LAB: USERNAME ENUMERATION VIA DIFFERENT RESPONSES

https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses

GÖREV:

Farklı yanıtlar aracılığıyla kullanıcı adı numaralandırma

AÇIKLAMA:

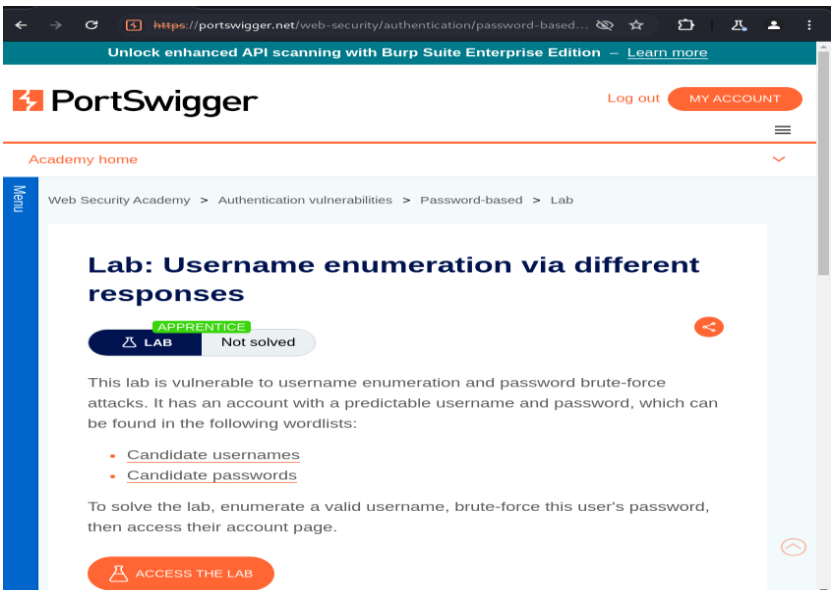
Bu laboratuvar, kullanıcı adı numaralandırma ve parola kaba kuvvet saldırılarına karşı savunmasızdır. Aşağıdaki kelime listelerinde bulunabilecek tahmin edilebilir bir kullanıcı adı ve parolası olan bir hesabı vardır:

- Candidate usernames
- Candidate passwords

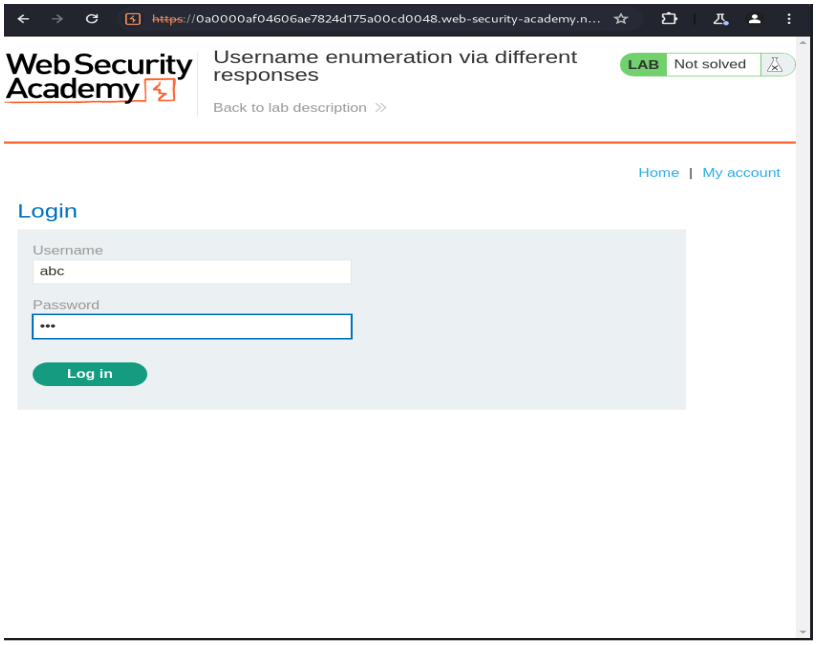
Laboratuvarı çözmek için geçerli bir kullanıcı adını numaralandırın, bu kullanıcının parolasını kaba kuvvetle girin ve ardından hesap sayfasına erişin.

ÇÖZÜM:

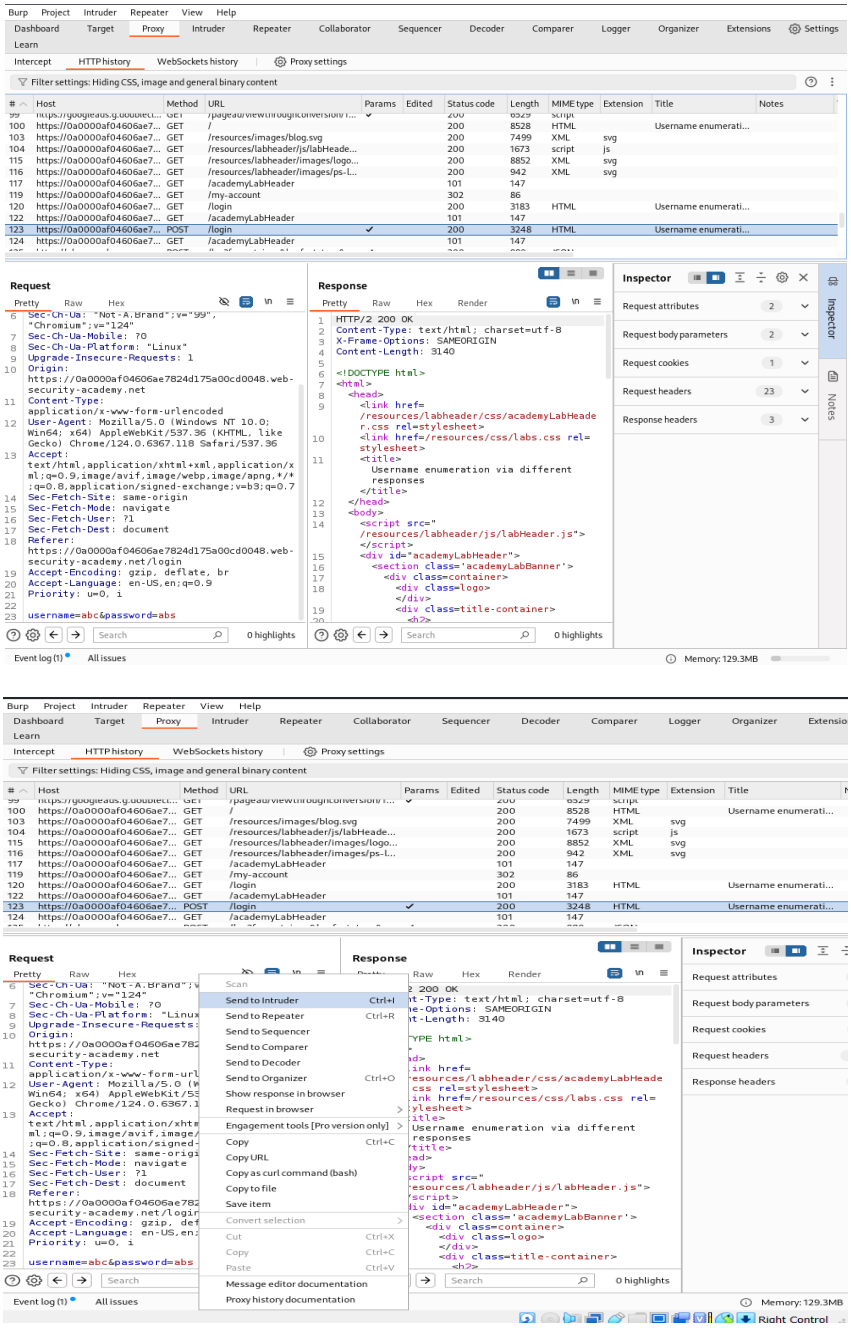
Laboratuvara erişimi başlatıyoruz.



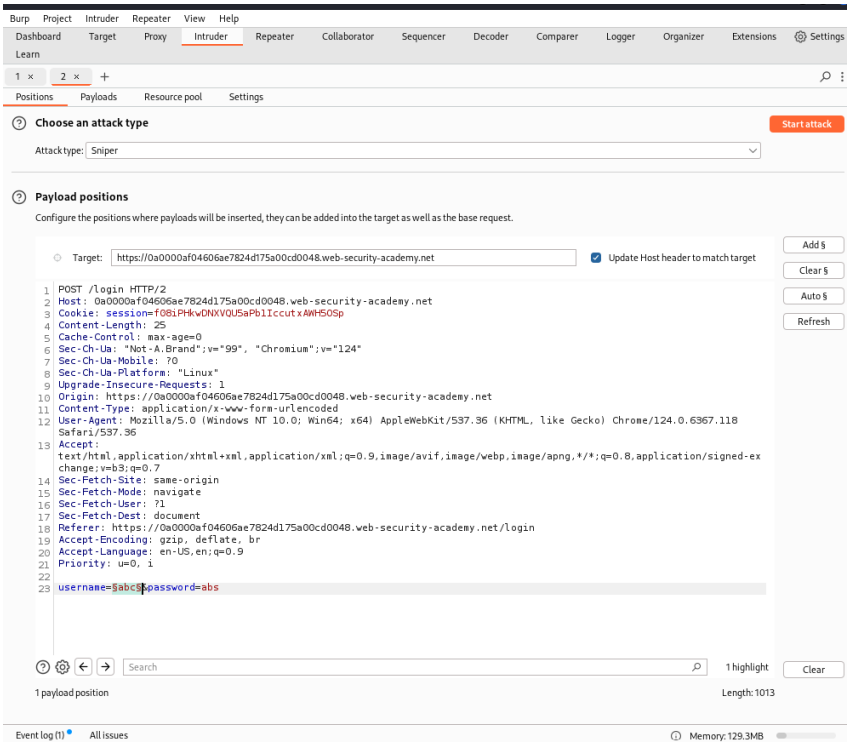
Choromium yani burp tarayıcısını açıp labımıza erişimi başlatıyoruz. Bize bir blog sayfası veriyor giriş yapmamız gerekmektedir. Bunun için “username” ve “password” bilgilerimizi girmemiz gerekmektedir.



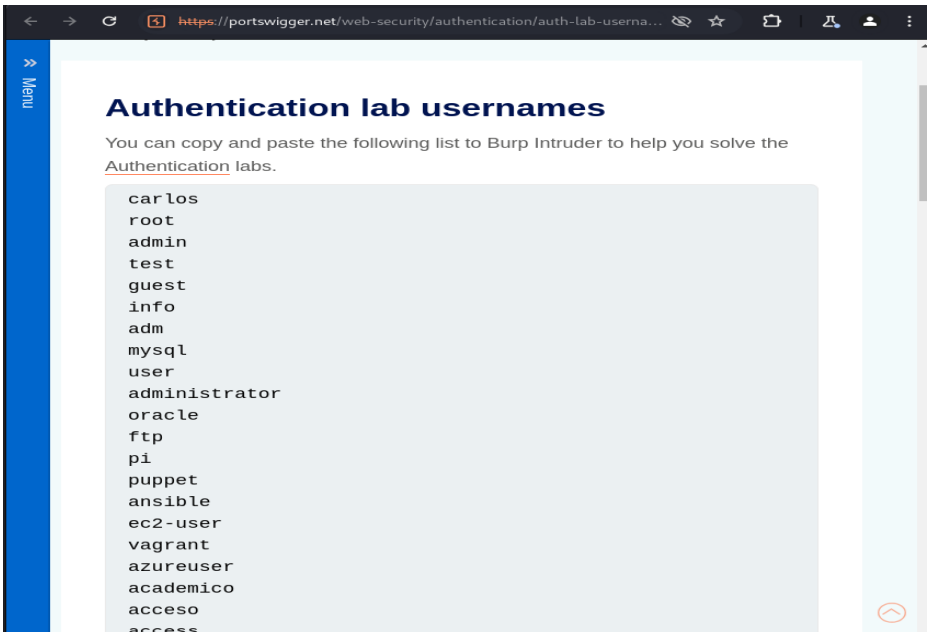
HTTP history'den girdiğimiz password ve username ifadelerini görmekteyiz. Giriş bilgilerini bulabilmek için Intruder'a gönderip "Sniper attack" saldırı türüyle login olacağız.



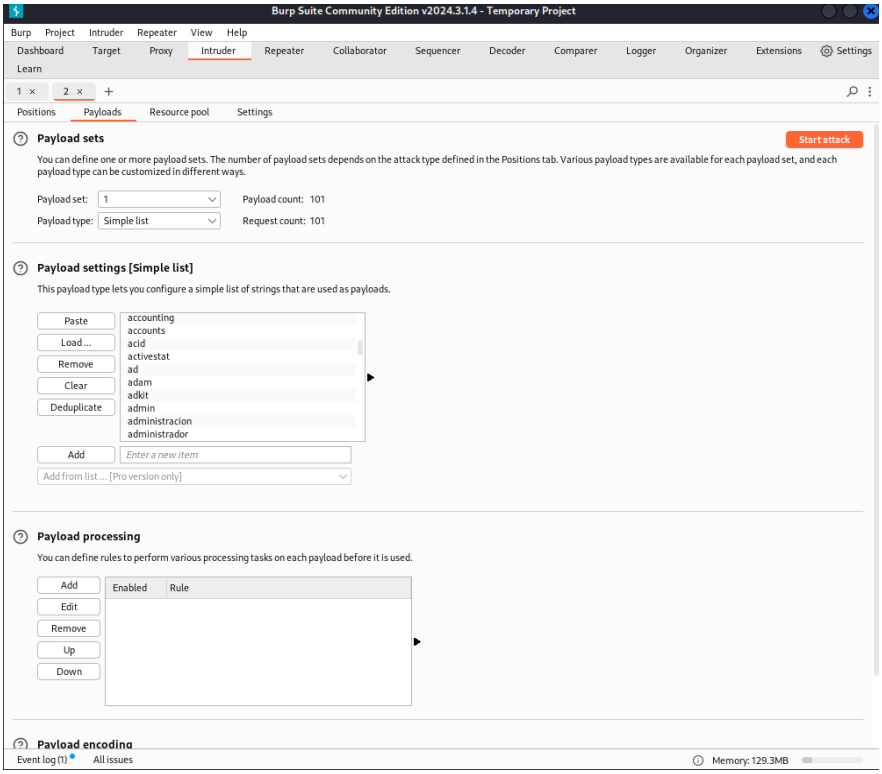
İlk başta “username“ ifadesini add butonuna basıp seçili hale getirip Payloads sekmesine geçiyoruz.

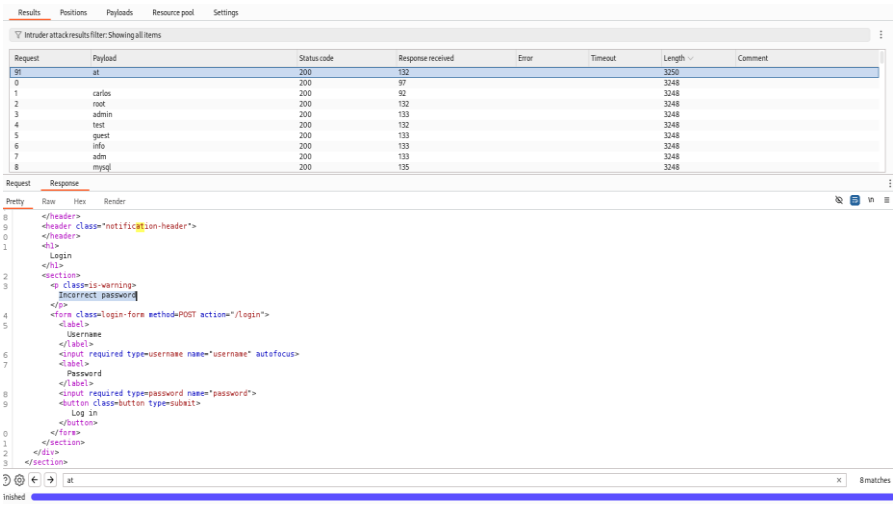


Laboratuvarı ilk açtığımızda bize “username” ve “password” için kullanabileceğimiz bir liste vermektedir. Kopyalayıp Sniper saldırısını başlatmamız gerekmektedir.

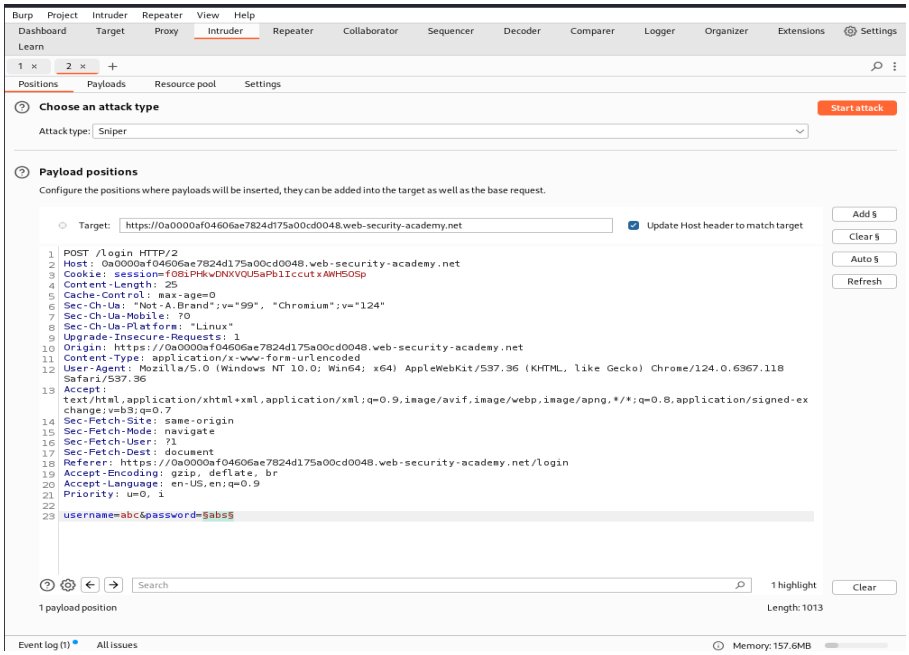


Kopyaladığımız listeyi yapıştırıp saldırıyı başlatıyoruz.

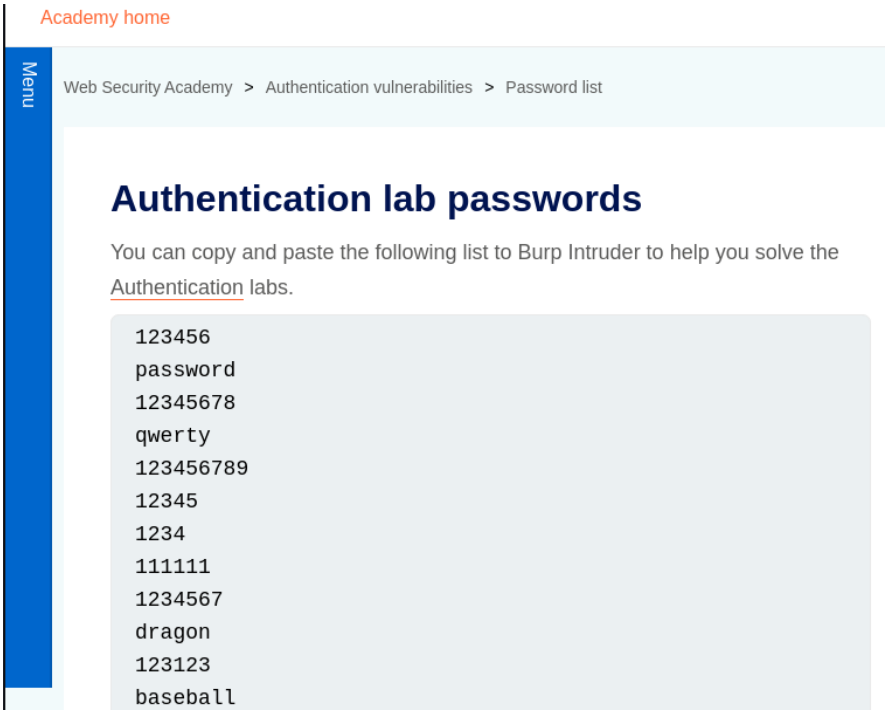




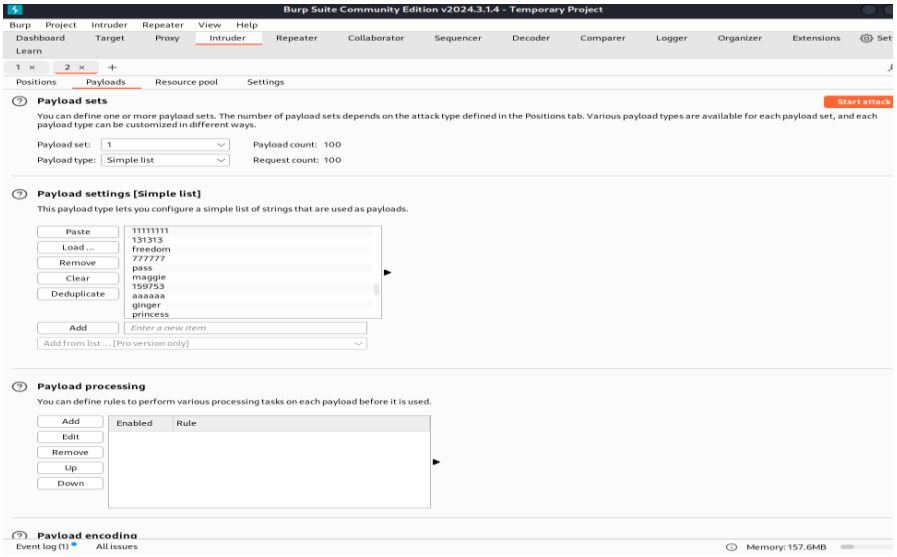
Tarama sonucunda username ifadesini bulduk fakat password değerimiz yanlış. Aynı işlemi password için de tekrarlıyoruz. Password ifadesini add butonuna basarak işaretliyoruz.

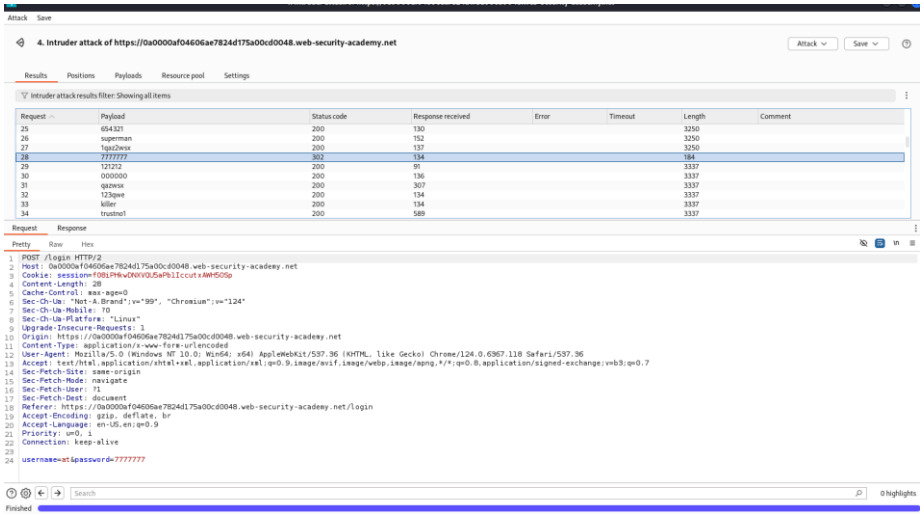


Laboratuvara erişimi başlattığımız yerde verilen password listesini kopyalıyoruz.

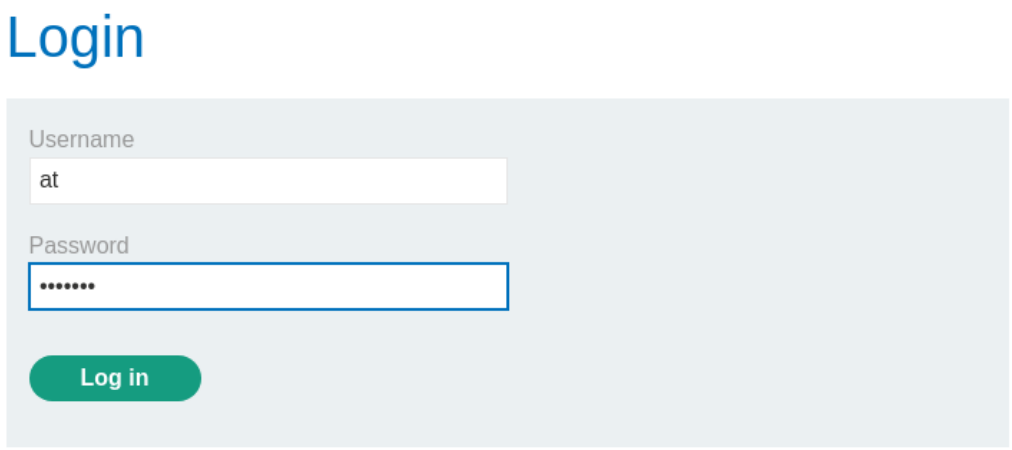


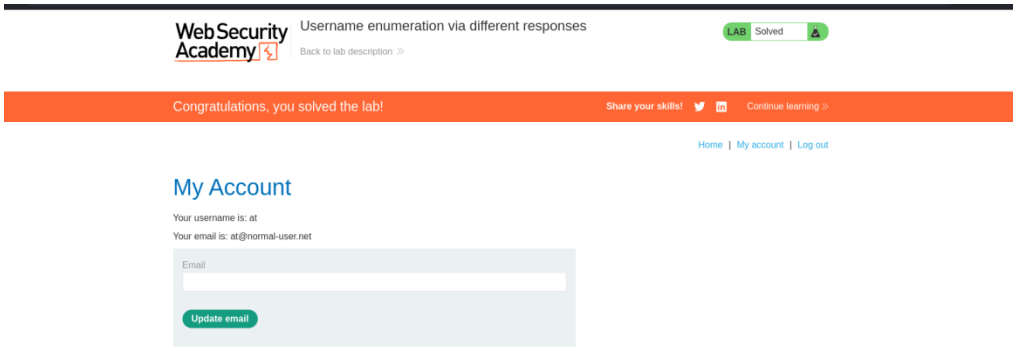
Kopyaldığımız listeyi yapştırıyoruz ve saldırıyı başlatıyoruz.





Tarama sonucunda username ve password ifadelerine erişimi sağlamış bulunmaktayız. Login sayfasına gidip giriş bilgilerini giriyoruz. Laboratuvar çözülmüştür.





ŞEYMA SAYLAN