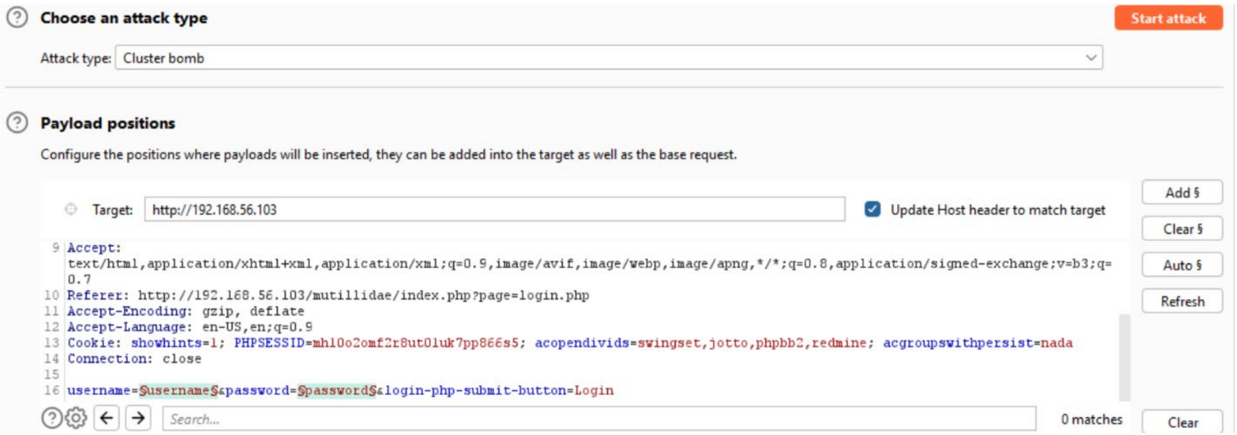
IFS4103: Graded Lab Tasks 3
(Burp Suite's Intruder – 2 marks)

For this GLT 3, you will need to submit your proof of work on utilizing **Burp Suite's Intruder**, which was covered in Lab 4. Using Intruder, you want to brute force the **login page of Mutillidae II**, which is also within the OWASP Broken Web Applications (BWA). Please ensure that the security level of Mutillidae II is set to **0 (hosed)** as described in Lab 2 so that you can perform your attack PoC.

First, you need to create **an account** in Mutillidae II. On the app's landing page, click on "Login/Register". After clicking on "Please register here", create an account with username = "**`ifs4103`**" and password = "**`superman`**". Do sign in using the created account to confirm your successful account creation. Using Burp Proxy, you can additionally observe how Mutillidae II handles a successful sign-in using a **redirection** with 302 status code. Please log out afterwards.

Next, you want to use Burp Intruder to **brute force** the login page by assuming that you *don't know* the created account. You can log in using some random username and password to get **an entry in Burp Proxy**, which can then be sent to Intruder. In the Intruder, do select the "**Cluster bomb**" attack type. Set your **payload positions** accordingly like in the shown screenshot below.


Choose an attack type
Start attack

Attack type: Cluster bomb

Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.56.103

☑ Update Host header to match target

Add §
Clear §
Auto §
Refresh

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Referer: http://192.168.56.103/mutillidae/index.php?page=login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: showhints=1; PHPSESSID=mh10o2omf2r8ut0luk7pp866s5; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Connection: close

username=§username§&password=§password§&login-php-submit-button=Login
```

In Intruder, for **payload set 1**, just select the **"Simple list"** payload type. You can manually add the following username entries into the list: "`ifs4102`", "`ifs4103`", "`cs4238`". For **payload set 2**, again, select the **"Simple list"** payload type. You can manually add the following password entries into the list: "`superman`", "`batman`", "`spiderman`". Before running your attack, in the **Intruder's settings**, do enable the "**Follow redirections**" option.[1] For your PoC, you can select either "on-site only", "in-scope only" or "always".

For your answer submission, do the following:

1. Attach a screenshot (*in colour*) of your Intruder's **Results** window, which shows all the **9 sent request entries**, including the entry for the correct username and password (shown with its "Redirects followed" value of "1").

2. In your Intruder's Results window, first click on the entry with "`ifs4103`" and "`superman`", and then view its **response** (with "**Render**" display mode). You should see a page with this string shown: "`You are logged in as ifs4103`". Attach a screenshot (*in colour*) of your Intruder's **Results** window that also shows the rendered response page.

Like our previous GLTs, do follow these **instructions** for your submission:

- Please put the requested screenshots in a self-contained **PDF file** by using your name and matric number as part of your file name, e.g. JackLee-A012345-**GLT3**.pdf.
- Upload your PDF file via "**`Graded Lab Tasks 3`**" Assignment by **Tuesday, 27 February 2024, 23:59 SGT**. Again, the deadline is a ***firm & final*** **deadline**. You are thus advised to submit **well before** the cut-off time so as to avoid any technical issues with Canvas access or your uploading!

Happy brute forcing!

[1] See also https://portswigger.net/burp/documentation/desktop/tools/intruder/configure-attack/settings.