**Steps**:

1. Send a login request, and observe that you get 401 unauthorized.



2) Open the file provided <https://github.com/roottusk/vapi/tree/master/Resources/API2_CredentialStuffing>

observed that there are usernames and passwords, and now we can perform a Credential Stuffing attack.

3) Send the request to the intruder, set the attack type to pitchfork,

3.1) Set payload 1 to email

3.2) Set payload 2 to password

Make sure that the payload encoding is not marked with V

4) Filter the results base on the status and find the ones with 200. There are three with 200

* [savanna48@ortiz.com](mailto:savanna48@ortiz.com)
* [hauck.aletha@yahoo.com](mailto:hauck.aletha@yahoo.com)
* [harber.leif@beatty.info](mailto:harber.leif@beatty.info)

5) Add the token from the request to the GET request. Don’t forget to add the Authorization-Token header.

You will receive a list of users, there you will find the flag under user ID flag{api2\_6bf2beda61e2a1ab2d0a}