LAB: PASSWORD RESET BROKEN LOGIC

https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-broken-logic

GÖREV:

Şifre sıfırlama bozuk mantığı

AÇIKLAMA:

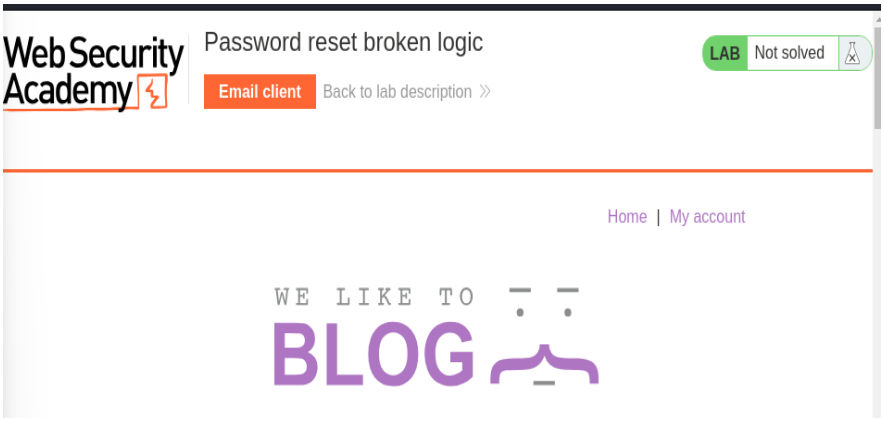
Bu laboratuvarın parola sıfırlama işlevi savunmasızdır. Laboratuvarı çözmek için Carlos'un şifresini sıfırlayın, ardından oturum açın ve "Hesabım" sayfasına erişin.

Kimlik bilgileriniz: **wiener:peter**

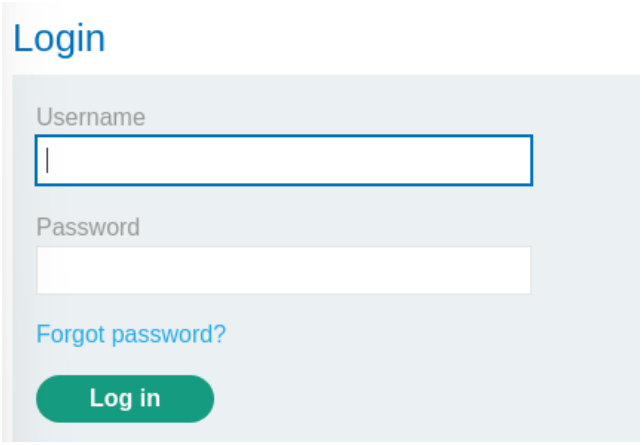
Kurbanın kullanıcı adı: **Carlos**

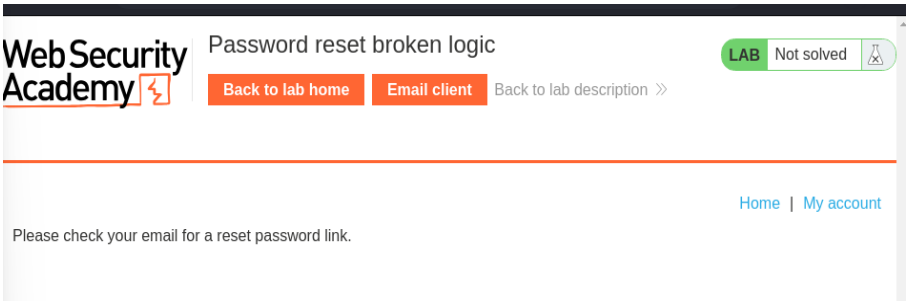
ÇÖZÜM:

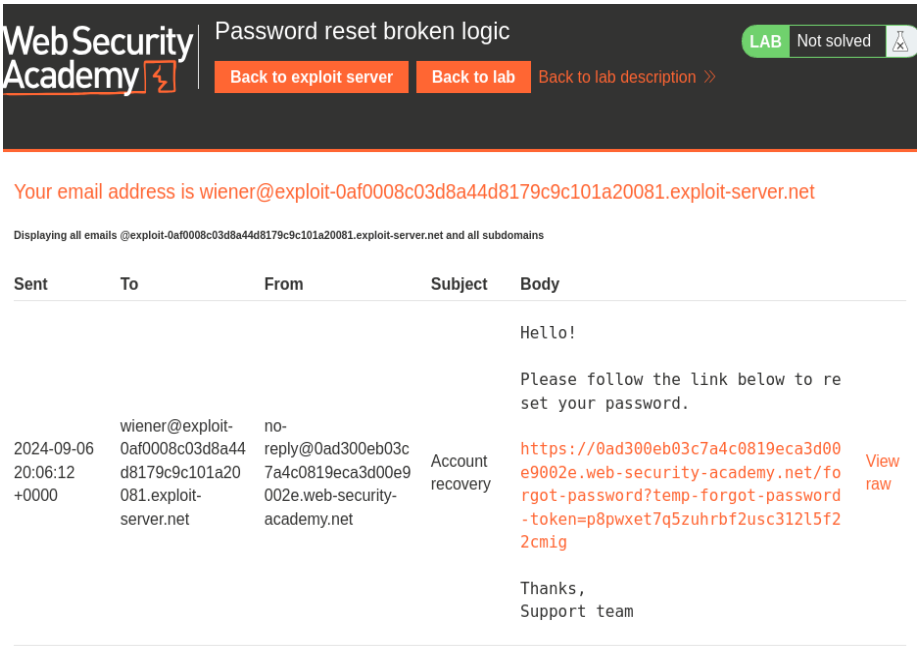
Laboratuvara erişimi başlatıyoruz.



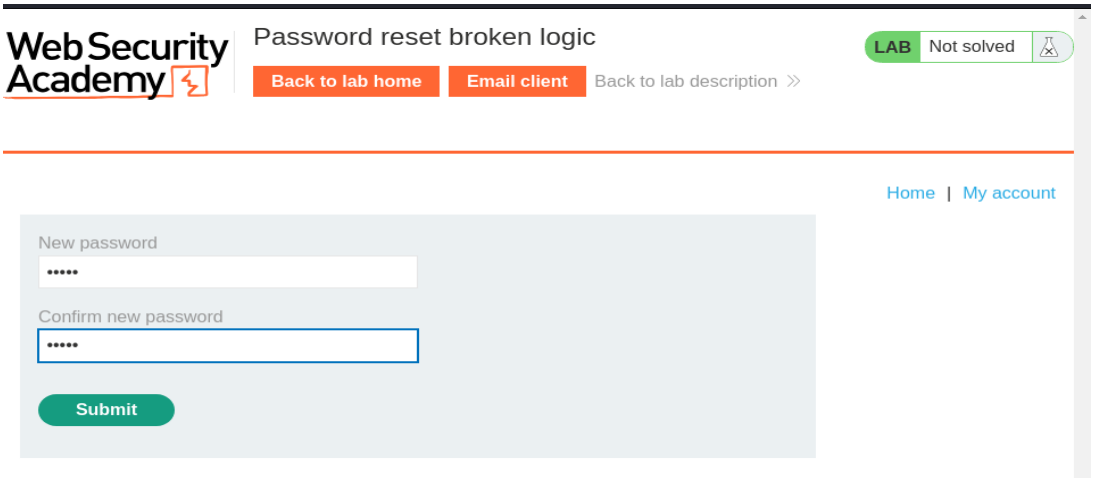
Bize kullanıcı adı ve parola bilgileri verilmiştir. Bu bilgilerle hesaplara giriş yapmamız gerekmektedir. Fakat burada parola bilgilerimizi sıfırlamamız gerekeceği için giriş yapmadan şifremi unuttum yapmamız gerekmektedir.



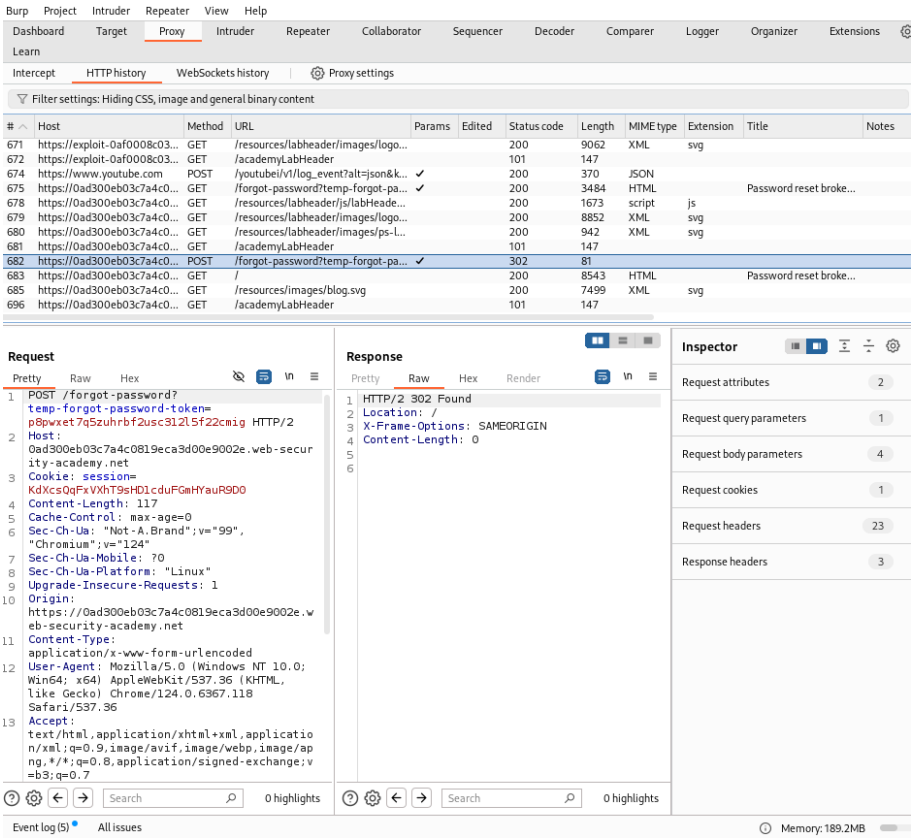




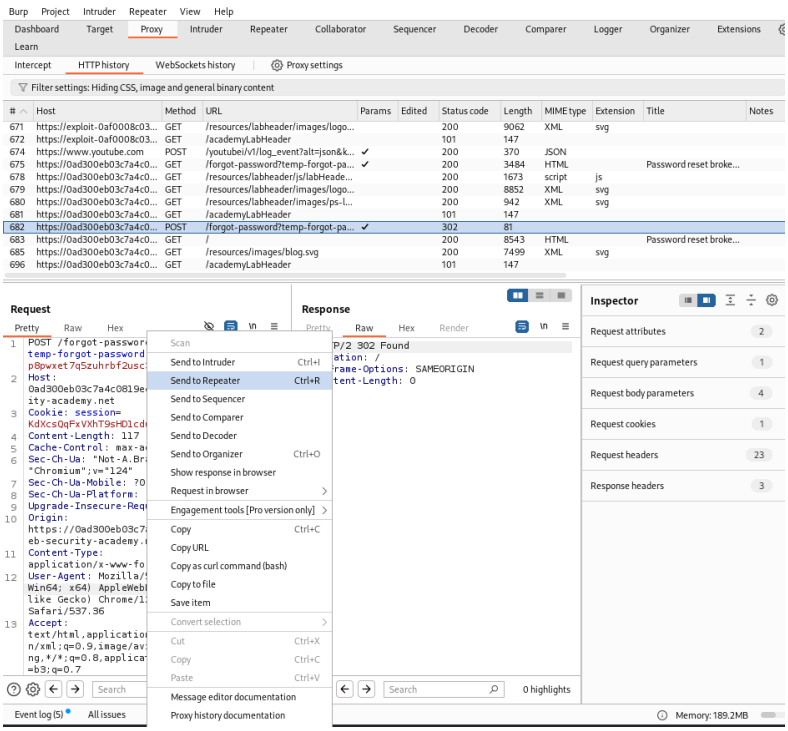
Yeni şifre oluşturuyoruz. Şifremiz peter.



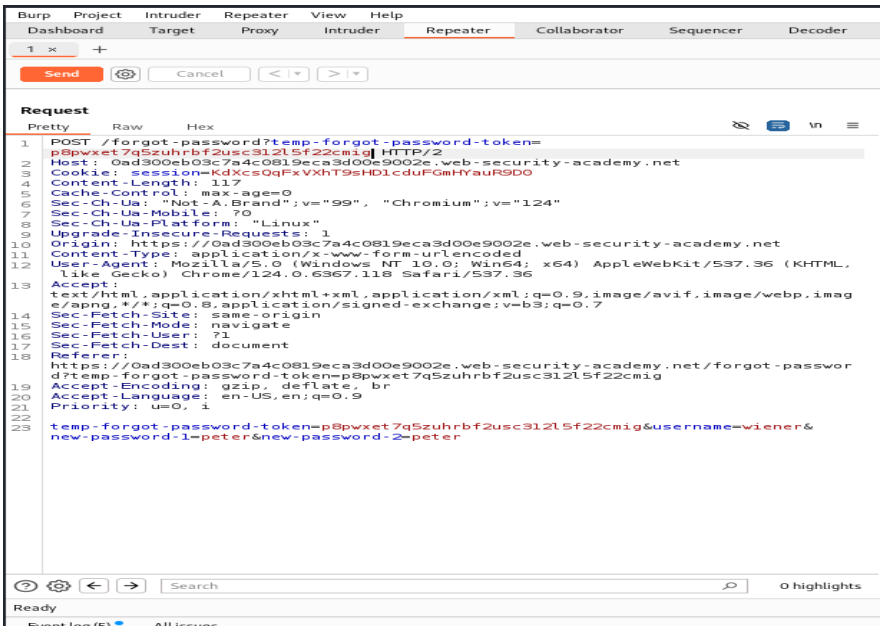
Bu yaptığımız işlemleri http history'den takip edip kullanacağımız olanı incelemeye başlıyoruz.

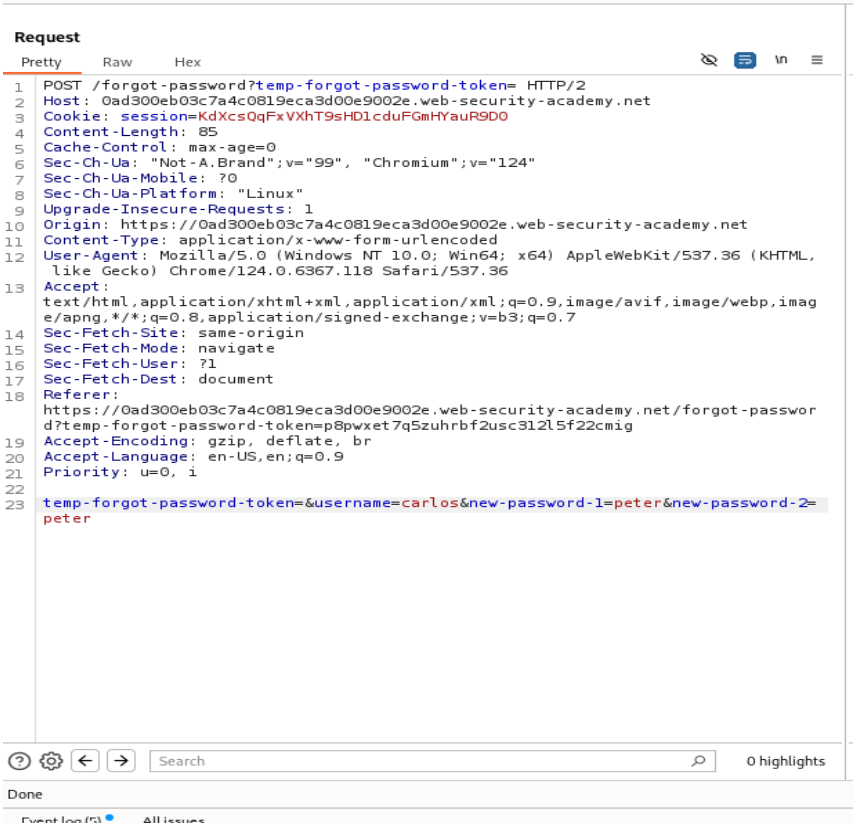


Repeater'a göndermemiz gerekmektedir.

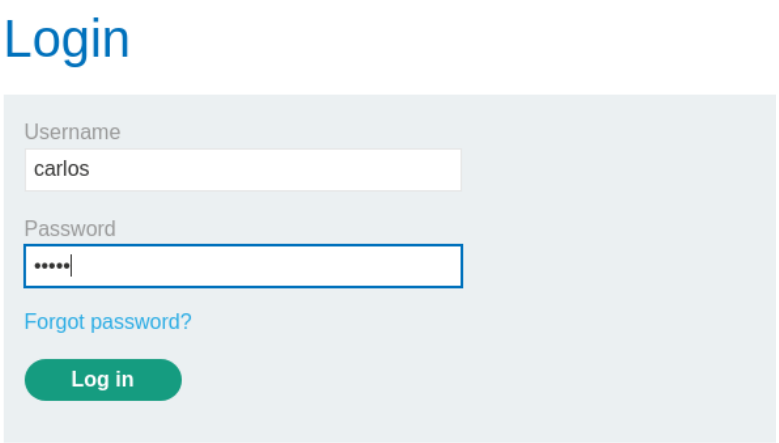


Burada yapacağımız işlem ise verilen tokenları silip kullanıcı adı yerine carlos yazmamız gerekmektedir

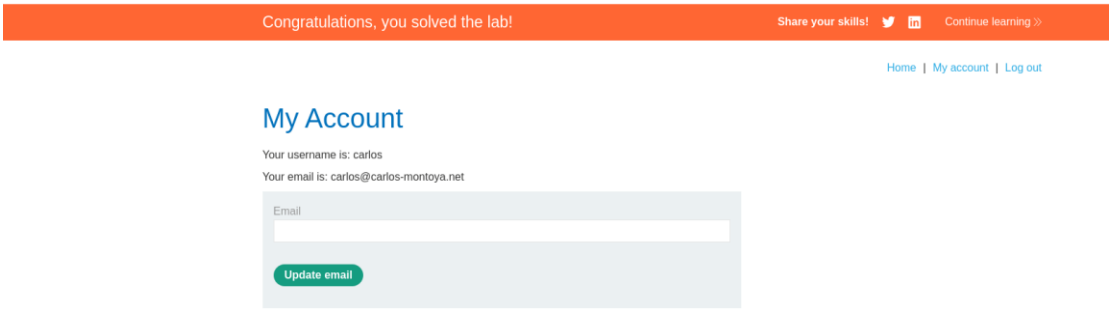




Tekrardan giriş sayfasına gelip carlos adını yazıp önceden koyduğumuz peter şifresini girmemiz gerekmektedir.



Login bilgilerini girdikten sonra ise laboratuvarımızı tamamlamış bulunmaktayız.



ŞEYMA SAYLAN