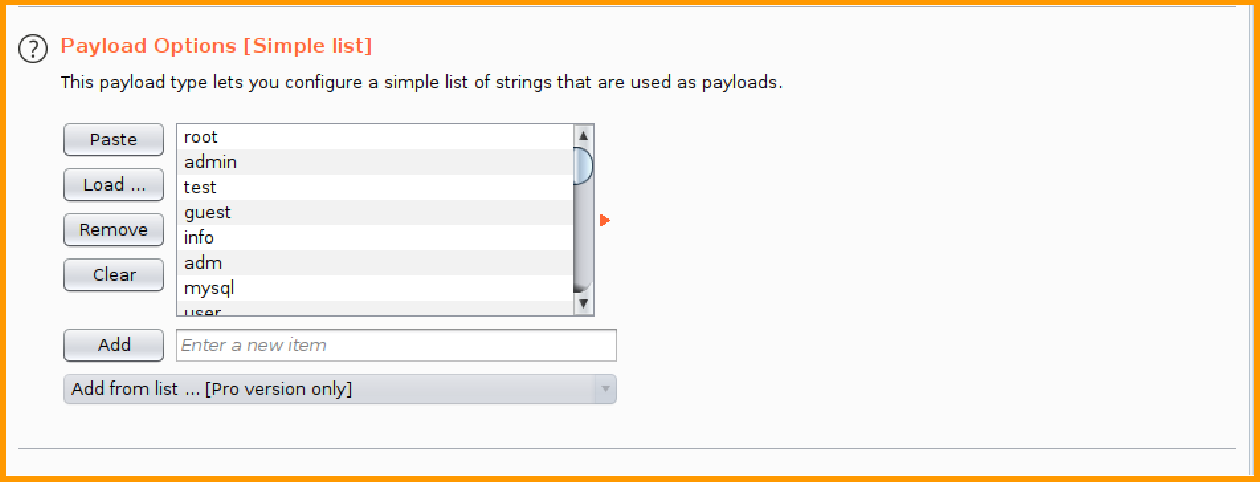
* Highlight the value of the username parameter and click "Add" to set it as a payload position. This position will be indicated by two § symbols, for example username=§invalid-username§. Leave the password as any static value for now.



**Step 05**

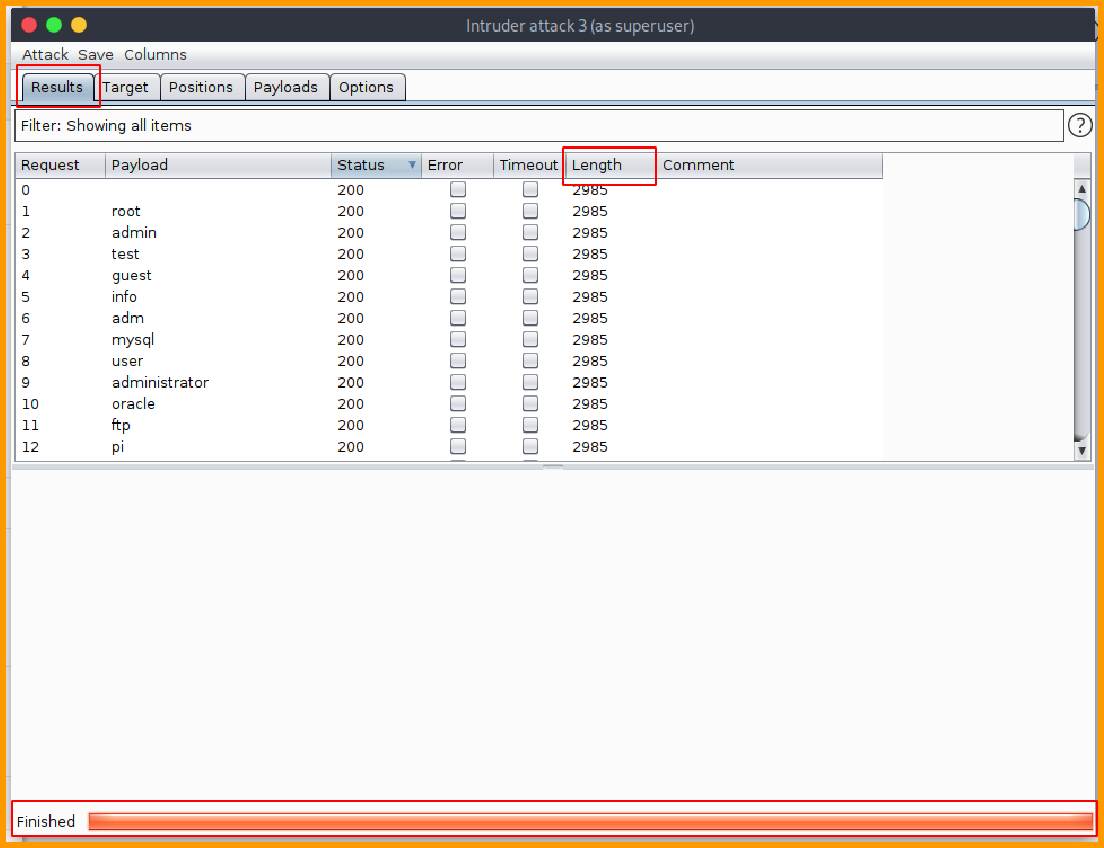
* On the "Payloads" tab, make sure that the "Simple list" payload type is selected.
* Under "Payload options", paste the list of candidate usernames. Finally, click "Start attack". The attack will start in a new window.





**Step 06**

* When the attack is finished, on the "Results" tab, examine the "Length" column.

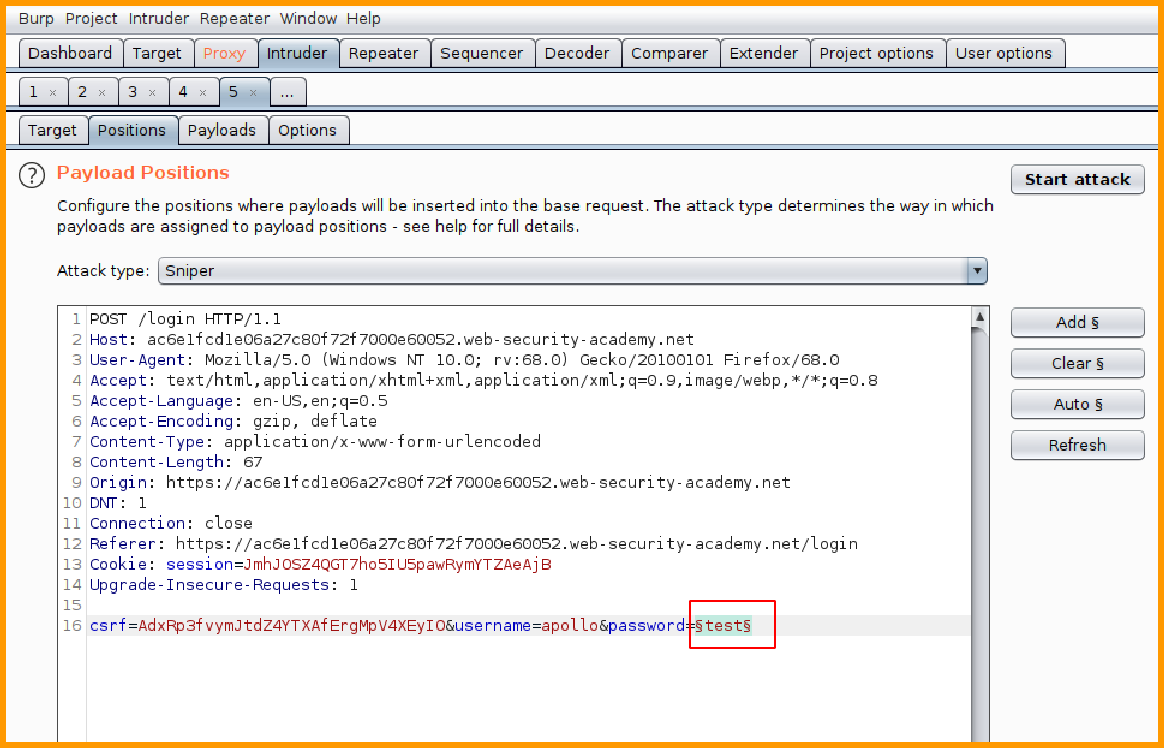


* You can click on the column header to sort the results. Notice that one of the entries is longer than the others.
* Compare the response to this payload with the other responses. Notice that other responses contain the message Invalid username, but this response says Incorrect password. Make a note of the username in the "Payload" column.

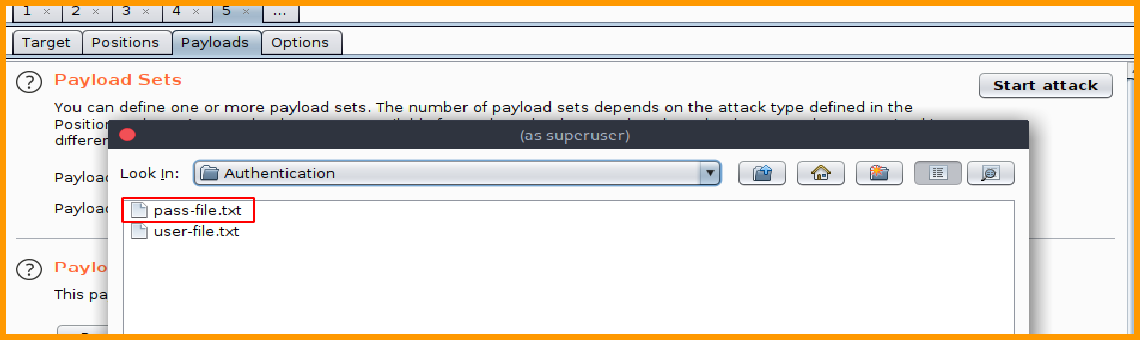
**Step 07**

* Close the attack and go back to the "Positions" tab. Click "Clear", then change the username parameter to the username you just identified. Add a payload position to the password parameter. The result should look something like this:

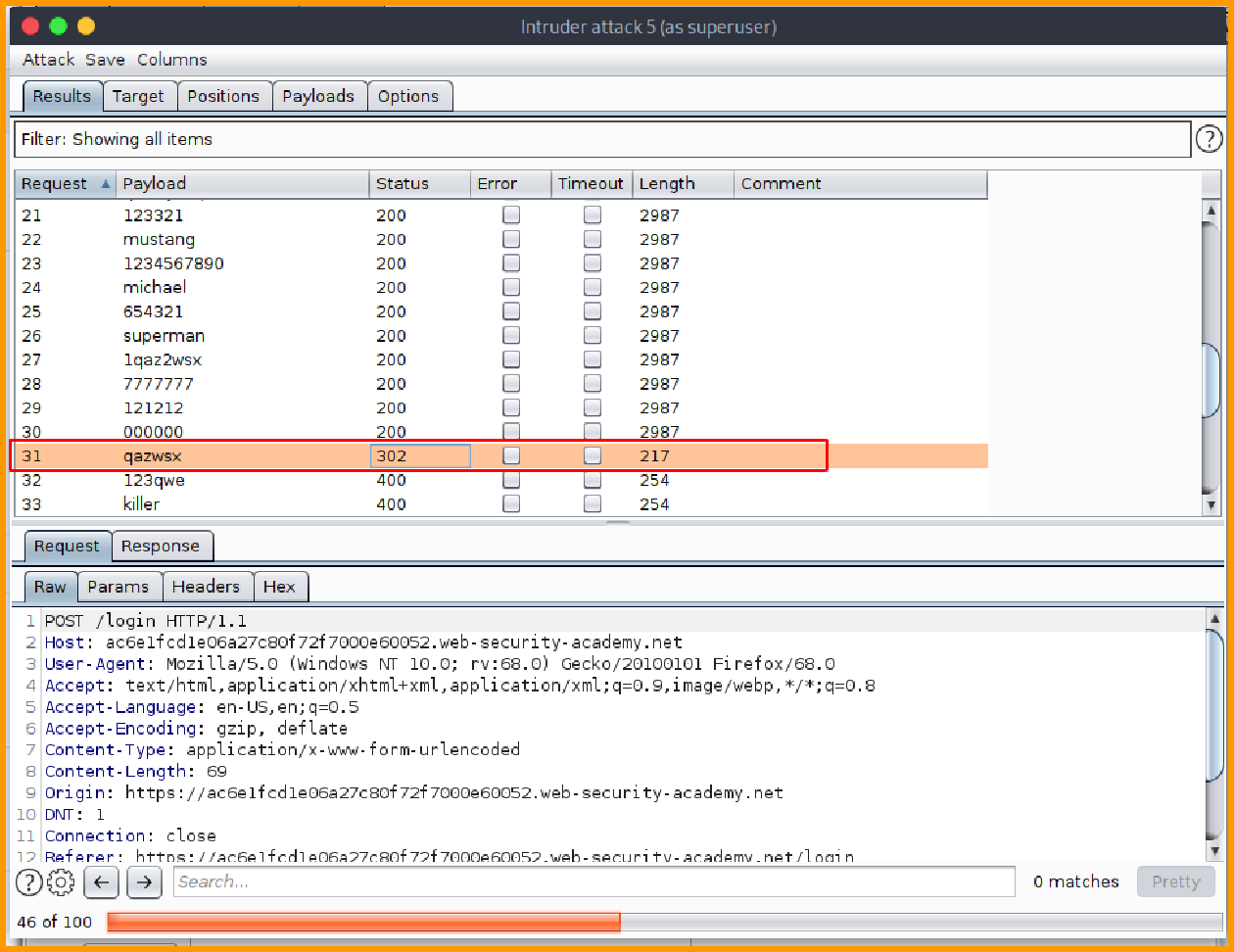
username=identified-user&password=§invalid-password§



* On the "Payloads" tab, clear the list of usernames and replace it with the list of candidate passwords. Click "Start attack".



* When the attack is finished, look at the "Status" column.
* Notice that each request received a response with a 200 status code except for one, which got a 302 response. This suggests that the login attempt was successful - make a note of the password in the "Payload" column.



* Log in using the username and password that you identified and access the user account page to solve the lab.

