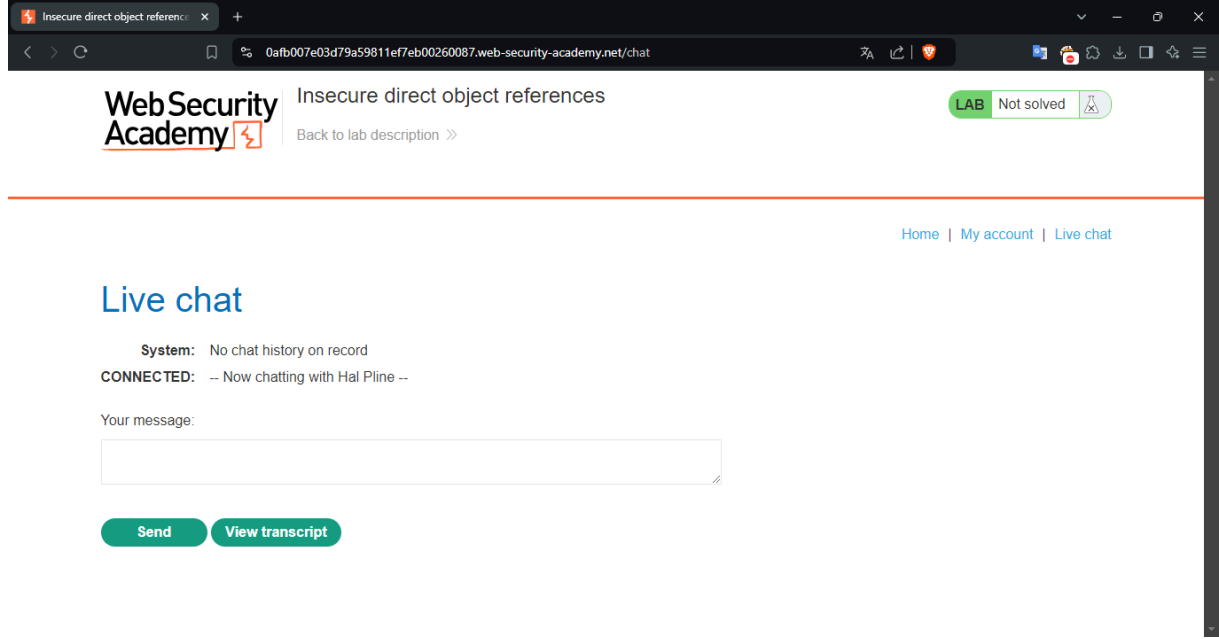


Broken Access Control

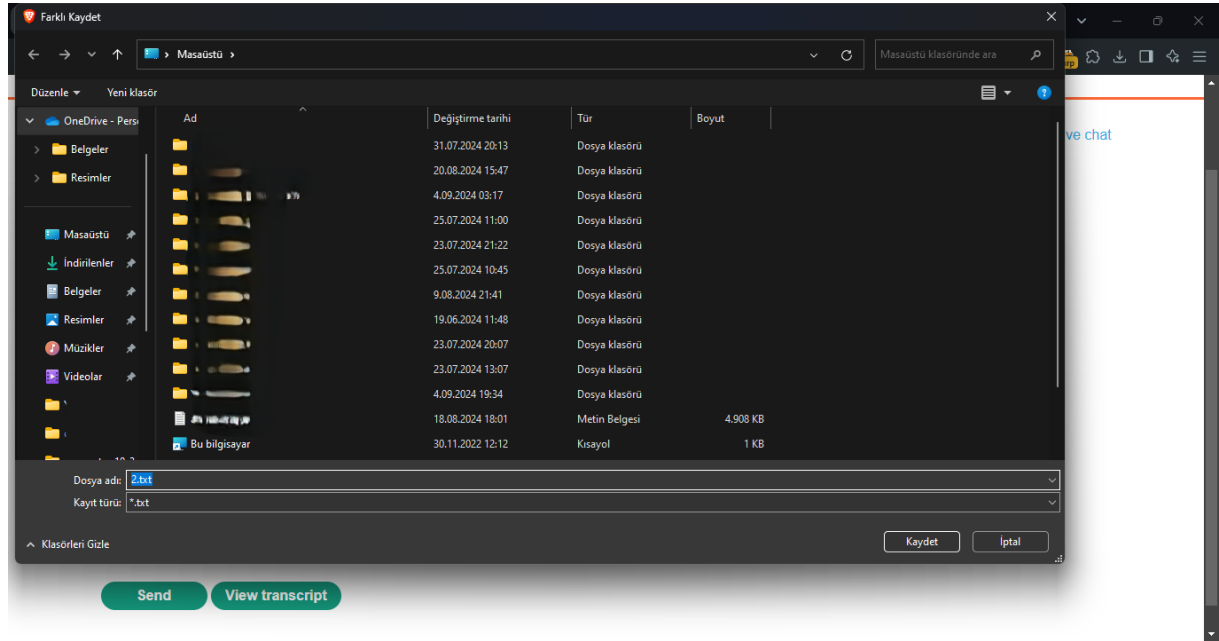
LAB_1: Insecure Direct Object References (IDOR)

Laboratuvar hedef olarak *carlos* isimli kullanıcının şifresinin bulunmasını ve giriş yapılmasını istiyor. Çözüm içinde sohbet kayıtlarını direkt olarak sunucudan dosya sistemine aktardığını ve URL'de barındırdığını söylüyor. Demek ki burada hedefimiz sohbet kısmı...

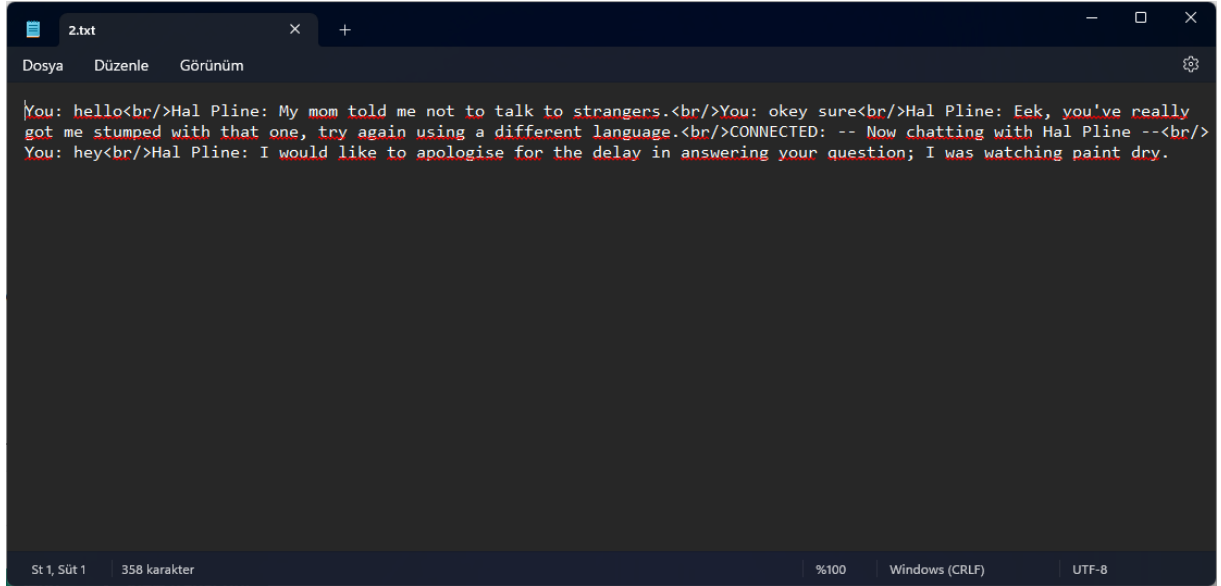


Direkt olarak chat kısmına giriş yaptım. Burada biraz mesaj göndermeyi deneyelim.

Mesajlaşma sırasında herhangi bir http paketi yakalanmadığı için transcript göster butonuna basıyorum ve olacak olayları inceliyorum.



Bu şekilde bir kaydetme penceresi bizi karşıladı. 2.txt isimindeki dosyayı indirmek istiyor.



```
You: hello<br/>Hal Pline: My mom told me not to talk to strangers.<br/>You: okey sure<br/>Hal Pline: Eek, you've really got me stumped with that one, try again using a different language.<br/>CONNECTED: -- Now chatting with Hal Pline --<br/>You: hey<br/>Hal Pline: I would like to apologise for the delay in answering your question; I was watching paint dry.
```

İçeriği bu şekilde.

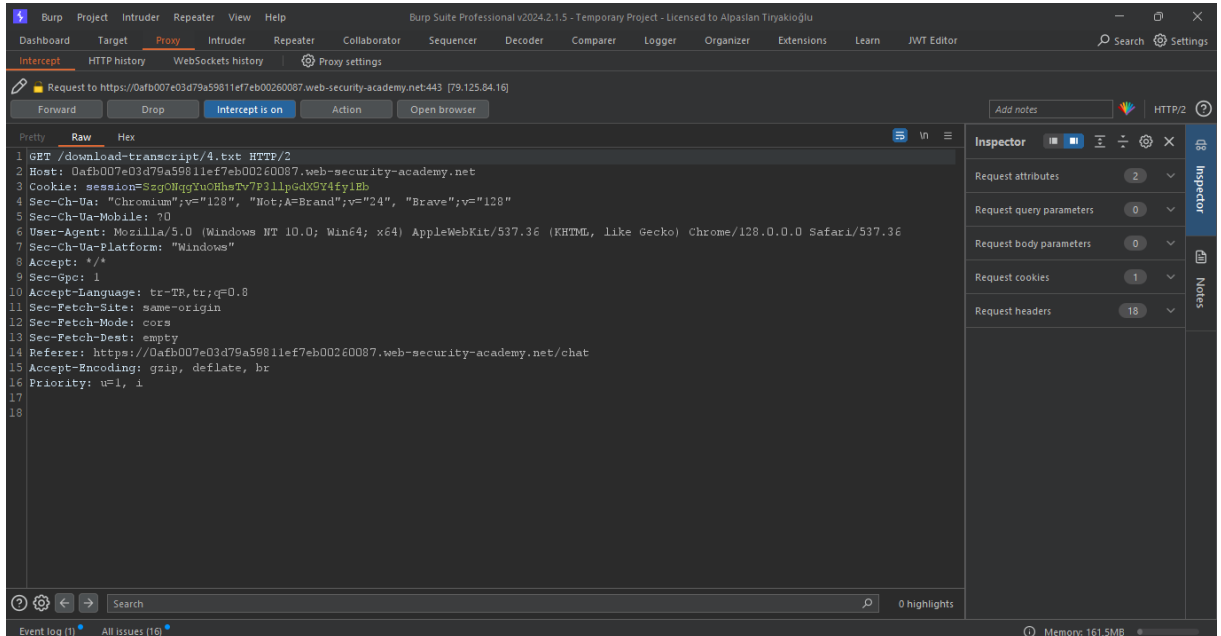


Dosya adı: 3.txt

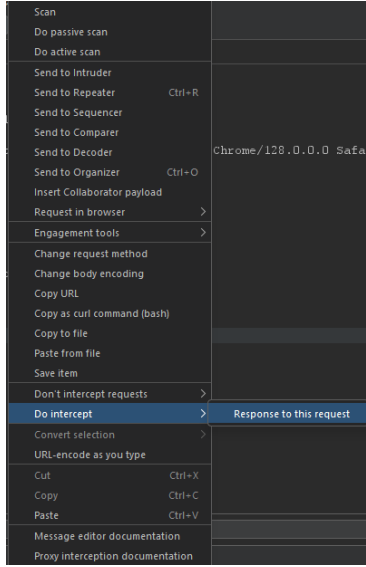
Kayıt türü: *.txt

Kaydet İptal

Tekrar denediğimde 3.txt olarak gittiğini görüyorum. Doğrusal bir şekilde arttığını düşünürsek başlangıç noktası olarak 2.txt vardı. 1.txt ile başlamamız gerekiyordu mantiken. Burp Suite ile araya girip paketi inceleyelim. En başta bize söylenen durumdaki gibi adres satırında bununla ilgili bir şey bulunabilir.



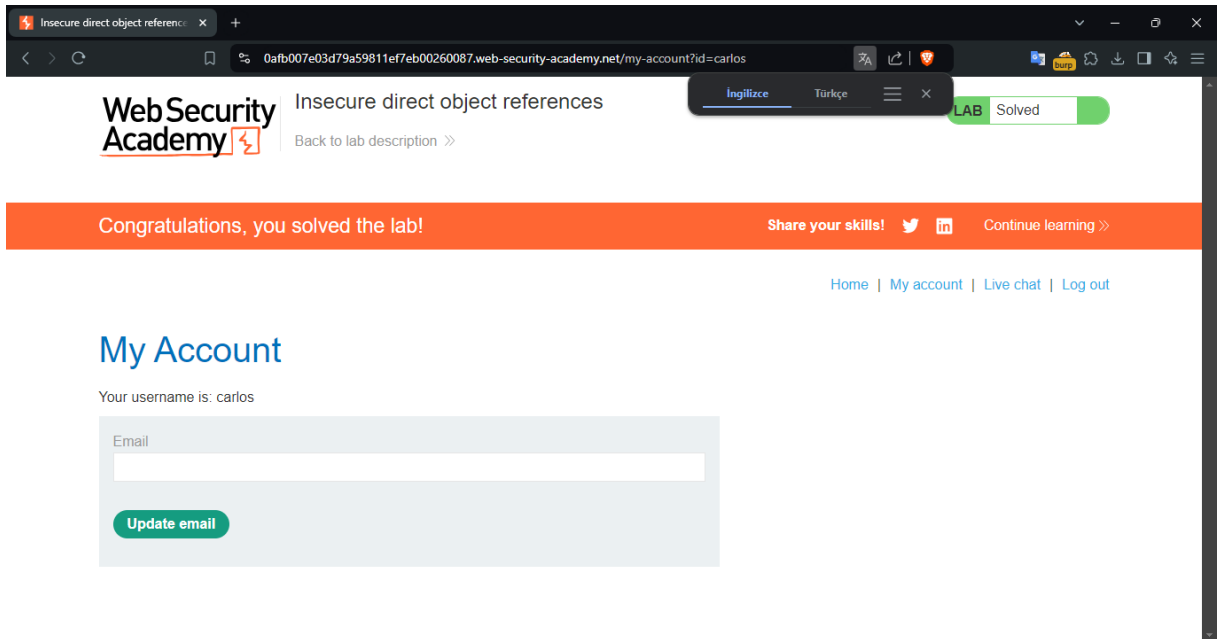
Proxy sekmesinde paketleri geçerken bunu görebiliriz. İstersek Repeater aracına gönderebilir istersek buradan direkt değişiklik yapabiliriz. Ben kısa yoldan buradaki değeri değiştiriyorum.



Buradaki özelliği de kullanarak bu paketten dönen response'u görebiliyoruz.

```
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="1.txt"
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 520
6
7 CONNECTED: -- Now chatting with Hal Pline --
8 You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
9 Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
10 You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
11 Hal Pline: Takes one to know one
12 You: Ok so my password is m24x184pliq0qhzc0eyy. Is that right?
13 Hal Pline: Yes it is!
14 You: Ok thanks, bye!
15 Hal Pline: Do one!
16
```

Gördüğümüz gibi 1.txt dosyasının içeriği de http paketinde okunuyor. Buradan da şifre değerini elde edebiliriz.

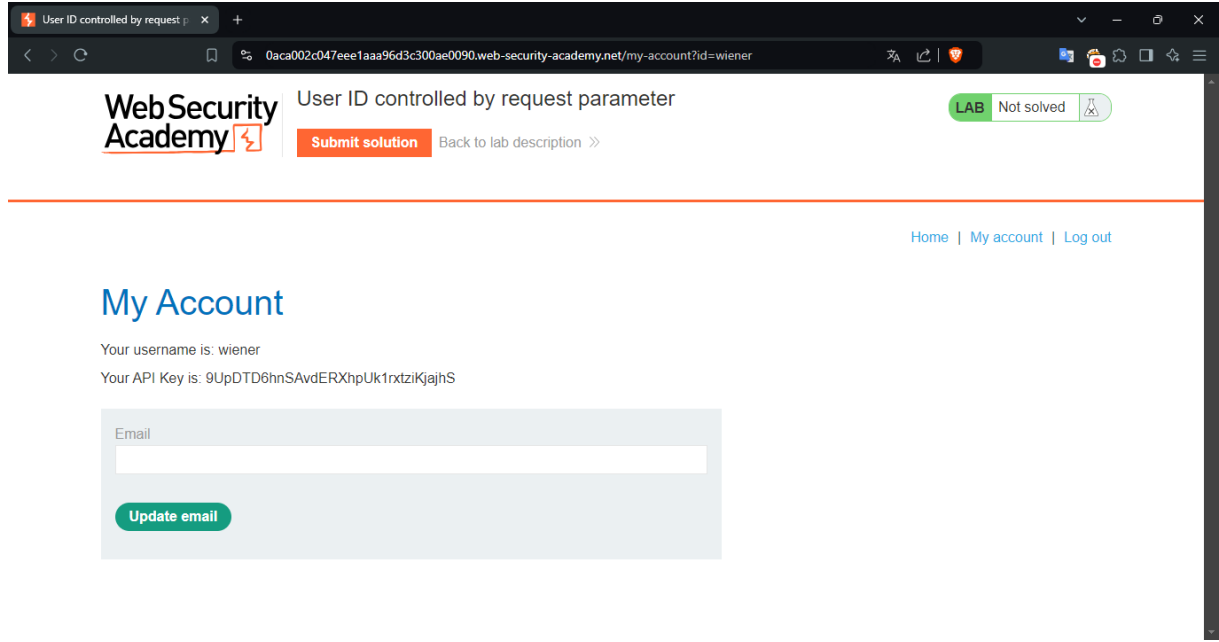


Görüldüğü gibi elde ettiğimiz credential ile giriş yaptık ve çözüme ulaştık. Bu şekilde IDOR zafiyetini istismar etmiş bulunduk.

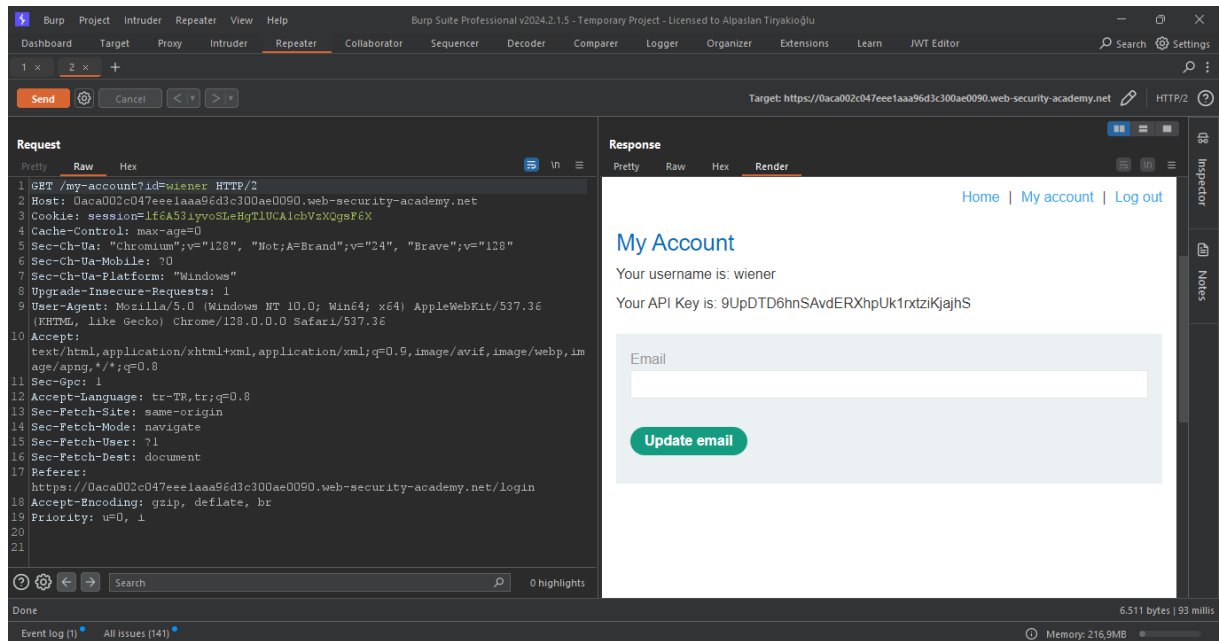
LAB_2: User ID controlled by request parameter

Laboratuvar açıklamasında kullanıcı hesabı sayfasında dikey yetki yükseltme zafiyetinin mevcut olduğu yazıyor. Çözmek için *carlos* kullanıcısının API anahtarını elde etmemizi istiyor. Ve varsayılan bir credentials verilmiş. *wiener:peter*

Bu açıklamaların siteye girer girmez kullanıcı hesabına giriş yapmaya çalışacağım.

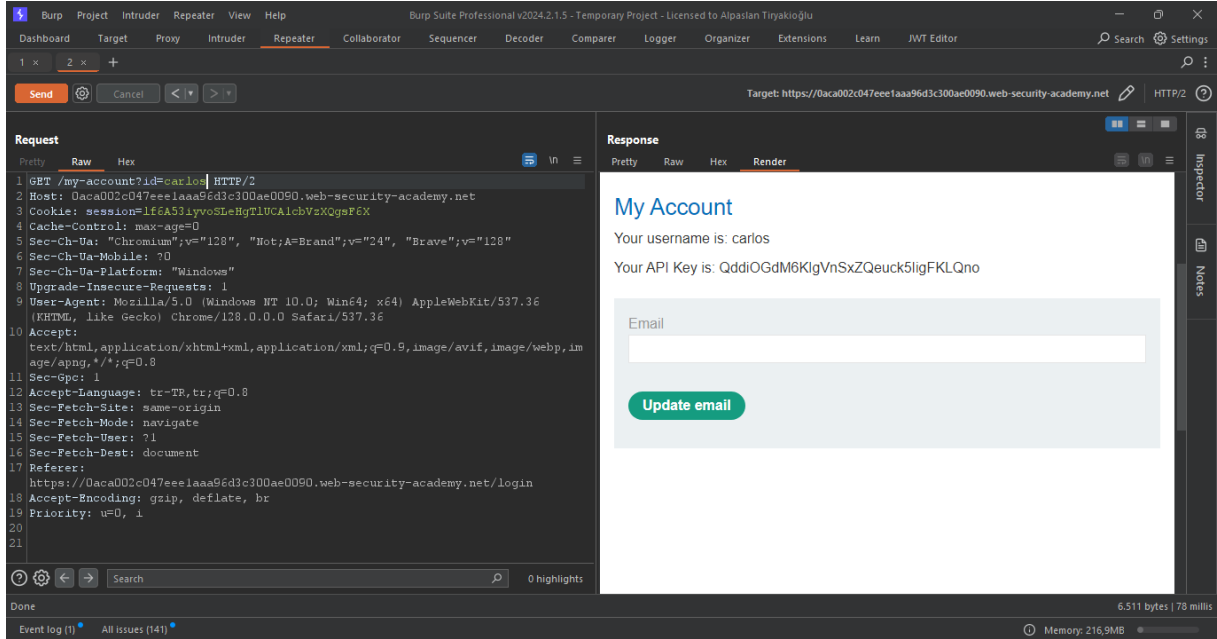


Verilen credential ile giriş yaptım ve bir key beni karşıladı. Bu tabi ki bizim ihtiyacımız olan değil. Burp suite ile login paketleri inceleyelim.

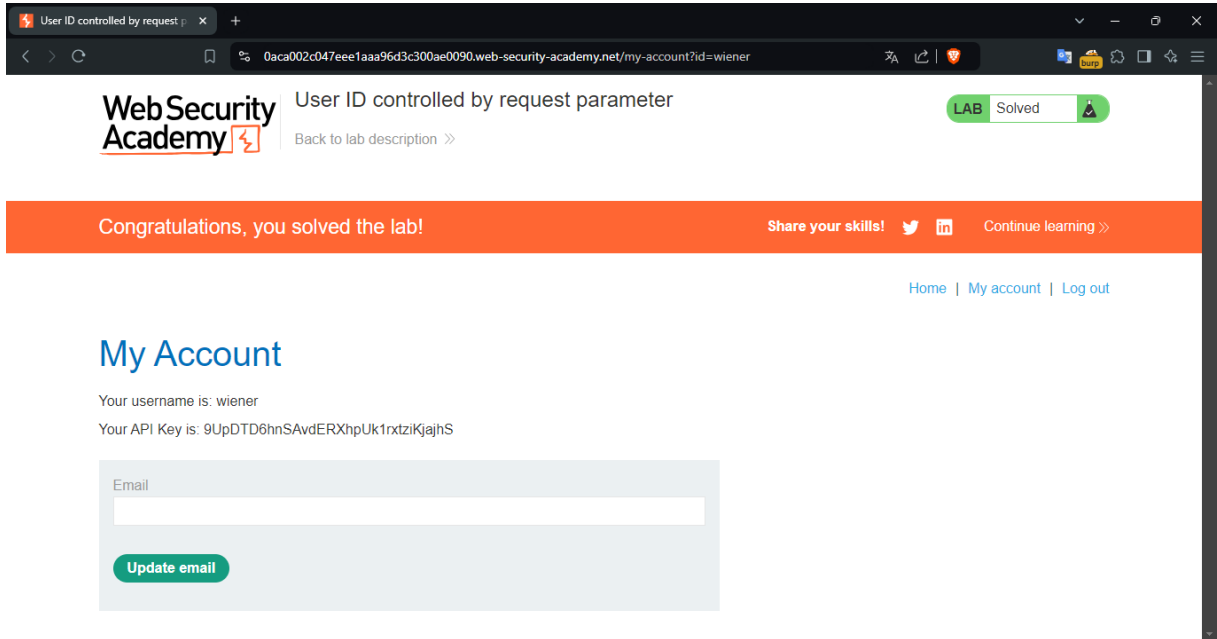


Hesaba giriş yaparken giden bir pakette direkt kullanıcı adının bulunduğunu tespit ettim ve bunu repeater aracına attım net görmek için. paketi gönderip render aldığımda bu görüntü ile

karşılaştım. Demek ki hangi kullanıcıyı yazarsam onu getirecek. O halde bunu *carlos* olarak değiştirirsem;



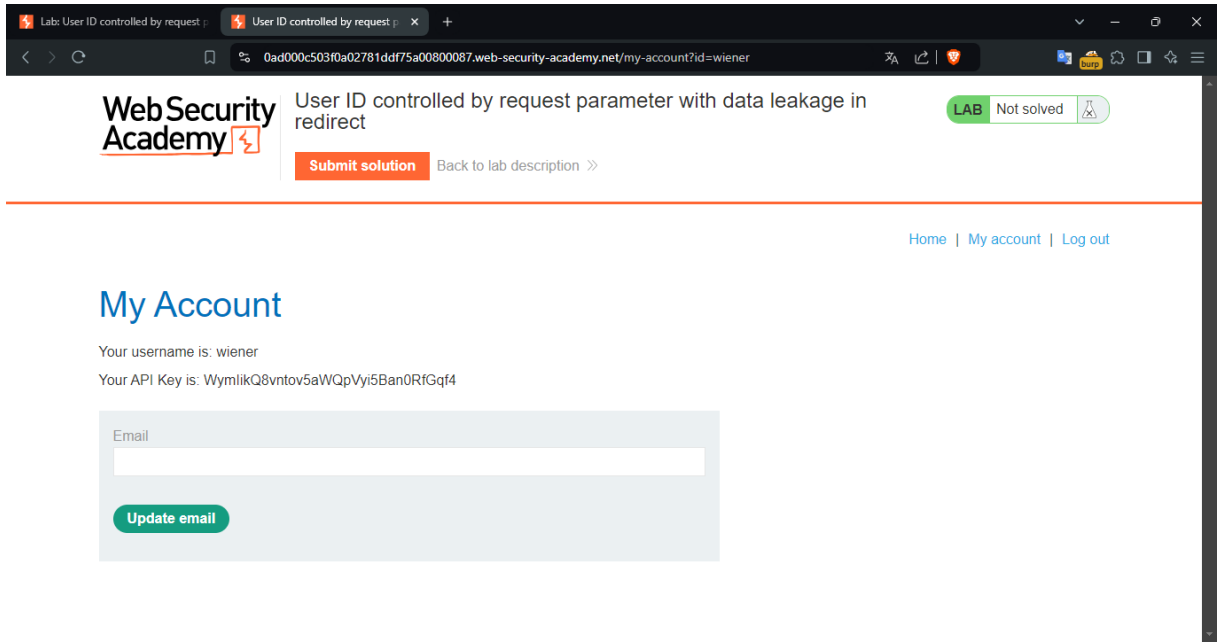
Farklı bir API anahtarı mevcut. Hemen Pretty kısmında anahtarı kopyalayıp gerçek sayfaya geldim. Çözüm kısmına anahtarı gönderdim. Sayfayı yenilediğimde;



Kullanıcı wiener olarak değişse de laboratuvarı çözmüş bulunuyoruz.

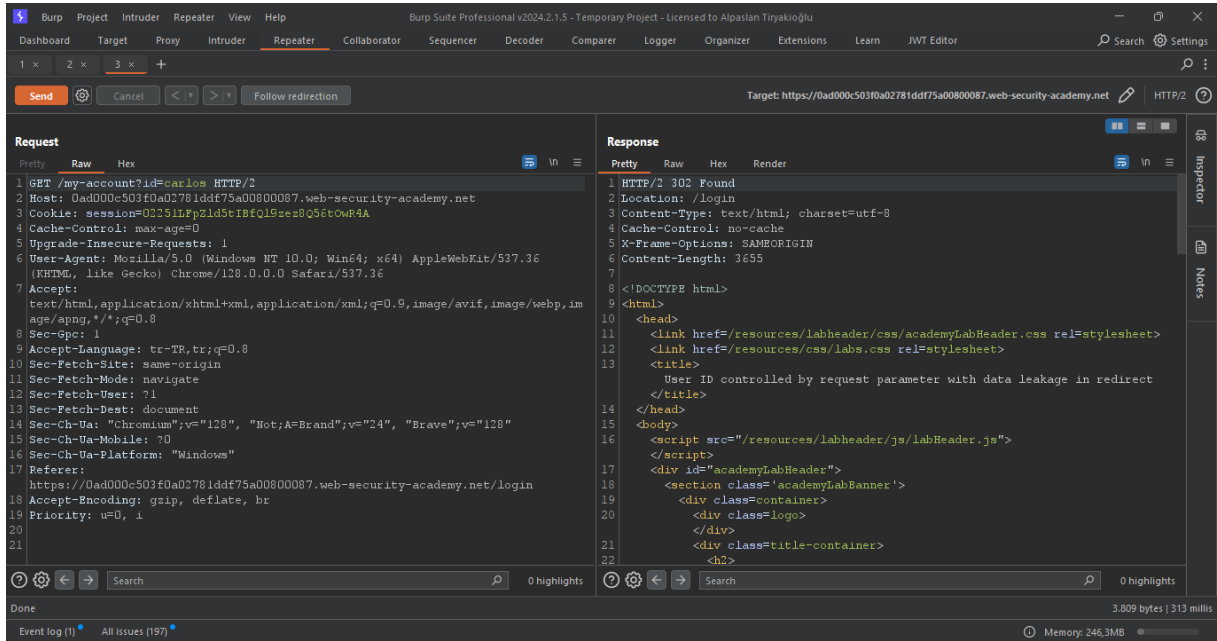
LAB_3: User ID controlled by request parameter with data leakage in redirect

Bu laboratuvarıda dönen response içerisinde hassas bir bilgi olduğunu ve bu bilgi ile erişim kontrolü zafiyeti olduğunu belirtiyor. Öncekinde olduğu gibi *carlos* kullanıcısının API anahtarını istiyor bizden. Verilen kullanıcı bilgileri ise *wiener:peter*

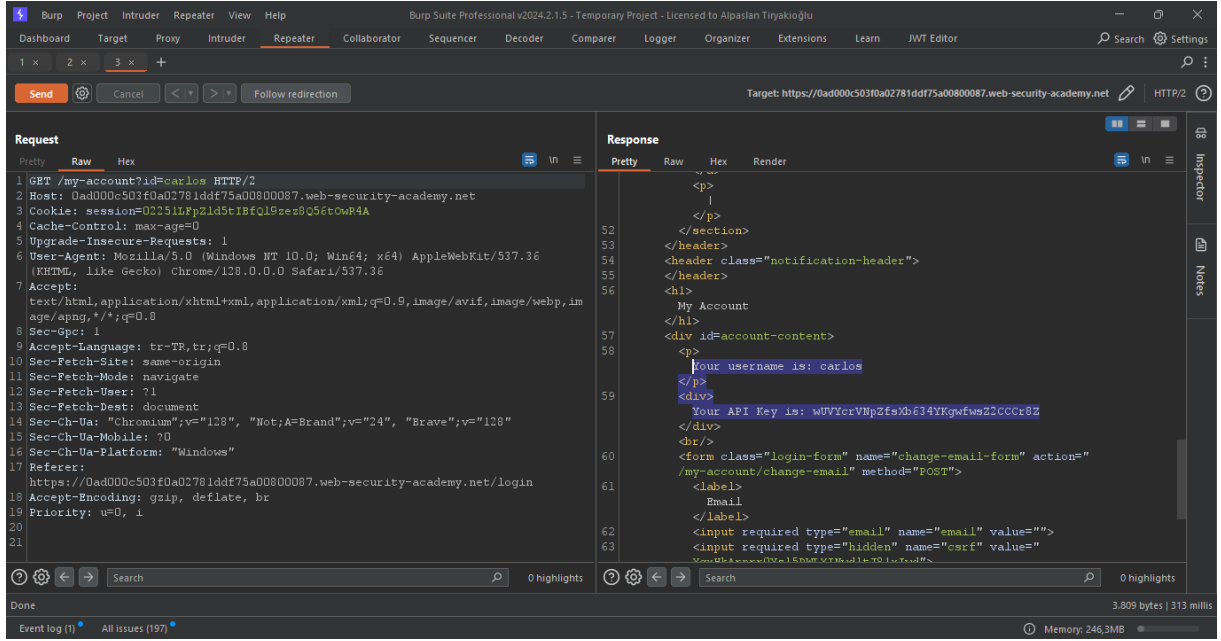


Verilen bilgiler ile giriş yaptıktan sonra bir farklılık olmadığını gördüm ve burp suite ile paketlere tek tek bakacağım.

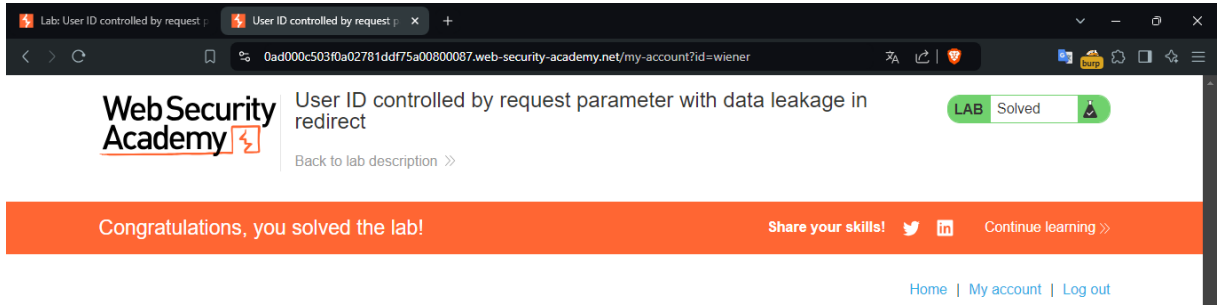
İlk aşamada kaynak kodunda da herhangi bir hassas veri elde edemedim. Önceki laboratuvarıda olduğu gibi parametreyi *carlos* yapıp deneyelim.



302 Found yani yönlendirme işlemi gerçekleşecek. Nereye olduğu da yazıyor. Ancak dikkat çeken kısım aşağıda dokuman nereyse tamamen yüklenmiş. Render aldığım zaman gerçek sayfanın yönlendirmeden önce yüklendiğini görebilirim.



Kod kısmında da bu şekilde görünüyor. Alıp çözüme kavuşturuyorum.



Broken Access Control kategorisi ile ilgili laboratuvar çözümleri tamamlandı.