OWASP TOP 10 LAB RAPORU

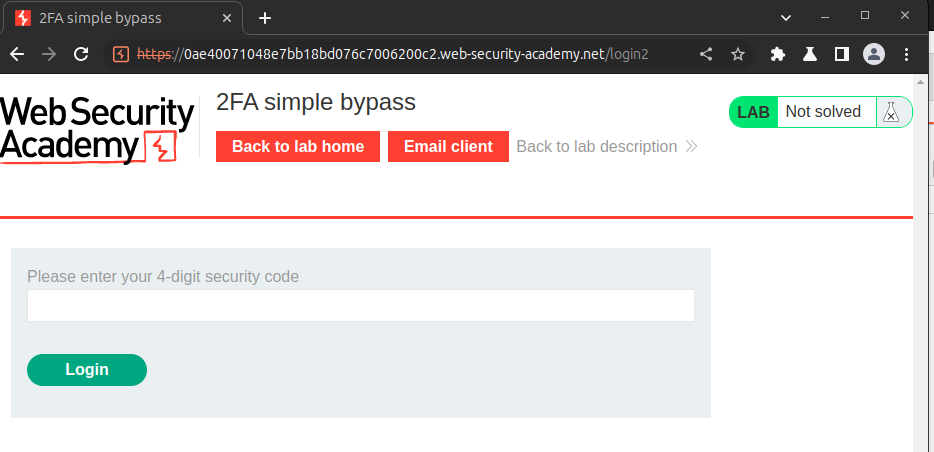
Portswigger authentication vulnerabilities

1. 2FA simple bypass:

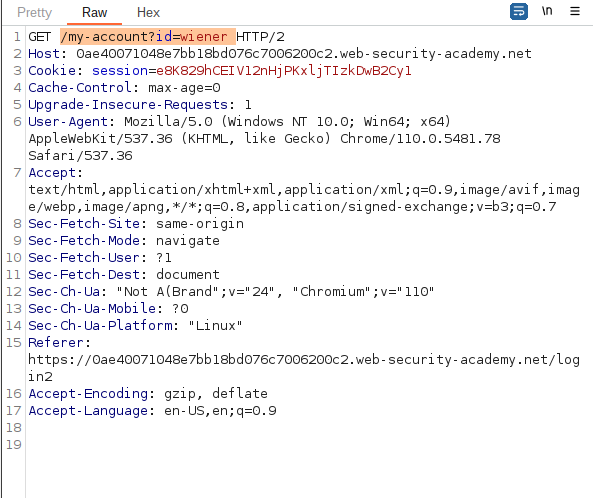
İçerik : This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

* Your credentials: wiener:peter
* Victim's credentials carlos:montoya

Lab Çözümü: Bize verilen kullanıcı adı ve şifreyle hesaba giriş yaptığımızda karşımıza doğrulama sayfası çıkıyor.



Doğrulama kodunu email client sayfasına baktığımda 1357 olarak gördüm.Doğrulama kodunu girdiğimde url’deki parametrenin /my-account?id=wiener olarak değiştiğini gördüm.



Eğer url’deki id kısmını Carlos yaparsak doğrulama kodu gerekmeden direkt Carlos’un hesabına erişebiliriz. Carlos’ un kullanıcı bilgilerini girdikten sonra /login2 sayfasına eriştim.

Url i [web-security-academy.net/my-account?id=carlos](http://web-security-academy.net/my-account?id=carlos) olarak değiştirdim ve carlos’un hesabına giriş yapıldı.

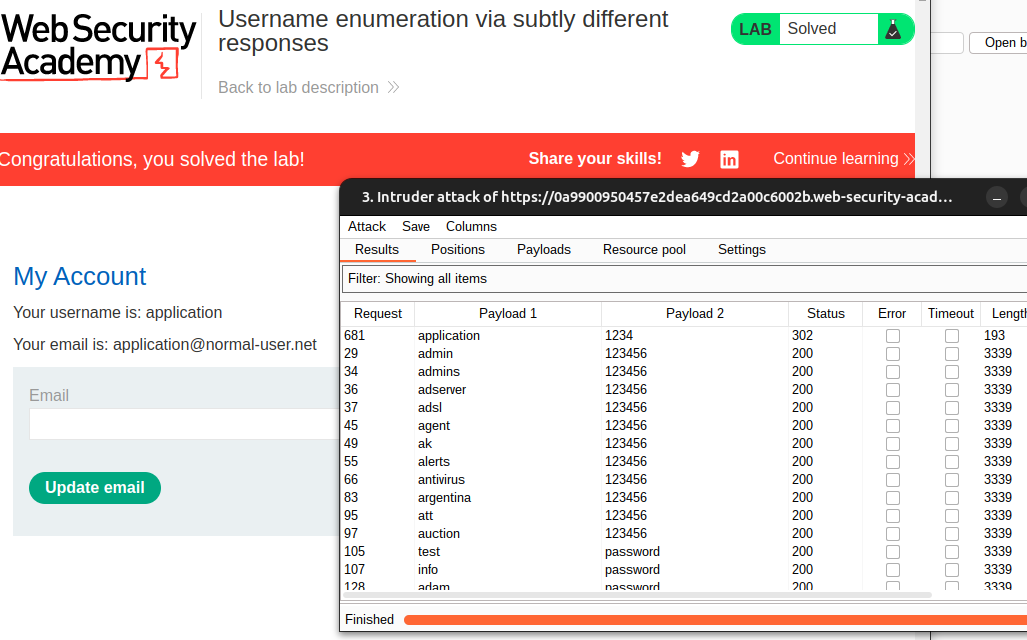
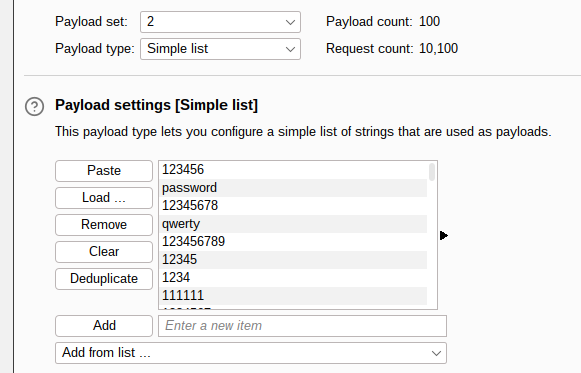
2.Username enumeration via subtly different responses:

İçerik :This lab is subtly vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

* [Candidate usernames](https://portswigger.net/web-security/authentication/auth-lab-usernames)
* [Candidate passwords](https://portswigger.net/web-security/authentication/auth-lab-passwords)

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

Lab Çözümü: Bize verilen wordlistlerden kayıtlı kullanıcı bilgilerinin olup olmadığına brute force atarak baktım.

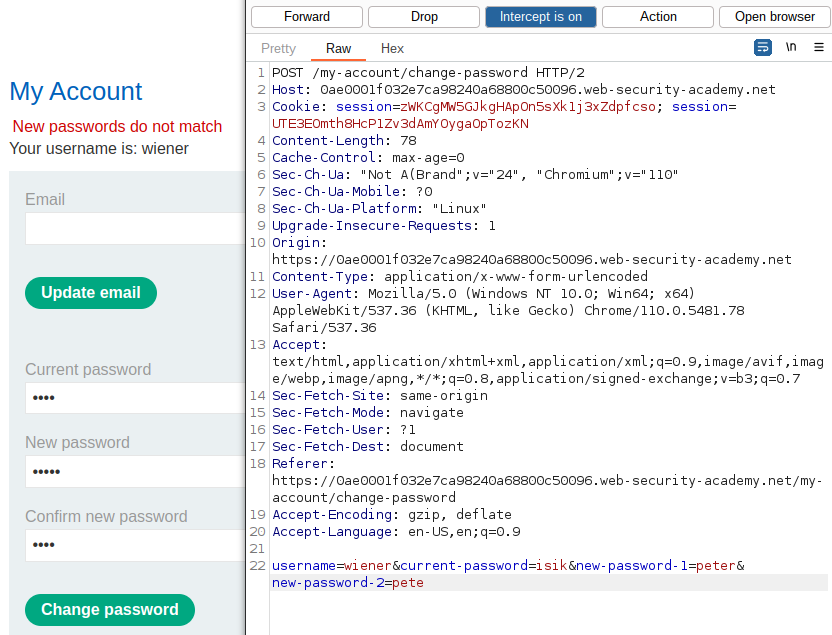


Brute force attıktan sonra statu kodu 302 olarak dönen kullancı adı application şifresi 1234 olan hesaba giriş yaptım.

3.Password brute-force via password change :

İçerik : This lab's password change functionality makes it vulnerable to brute-force attacks. To solve the lab, use the list of candidate passwords to brute-force Carlos's account and access his "My account" page.

* Your credentials: wiener:peter
* Victim's username: carlos
* [Candidate passwords](https://portswigger.net/web-security/authentication/auth-lab-passwords)

Lab Çözümü: Verilen kullanıcı adıyla hesaba girdikten sonra şifre değiştirme sayfasına girdim.

Şifre değiştirme haricindeki seçenekleri denedim.

İlk seçenek; current password un yanlış girilmesi ve diğer iki new password birbiriyle eşleşmesi sonucunda kullanıcıyı hesaptan çıkarıp tekrar login sayfasına atıyor.

İkinci seçenek; current password un yanlış girilmesi ve

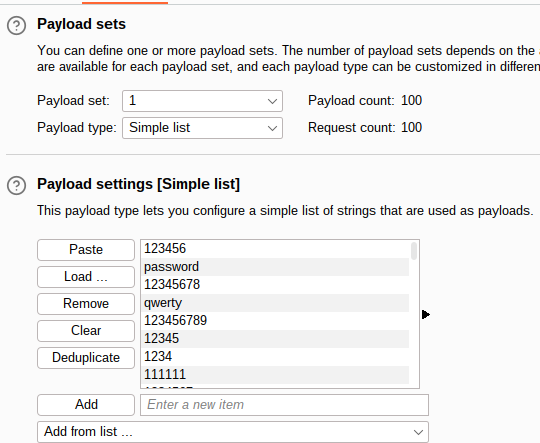
diğer iki new password birbiriyle eşleşmemesi sonucunda “Current password is incorrect” mesajı dönüyor.

Üçüncü seçenek; current password un doğru girilmesi ve

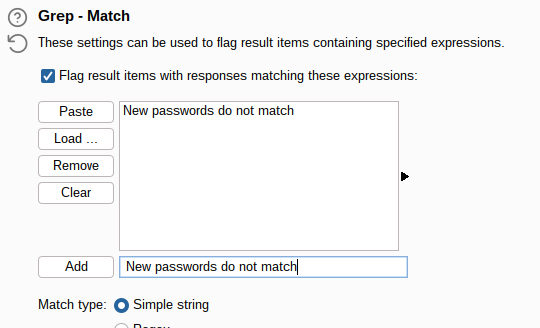
diğer iki new password birbiriyle eşleşmemesi sonucunda “New passwords do not match” mesajı dönüyor.

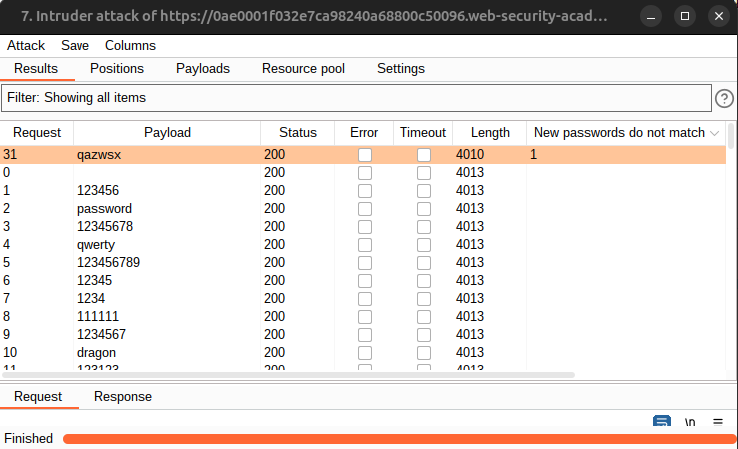
Bu mesajlardan yararlanarak carlos’un şifresini bulmaya çalıştım.Username’i carlos olarak değiştirip current passwordu doğru girdim ve diğer iki şifreyi birbirinden farklı girerek intruder a attım.

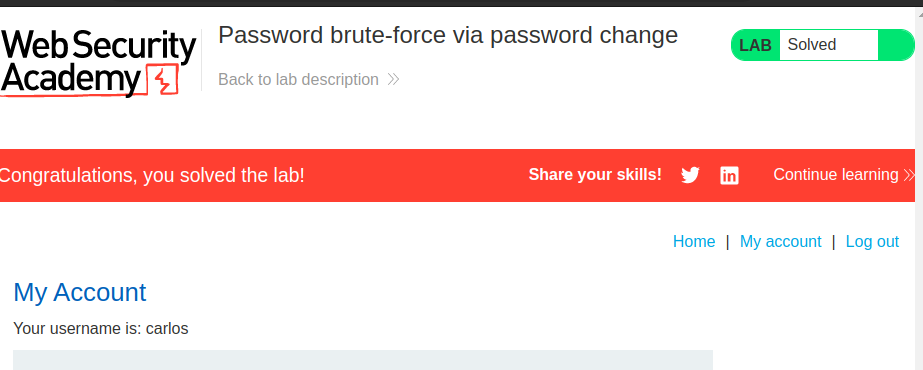




Grep-Match kısmında sonucu “New passwords do not match” mesajı dönenleri göstermesini istedim ki doğru şifreyi bulabilelim.





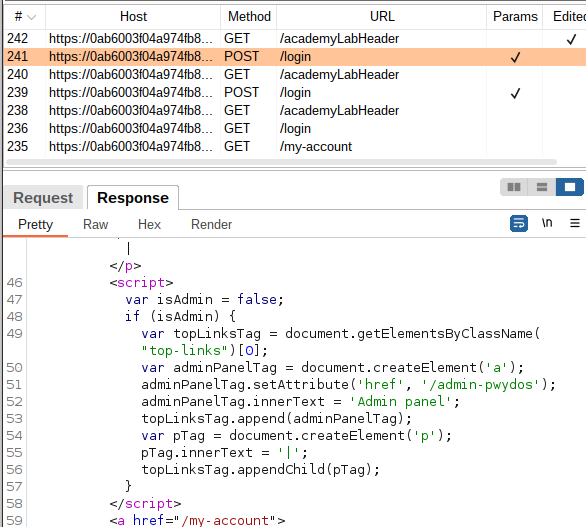


Portswigger access control vulnerabilities

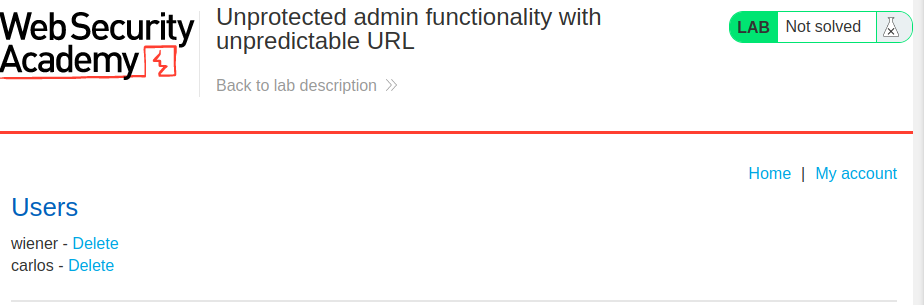
1.Unprotected admin functionality with unpredictable URL:

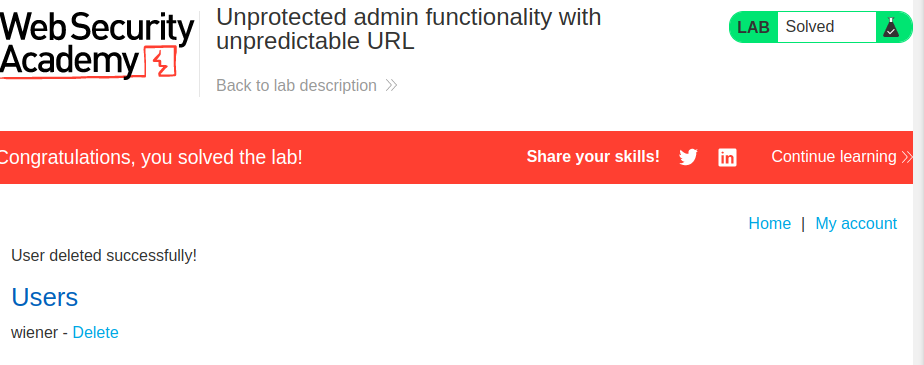
İçerik : This lab has an unprotected admin panel. It's located at an unpredictable location, but the location is disclosed somewhere in the application.

Solve the lab by accessing the admin panel, and using it to delete the user carlos.

Lab Çözümü:Herhangi bir kullanıcı bilgisiyle login olduktan sonra http historyden dönen response’lara baktığımda javascript kodu gördüm.

Kullanıcı adminse bu tag a giriyor ve url kısmında /admin-pwydos çalışıyor.

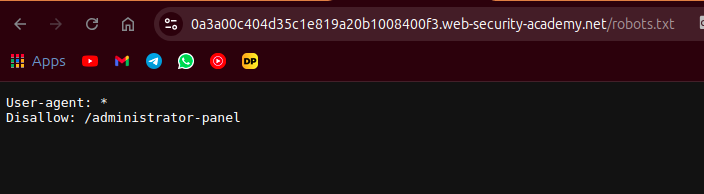
Admin paneline girdikten sonra carlos kullanıcısını sildiğimde lab çözülüyor.

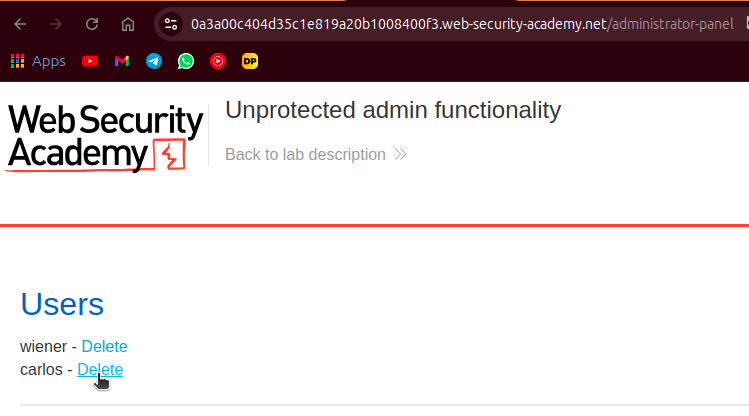


2.Unprotected admin functionality:

İçerik : This lab has an unprotected admin panel.

Solve the lab by deleting the user carlos.

Lab Çözümü: Url’e /robots.txt yazdığımızda bize admin sayfasına gidebileceğimiz parametreyi veriyor. 



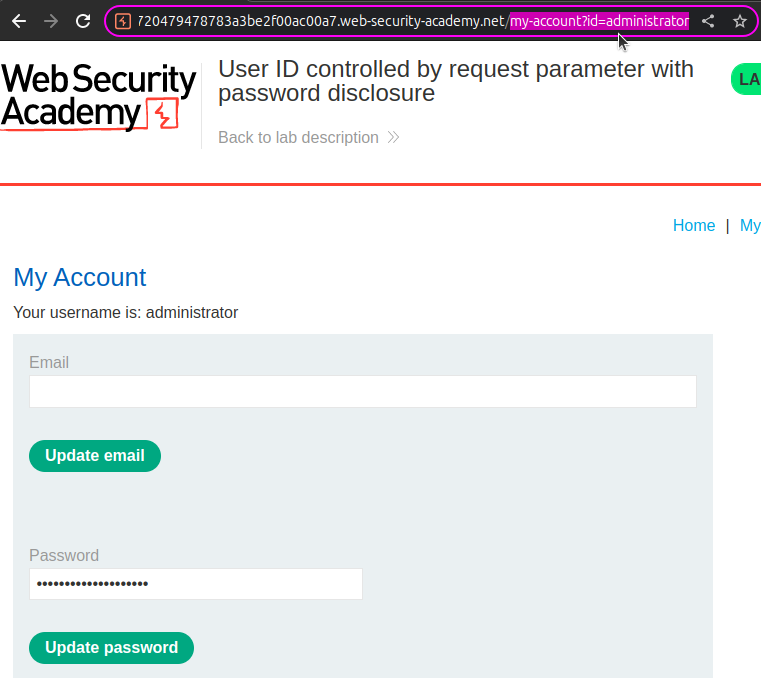
Carlos kullanıcısını sildiğimizde lab çözülüyor.

3.Lab: User ID controlled by request parameter with password disclosure:

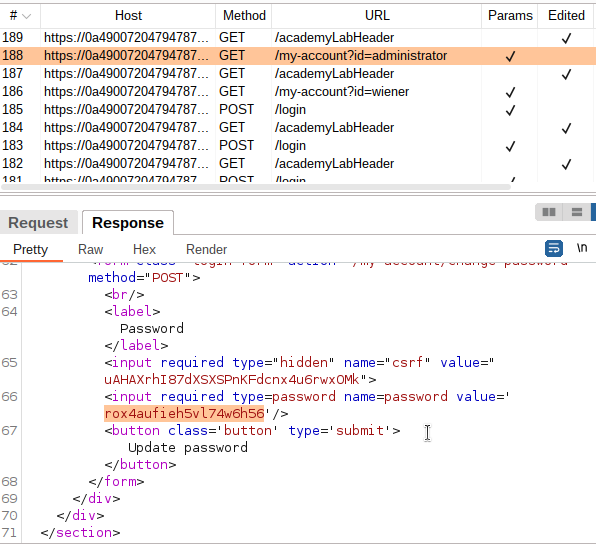
İçerik :This lab has user account page that contains the current user's existing password, prefilled in a masked input.

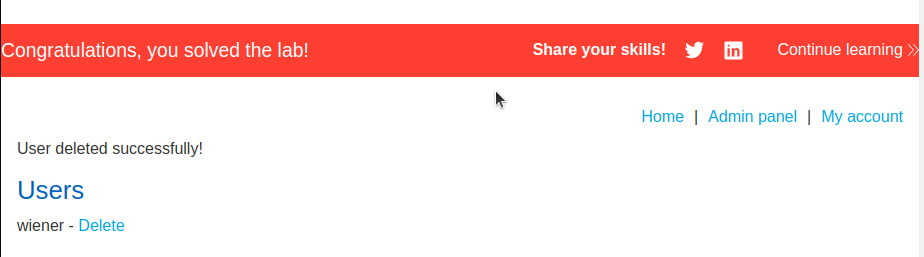
To solve the lab, retrieve the administrator's password, then use it to delete the user carlos.

You can log in to your own account using the following credentials: wiener:peter

Lab Çözümü: Wiener kullanıcısının hesabına girdikten sonra url’in /my-account?id=wiener olarak değiştiğini gördüm ve id parametresini administrator olarak değiştirerek adminin hesabına girebildim.

Password burada gizli olduğu için http historyden dönen response lara baktım.



Bu şifreyle admin hesabına girdikten sonra admin paneline tıkladım. Carlos kullanıcısını sildiğimde lab çözüldü.

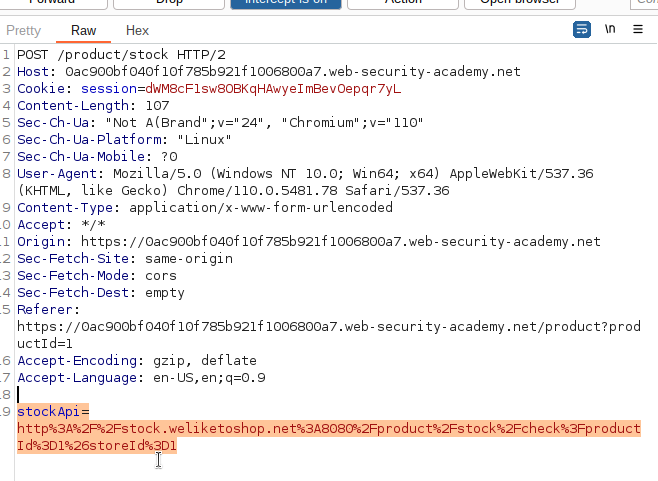
Portswigger SSRF

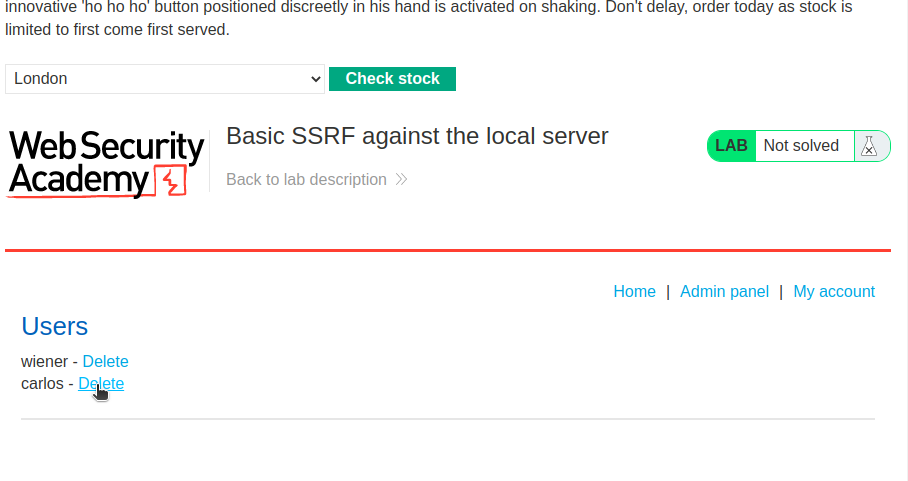
1.Basic SSRF against the local server :

İçerik :This lab has a stock check feature which fetches data from an internal system.

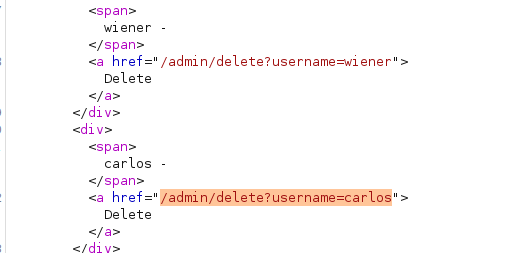
To solve the lab, change the stock check URL to access the admin interface at http://localhost/admin and delete the user carlos.

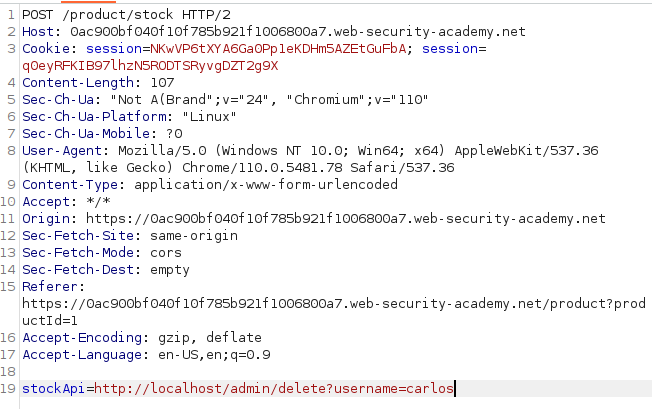
Lab Çözümü: Ürünlere baktığımız sayfada check stock kısmına tıkladığımda requestte stockApi gördüm ve administrator interface’e ulaşmak istediğim için url’i http://localhost/admin olarak değiştirdim.





Buradan Carlos’u direkt olarak silemiyoruz o yüzden nasıl silineceğine bakmak için response dan html koduna baktım.





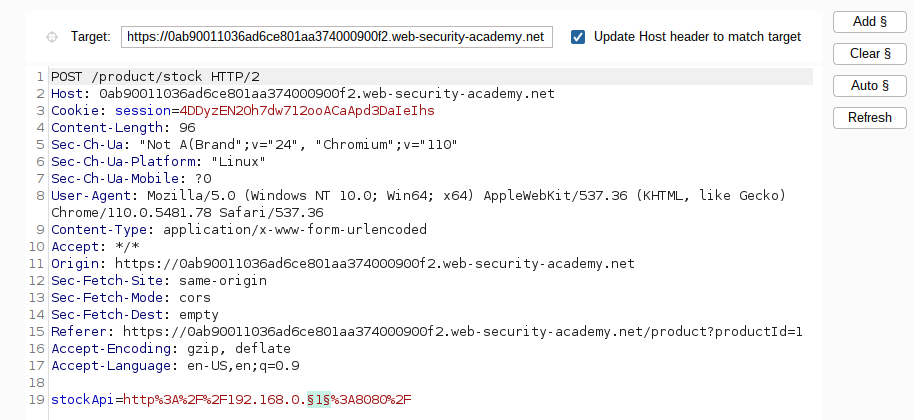
2.Basic SSRF against another back-end system:

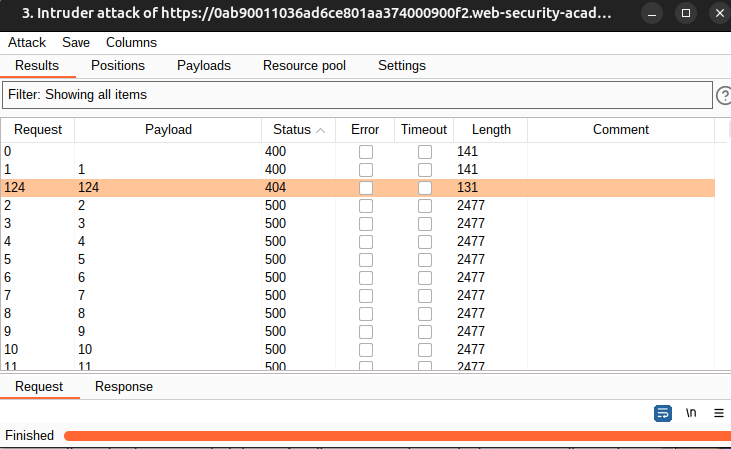
İçerik :This lab has a stock check feature which fetches data from an internal system.47

To solve the lab, use the stock check functionality to scan the internal 192.168.0.X range for an admin interface on port 8080, then use it to delete the user carlos.

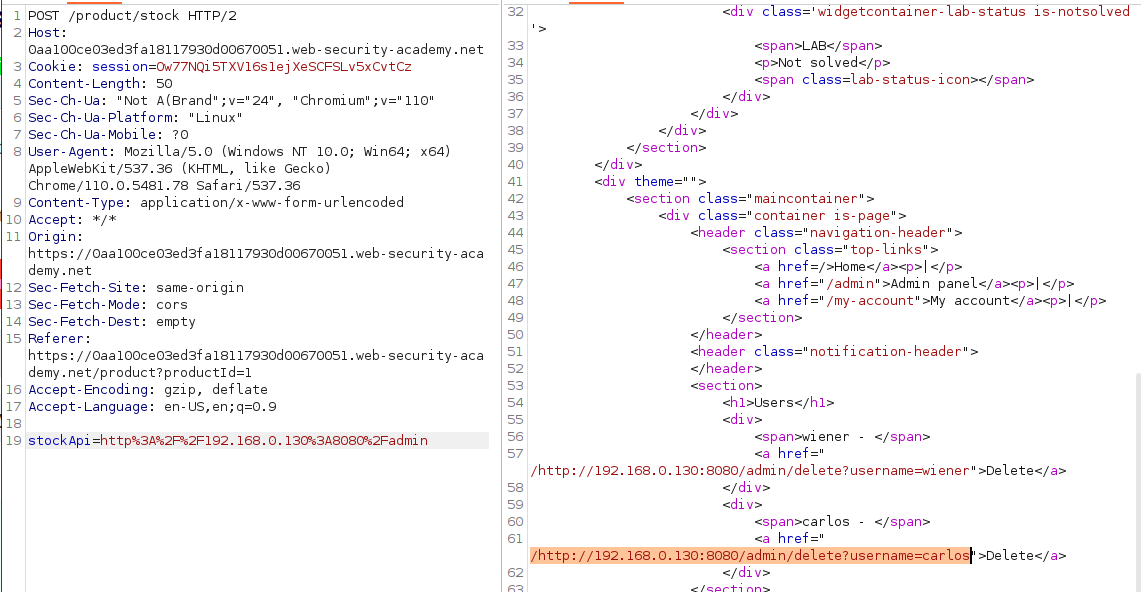
Lab Çözümü: Önceki labtaki gibi check stock kısmına tıkladığımızda requestte stockApi kısmını gördüm.

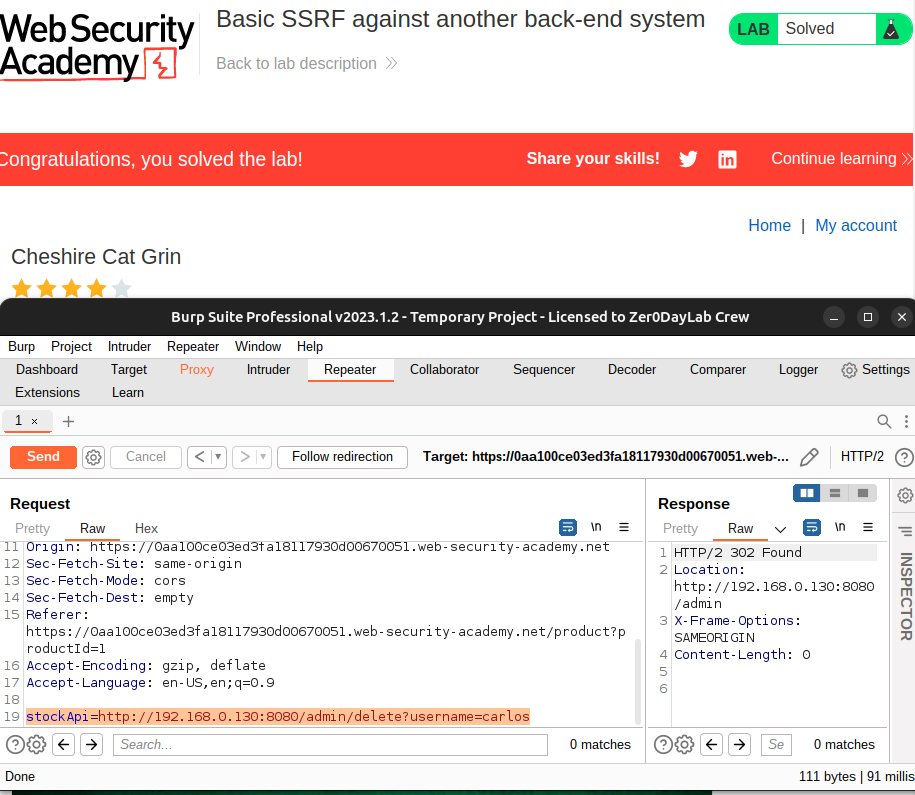
stockApi=http%3A%2F%2F192.168.0.1%3A8080%2F

Ve bizden istenilen 198.168.0.X in 8080 portunda çalışan admin arayüzünü bulabilmek. Bu yüzden isteği intruder a göndererek x kısmını 1-255 aralığı olmak üzere taradım.

Tarama sonucunda sadece 124’ten 404 Not Found döndü.Bu da sadece o Ip response verebiliyor demek.

stockApi=http%3A%2F%2F192.168.0.130%3A8080%2Fadmin

Yazıp response okuduğumuzda carlosu nasıl sileceğimizi öğreniyoruz.



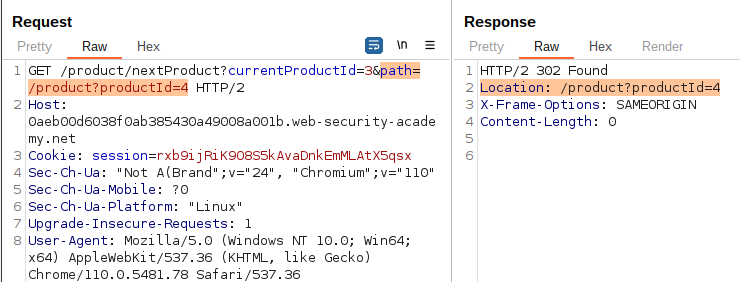
3.SSRF with filter bypass via open redirection vulnerability :

İçerik :This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at http://192.168.0.12:8080/admin and delete the user carlos.

The stock checker has been restricted to only access the local application, so you will need to find an open redirect affecting the application first.

Lab Çözümü: Ürünler sayfasında next product kısmına tıkladığımda redirection sağladığını gördüm. Location’ı path’ten alıyor ve biz path’te istediğimiz http isteğini çalıştıyor hale geliyoruz.



Pathi http://192.168.0.12:8080/admin olarak düzenleyip ürünün stok kısmındaki stockApi ‘ a attığımızda response’dan carlos kullanıcısını nasıl sileceğimizi görüyoruz.

