

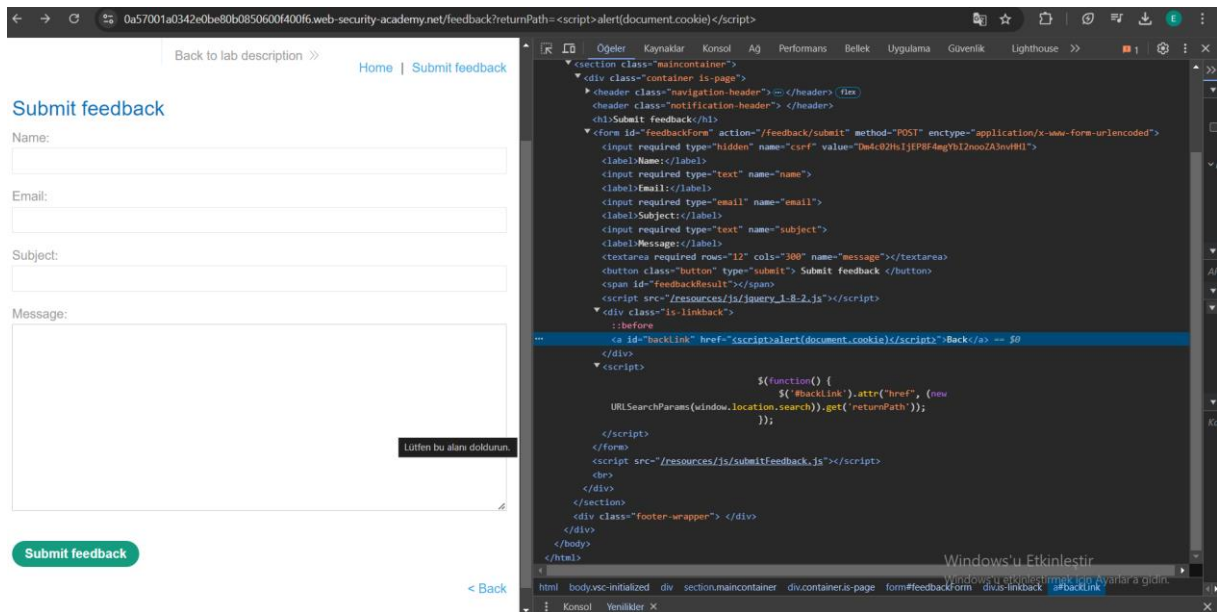
XSS (Cross Site Scripting)

1) Lab: DOM XSS in jQuery anchor href attribute sink using location.search source

<https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-jquery-href-attribute-sink>

Lab açıklamasında back tuşunu kullanmam gerektiğini belirtmiş bunun için sitede biraz gezindikten sonra back tuşunun olduğu yerleri tespit ettim ve incelemeye başladım.

Submit feedback kısmındaki url dikkatimi çekti.



Back için yazılmış script;

< script >

\$(function() {

\$('#backLink').attr("href", (new

URLSearchParams(window.location.search)).get('returnPath'));

});

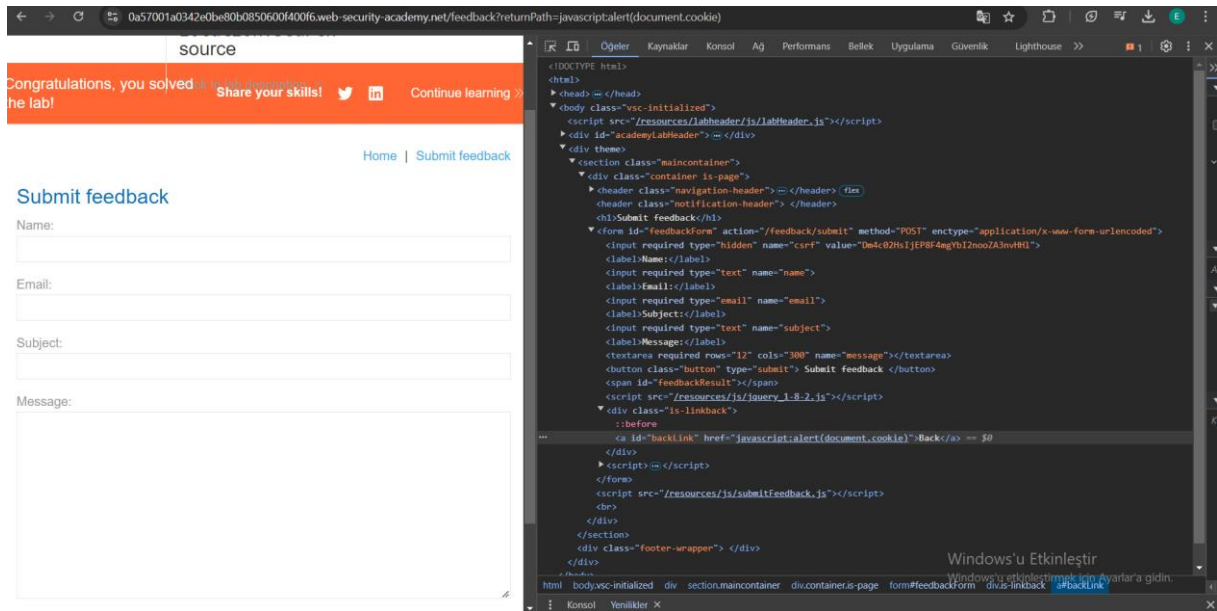
</ script >

get('returnPath')) kısmı url deki “?returnPath=” parametresinde bir şey olup olmadığına bakıyor orijinalinde ?returnPath=/ şeklinde bulunuyor ve back tuşunun “href” ögesini ?returnPath= kısmında yazan parametreye göre ayarlıyor.

Labda bize document.cookie yi tetiklememiz gerektiğini belirttiği için

Buna uygun payload deniyorum.

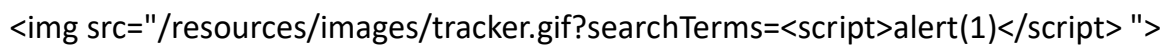
Payload: javascript:alert(document.cookie)



2) Lab: DOM XSS in document.write sink using source location.search

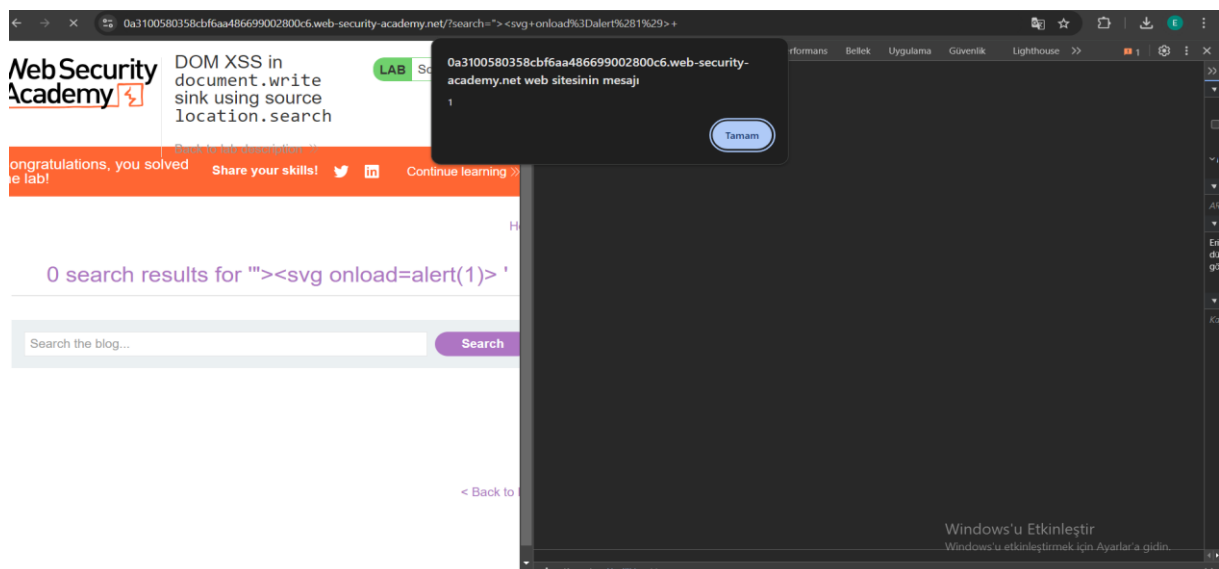
<https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink>

Payloadını denediğimde, denediğim payloadın



Mantığı ">" ile img etiketinden çıkıp yeni bir etiket eklemeye çalışmadan geliyor.

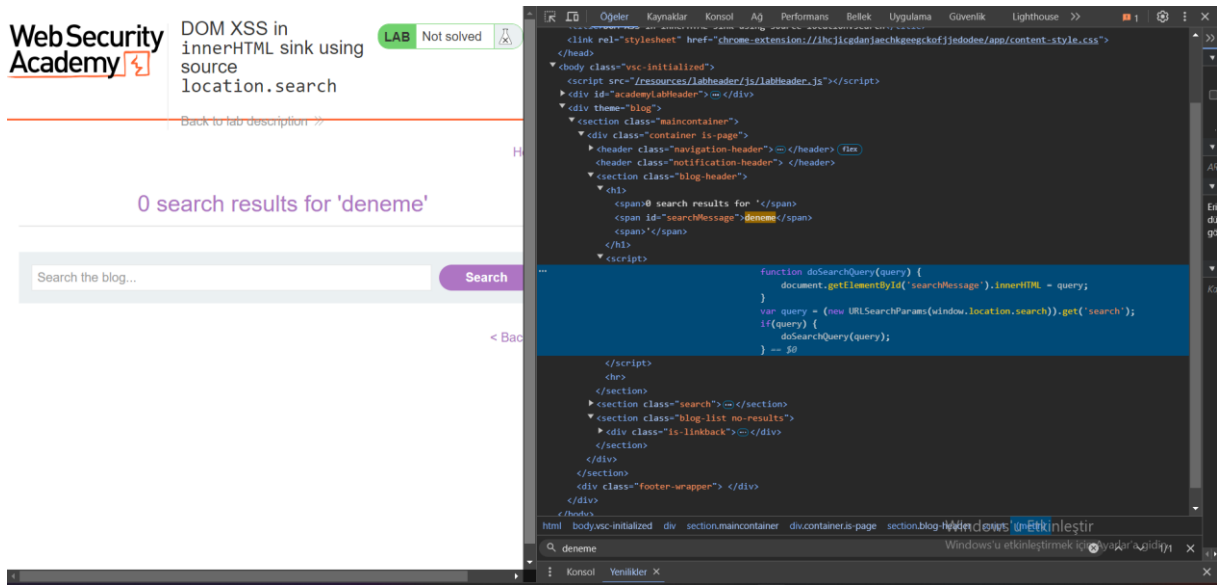
Payloadı denedğimizde çalışıyor.



<https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-innerhtml-sink>

The screenshot shows a web browser with the URL `0a-c900f904a85c988371e2cb00640005.web-security-academy.net/?search=<%2fscript>+<script>alert(1)</script>`. The page title is "WebSecurity Academy" and the main content area shows "0 search results for ''". The search bar contains the text "<script>alert(1)</script>" and a "Search" button. The developer tools are open, showing the HTML structure. The "section.blog-list no-results" element is highlighted. The console shows the execution of the script: `<script>alert(1)</script>`.

Sayfa kaynağını incelediğimde arama kısmı için şöyle bir script e denk geldim.



<script>

function doSearchQuery(query) {

document.getElementById('searchMessage').innerHTML = query; }

var query = (new

URLSearchParams(window.location.search)).get('search');

if(query) {

doSearchQuery(query); }

</script>

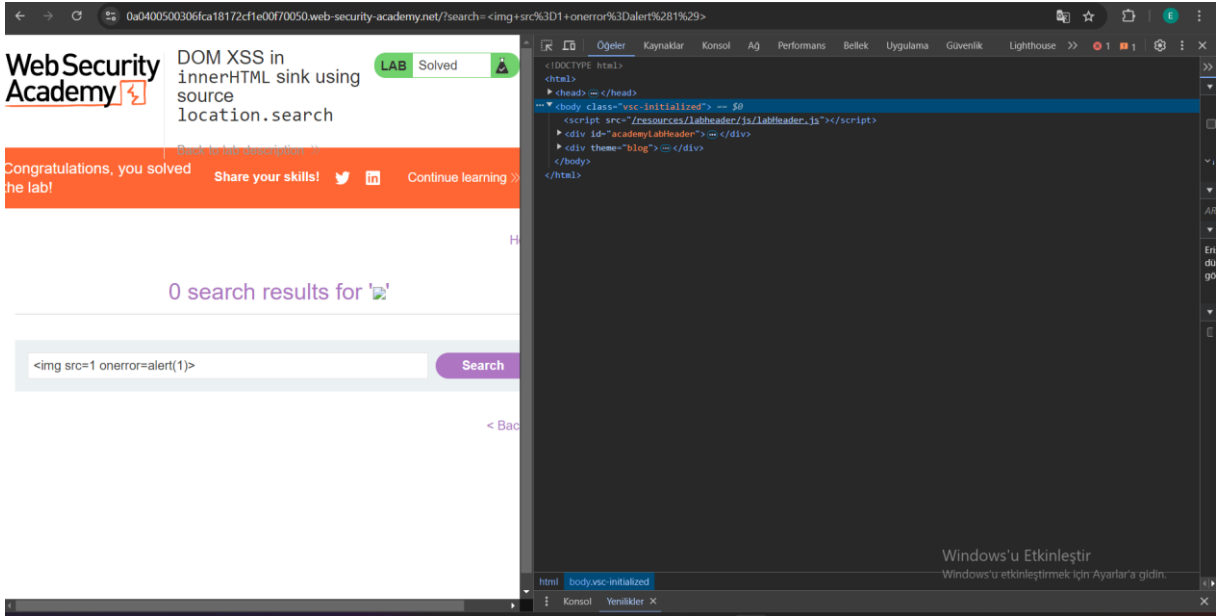
Bu kod, url deki "search" parametresini alıp sayfada yazdırıyor.

Url den "search" parametresi alır

Örneğin, "?search=deneme" ise query değişkeni "deneme" olur.

Sonrasında ise alınan parametre sayfadaki "searchMessage" olan yere eklenir.

Biz sayfada geçersiz src değerli bir resim yüklemeye çalışırsak hata verecektir. Ve `` payloadı ile bir hata ile karşılaştığında alert düşürmesini sağlamış olacağız.



Access Control

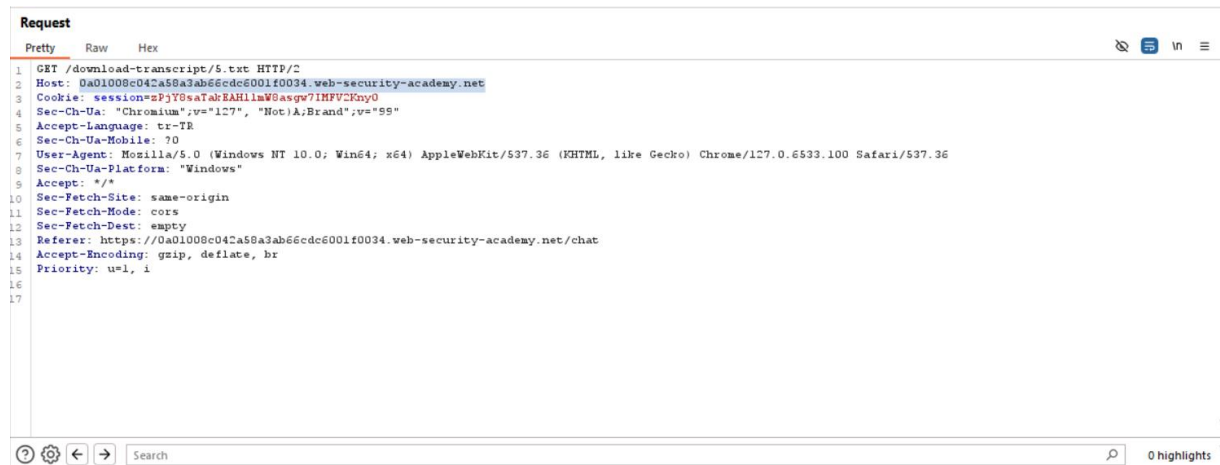
1)Lab: Insecure direct object references

<https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references>

Lab da verilen bilgide

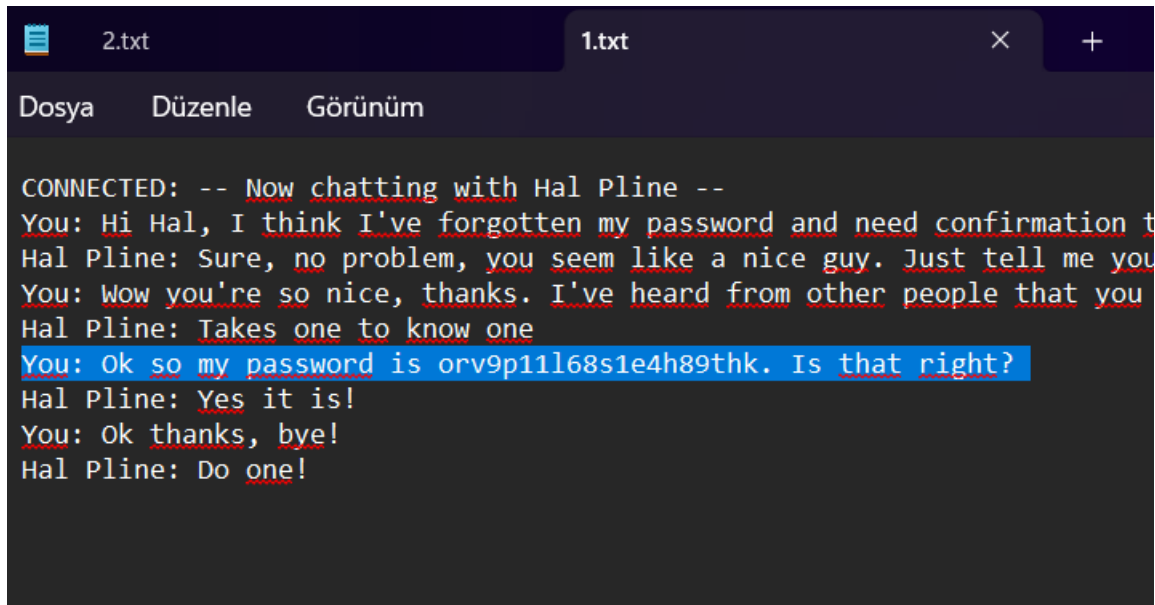
“Bu laboratuvar, kullanıcı sohbet kayıtlarını doğrudan sunucunun dosya sisteminde depolar ve bunları statik URL'ler kullanarak alır.”

İfadesi vardı ve direkt mesajlaşma kısmında zaafiyet aramaya başladım deneme mesajı attıktan sonra mesajlayı indirebildiğimi fark ettim ve indirmeyi denedim. 2.txt dosyası indirildi. 2 den başlaması dikkatimi ancak url e ulaşamadım bende Burp Suite kullanarak tekrar denedim ve



<http://0a01008c042a58a3ab66cdc6001f0034.web-security-academy.net/download-transcript/1.txt>

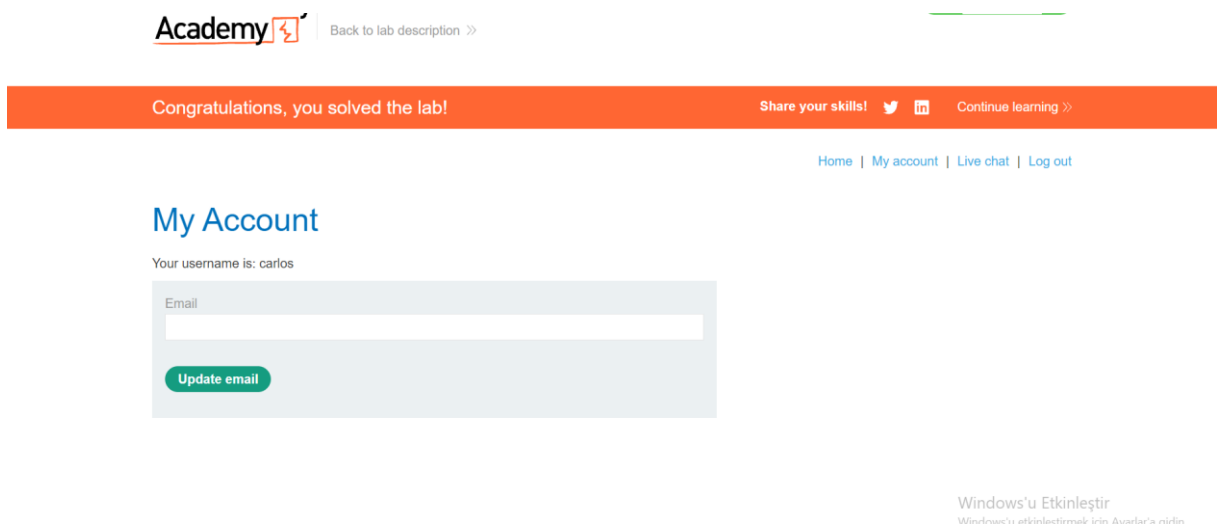
bu indirme linki sayesinde 1.txt dosyasına ulaştım.



The screenshot shows a terminal window with two tabs: '2.txt' and '1.txt'. The '1.txt' tab is active. The terminal has a dark background with light-colored text. At the top, there are menu options: 'Dosya', 'Düzenle', and 'Görünüm'. The chat conversation is as follows:

```
CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need confirmation t
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me you
You: Wow you're so nice, thanks. I've heard from other people that you
Hal Pline: Takes one to know one
You: Ok so my password is orv9p11l68s1e4h89thk. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!
```

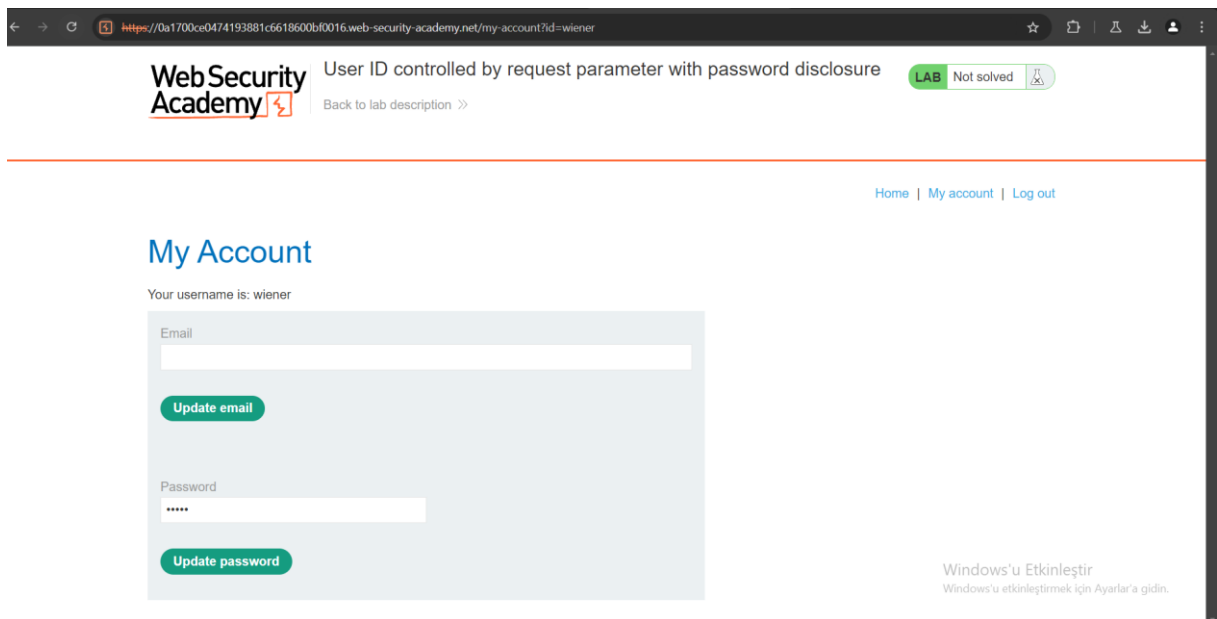
Txt dosyasından edindiğimiz şifre sayesinde Carlos un hesabına girdik.



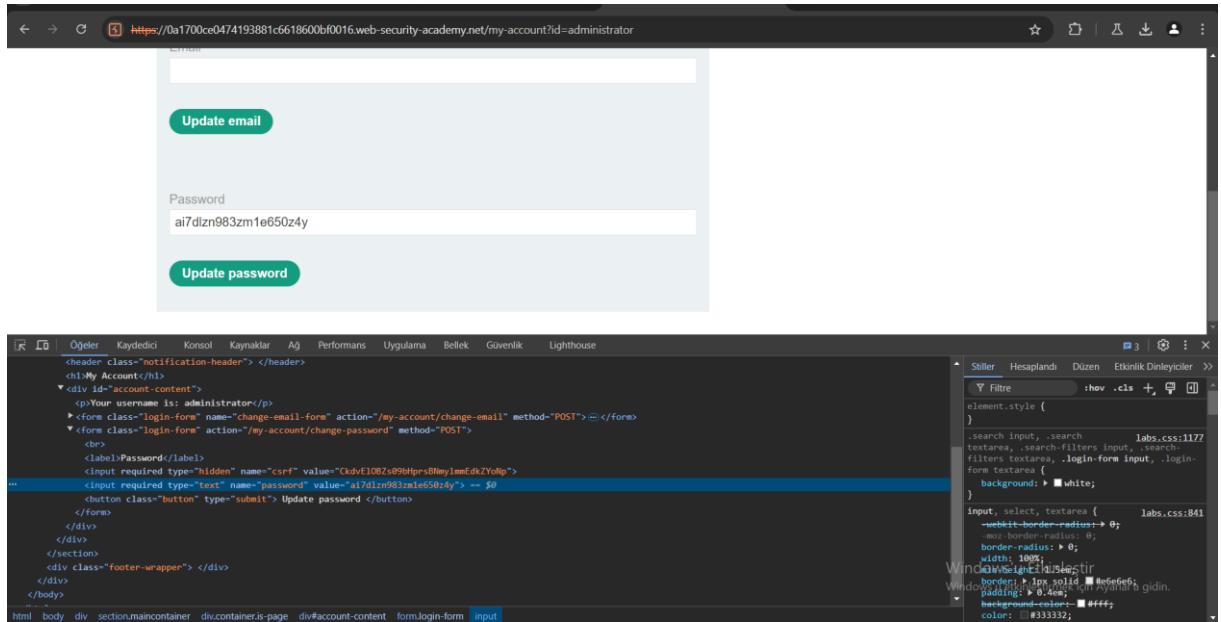
2) Lab: User ID controlled by request parameter with password disclosure

<https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-password-disclosure>

LABda verilen wiener peter bilgisi ile giriş yaptıktan sonra bizden bize Carlos kullanıcısı silmemizi istiyor. Ancak böyle bir seçenek olmadığı için önce BurpSuite ile http isteğinde admin kontrolü var mı diye kontrol ettim ancak bulamadım sonrasında urlde ki wiener dikkatimi çekti.

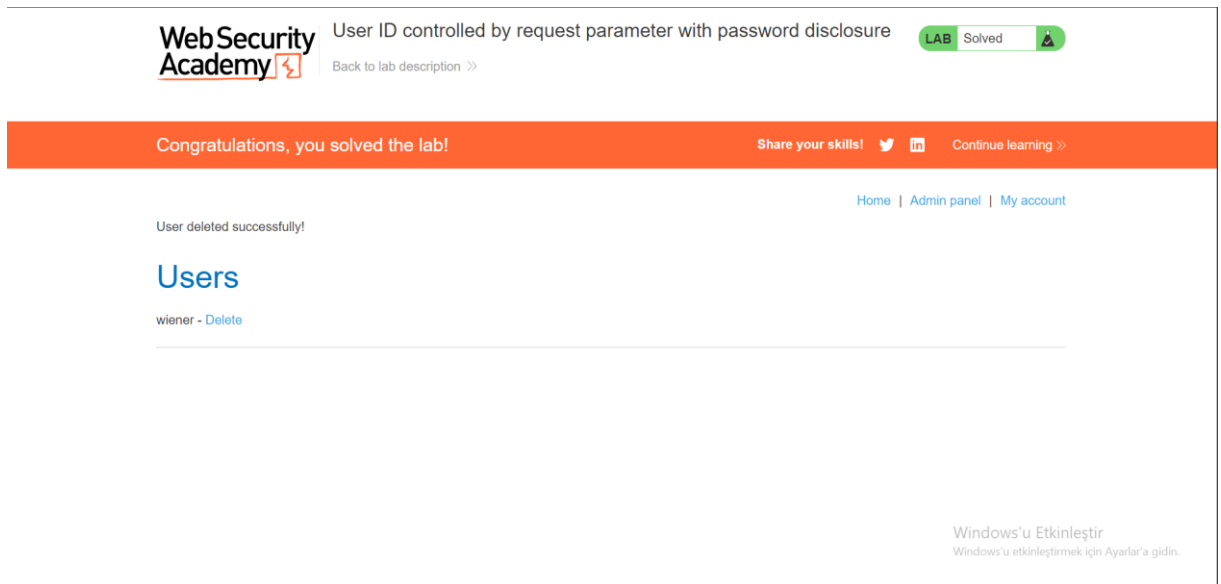


Wiener değiştirip admin ,administrator gibi kullanıcı adlarına sahip yetkilili bir kullanıcı olup olmadığını varsa geçiş yapıp yapamayacağımı denedim.



Administrator kullanıcısına direkt geçiş yaptı şifre yerinde bir şifre olduğunu gördüm type ı password yerine text olarak değişince şifre gözüksü.

Admin olarak giriş yaparak Carlos kullanıcısını sildik.



3) Lab: User ID controlled by request parameter with data leakage in redirect

<https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-data-leakage-in-redirect>

Labda verilen bilgilerle giriş yaptığımda bir API key verdiğini gördüm. Bizden Carlos un API key ine ulaşmamızı istiyordu.

Hon

My Account

Your username is: wiener

Your API Key is: M8duC6P6BcqW9ZwMiUJzYgddssSUj7At

Email

Update email

Aynı şekilde url deki wiener ı değiştirip Carlos yapmak istediğimde giriş yapmadığını görünce Burp Suite ile tekrar denedim.

The screenshot shows the Burp Suite interface. The left pane displays a list of requests, with the first one selected: a POST request to /login. The right pane shows the details of the selected request in the 'Inspector' tab. The 'Request' tab shows the raw HTTP request, and the 'Response' tab shows the raw HTTP response. The 'Request' tab is currently active, showing the following details:

- Method: POST
- URL: /login
- Host: 0a1e004503820e4800e867a500040034.web-security-academy.net
- Content-Type: application/x-www-form-urlencoded
- 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,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Dest: document
- Referer: https://0a1e004503820e4800e867a500040034.web-security-academy.net/login
- Accept-Encoding: gzip, deflate, br
- Priority: u=0, i

The 'Response' tab shows the following details:

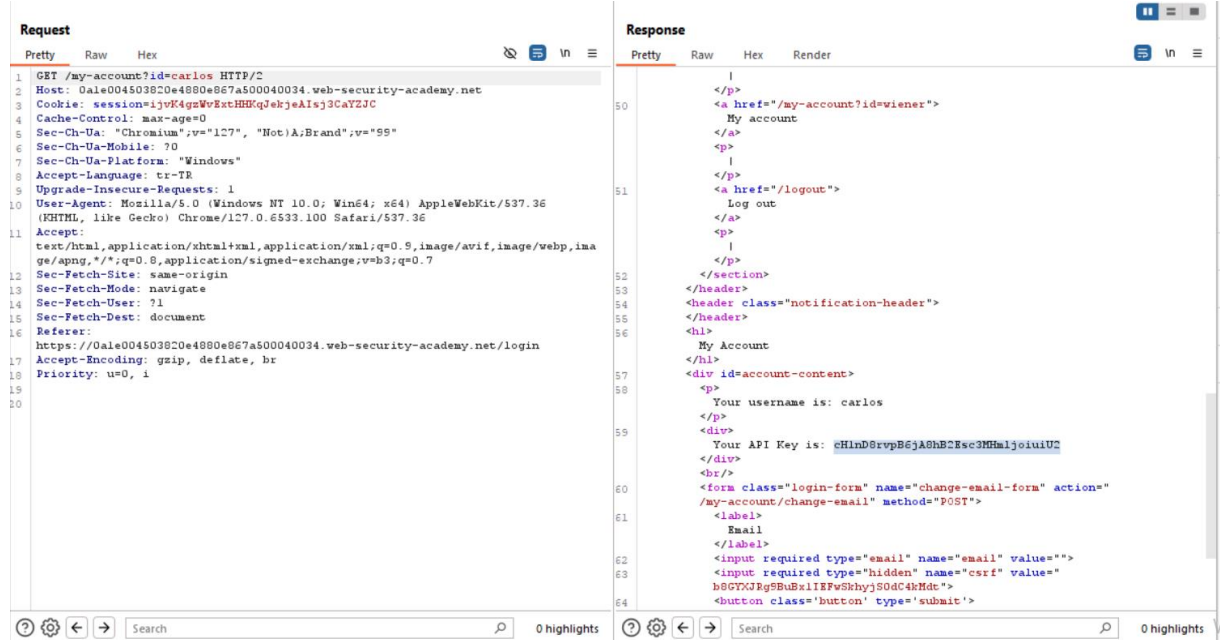
- Status: 200
- Content-Type: text/html
- Content-Length: 69
- Cache-Control: max-age=0
- Sec-CH-UA: "Chromium",v="127", "NotA;Brand",v="99"
- Sec-CH-UA-Mobile: 70
- Sec-CH-UA-Platform: "Windows"
- Accept-Language: tr-TR
- Upgrade-Insecure-Requests: 1
- Origin: https://0a1e004503820e4800e867a500040034.web-security-academy.net
- Content-Type: application/x-www-form-urlencoded
- 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,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Dest: document
- Referer: https://0a1e004503820e4800e867a500040034.web-security-academy.net/login
- Accept-Encoding: gzip, deflate, br
- Priority: u=0, i

The 'Request' tab shows the raw HTTP request, and the 'Response' tab shows the raw HTTP response. The 'Request' tab is currently active, showing the following details:

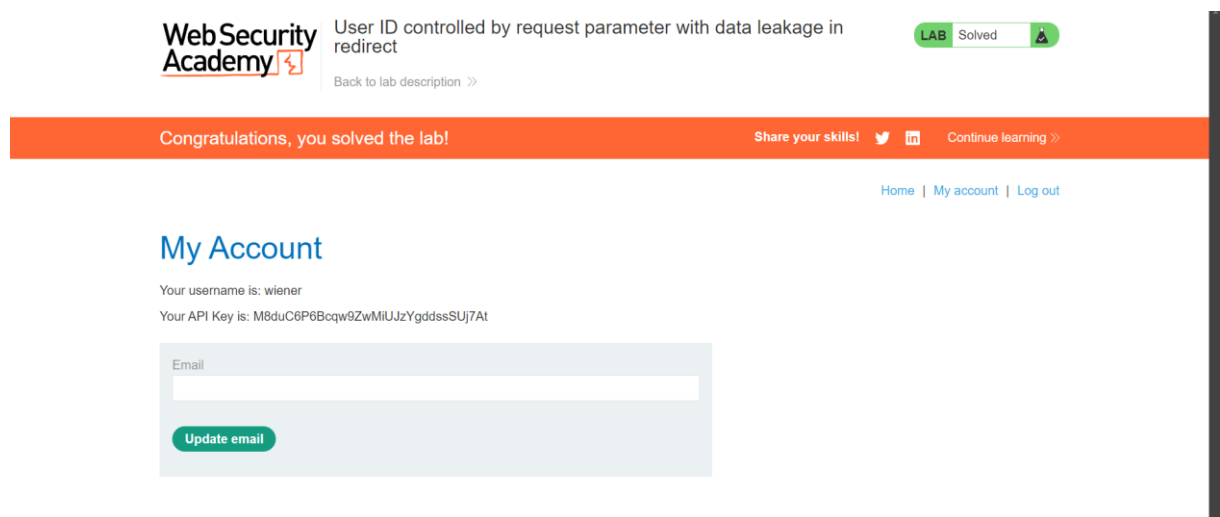
```
POST /login HTTP/2
Host: 0a1e004503820e4800e867a500040034.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 69
Cache-Control: max-age=0
Sec-CH-UA: "Chromium",v="127", "NotA;Brand",v="99"
Sec-CH-UA-Mobile: 70
Sec-CH-UA-Platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
Origin: https://0a1e004503820e4800e867a500040034.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
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,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0a1e004503820e4800e867a500040034.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

The 'Response' tab shows the raw HTTP response, which is a 200 status code with a content type of text/html. The response body is a redirect to the user's account page.

Carlos olarak değiştirmem bir şeyi değiştirmedim.



Bende repetar a tarak birde orda denedim ve Carlos un api key ine ulaşmış oldum.



Ve cevap kısmına yapıştırdığımda lab çözülmüş oldu.