

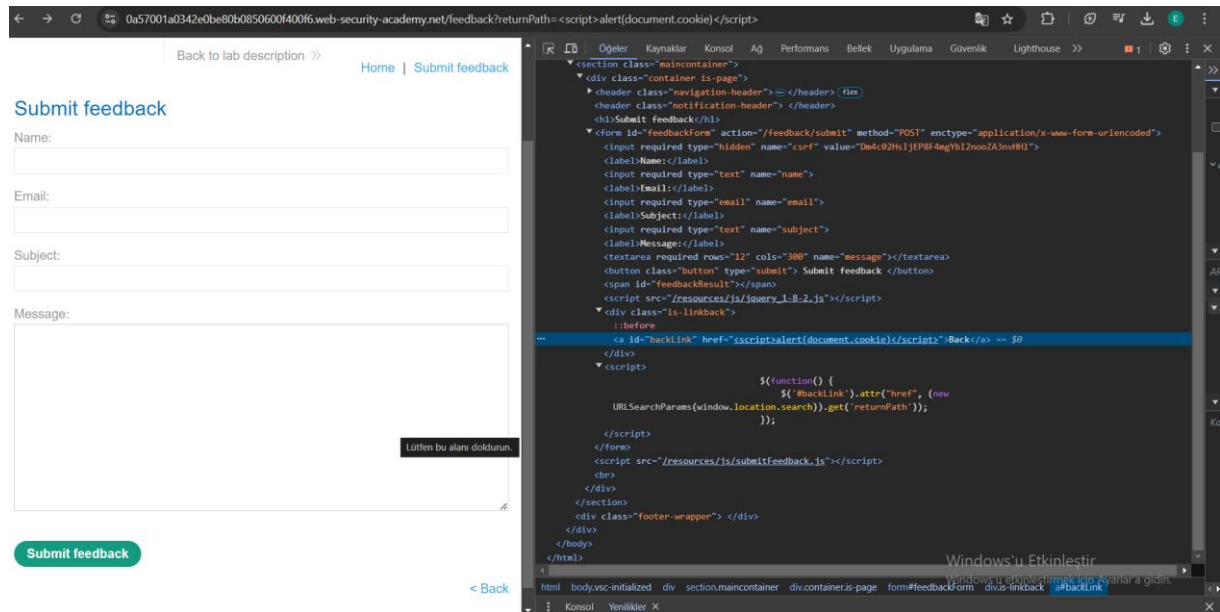
XSS (Cross Site Scripting)

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'));

});

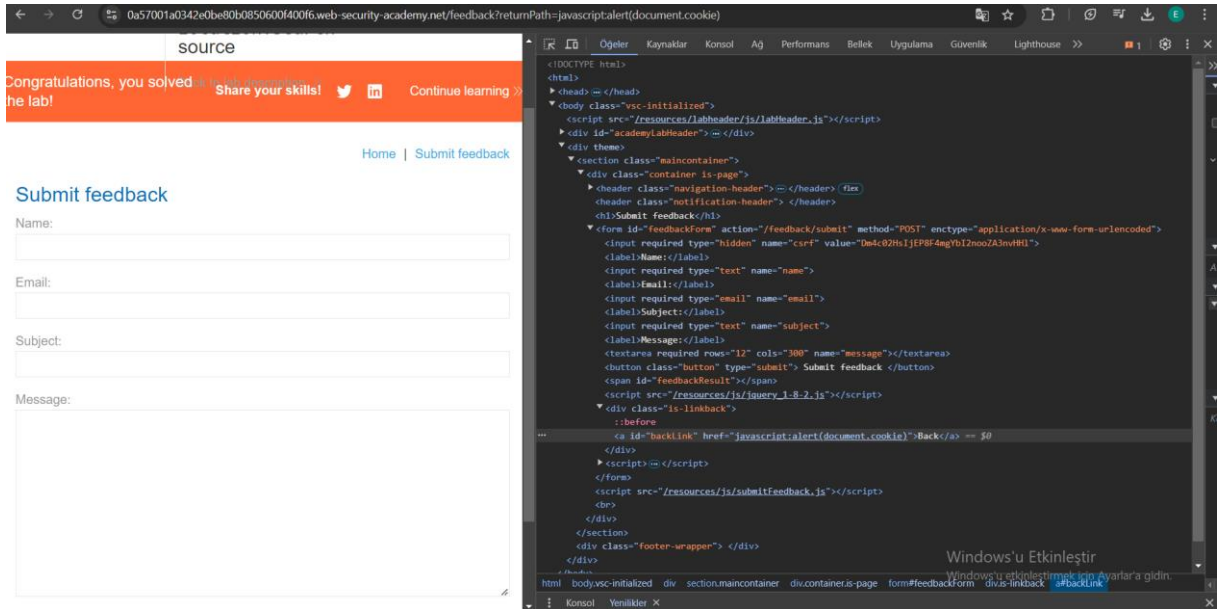
</ script >

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)

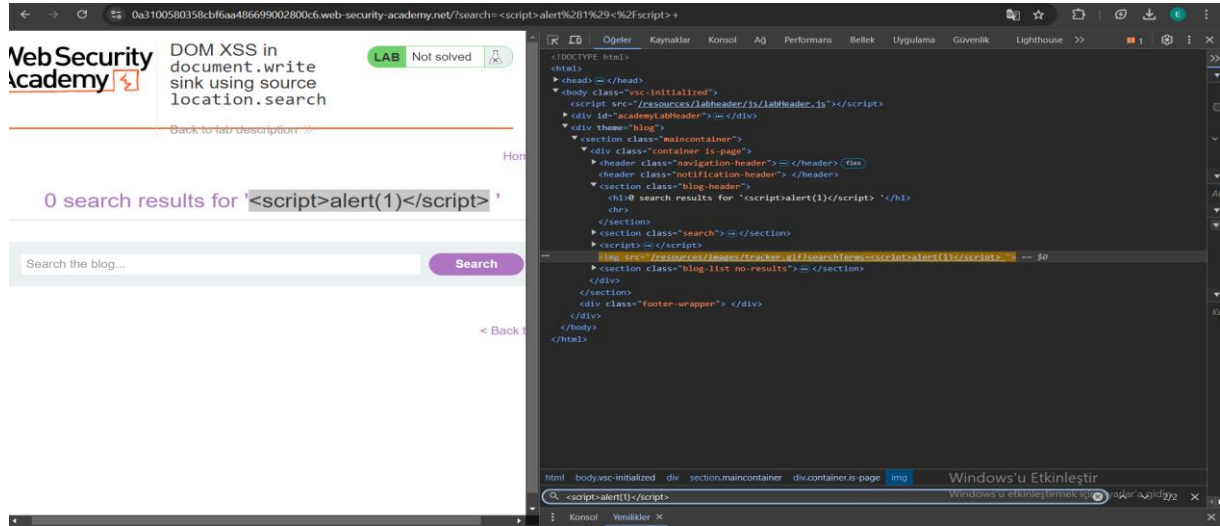


2) Lab: DOM XSS in document.write sink using source location.search

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

LAB da verilen açıklamda arama işlevselliği ile ilgili olduğu bilgisini vermiş.
Search kısmında deneme amaçlı `<script>alert(1)</script>`

Payloadını dendiğimde, dendiğim payloadın

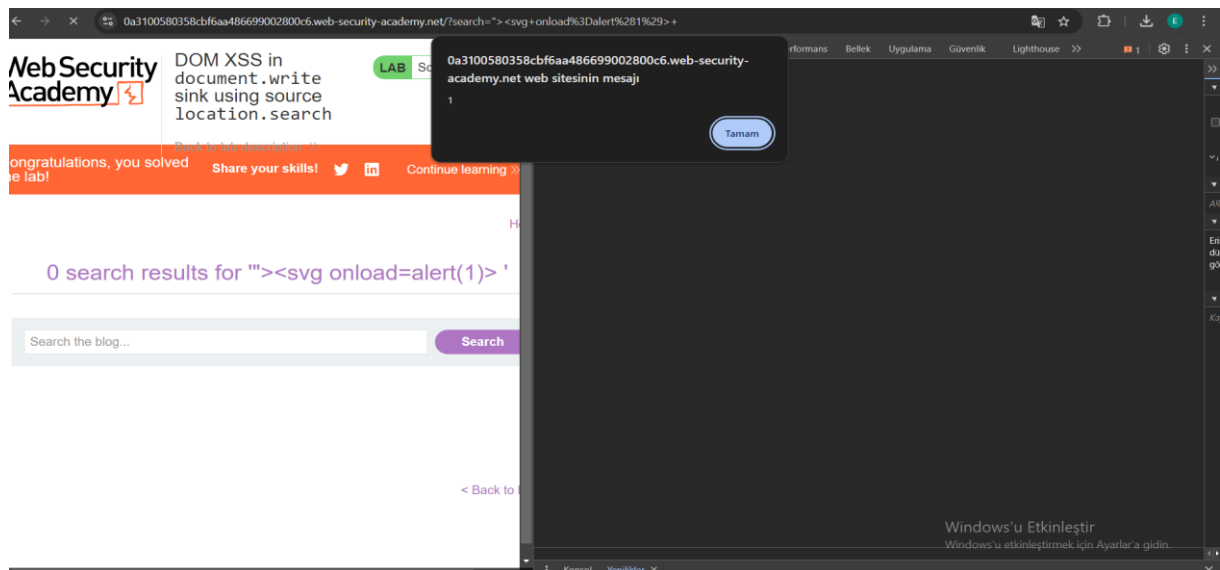


``

İçerisinde kullanıldığını gördüm ve önceki çözdüğüm lablardan dolayı aklıma direkt `"><svg onload=alert(1)>` payloadı geldi.

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

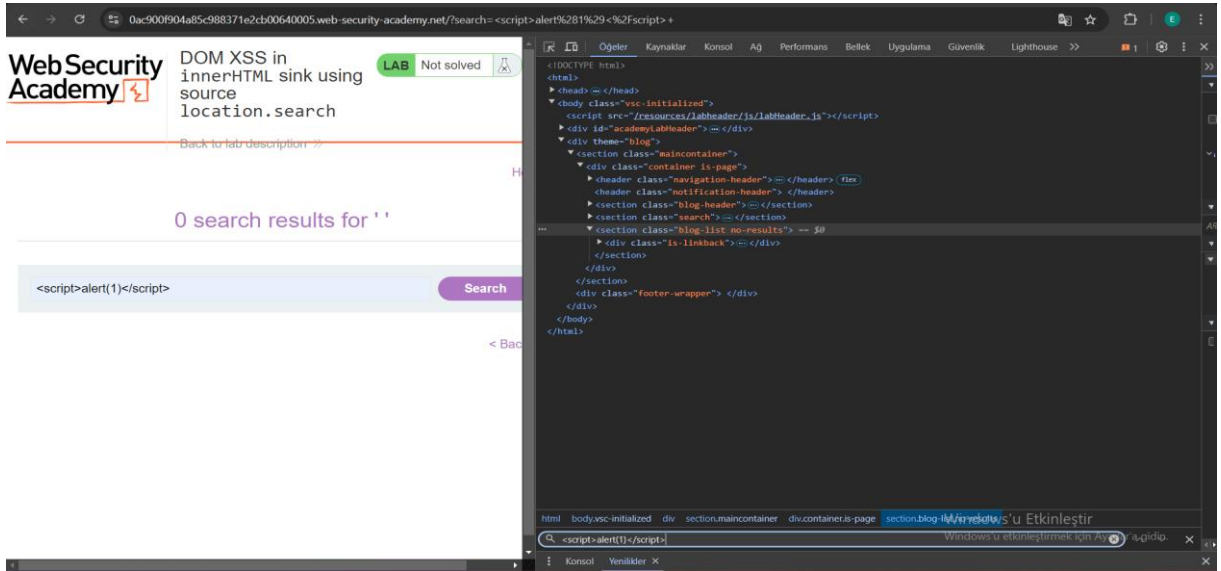
Payloadı dendiğimizde çalışıyor.



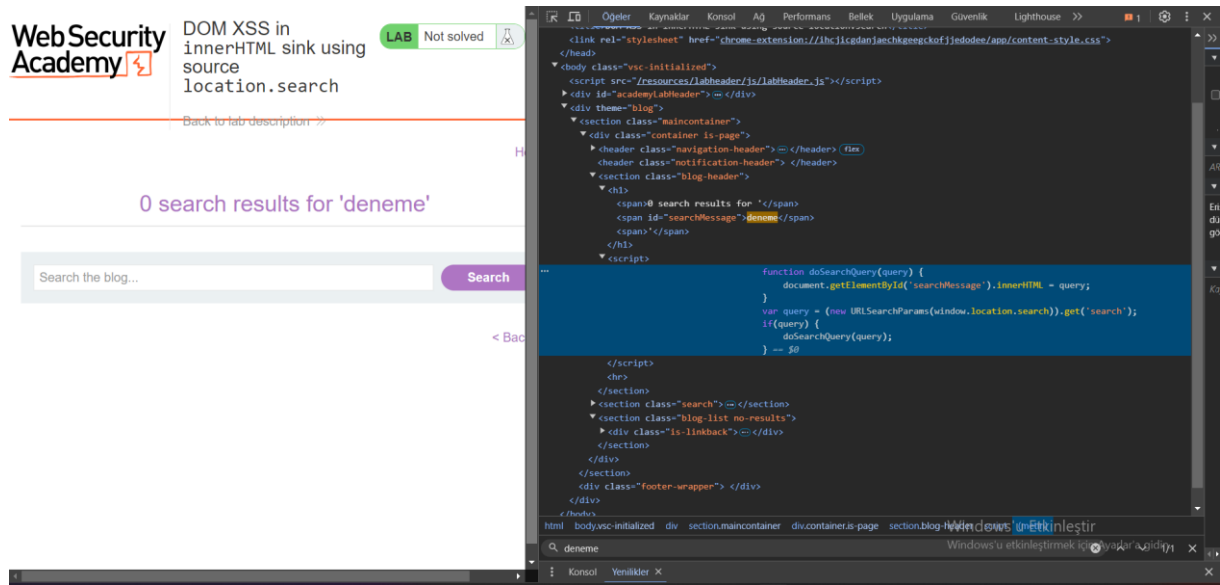
3) Lab: innerHTMLLab: Kaynak kullanarak havuzda DOM XSSlocation.search

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

LAB da verilen açıklamda arama işlevselliği ile ilgili olduğu bilgisini vermiş. Deneme amaçlı `<script>alert(1)</script>` payloadını arattığımda aranan metin olarak veya incele dediğimde hiçbir yerde göremedim buda bana arka tarafta kullanıldığını ama alert düşürmediğini düşündürdü.



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>
```

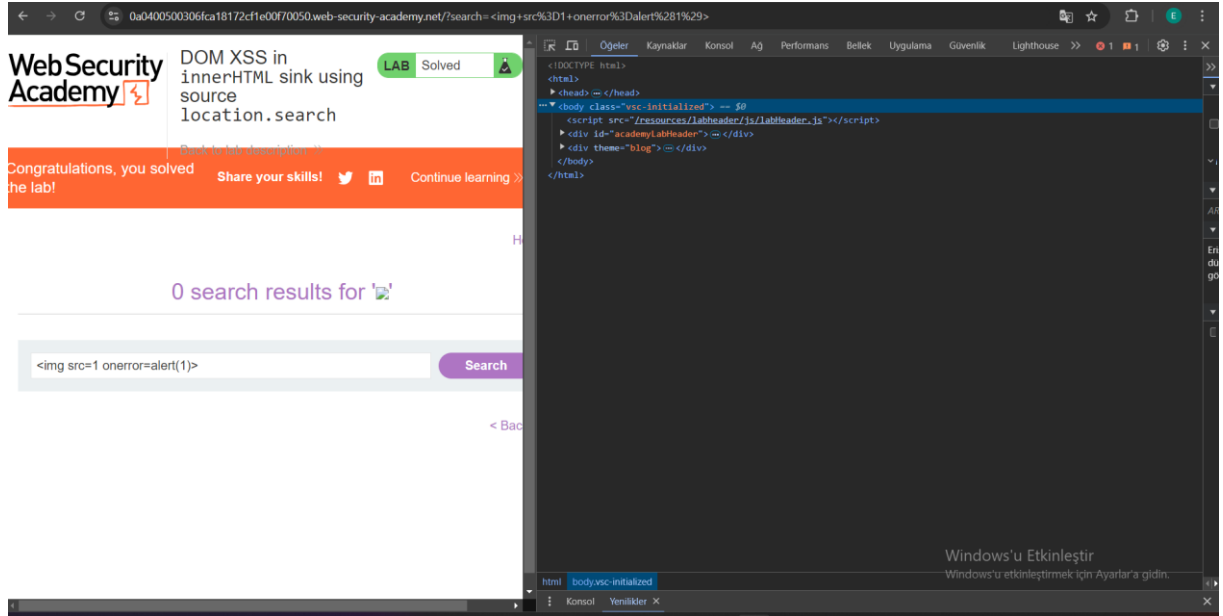
Bu kod, url deki "search" parametresini alıp sayfada yazdırıyor.

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

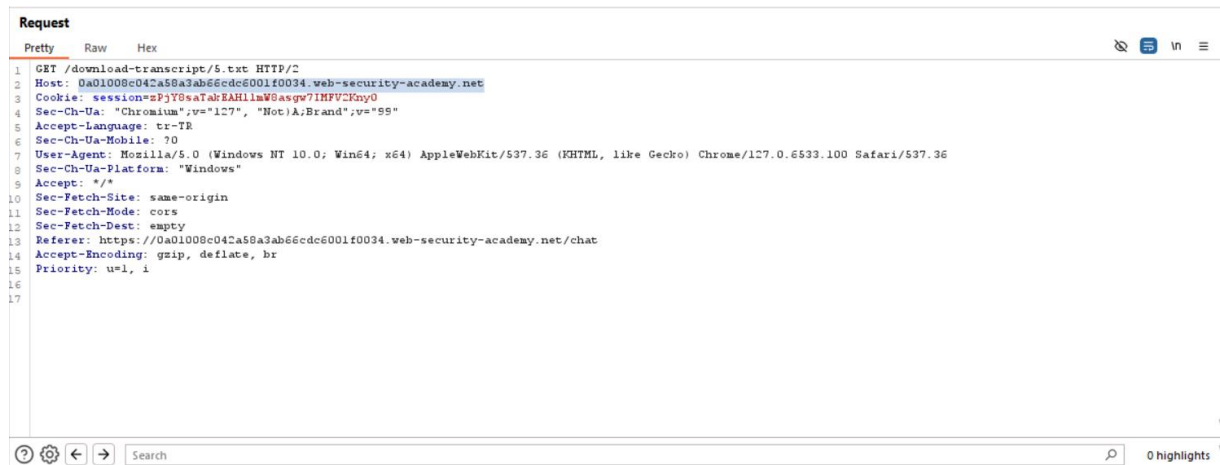
1)Lab: Insecure direct object references

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

Lab da verilen bilgide

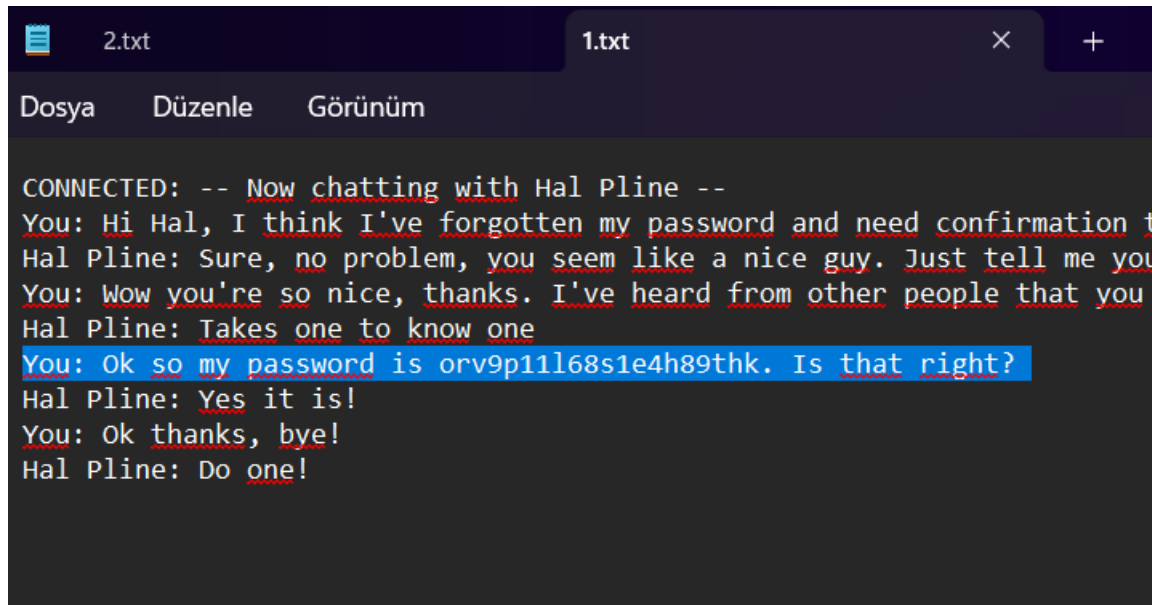
“Bu laboratuvar, kullanıcı sohbet kayıtlarını doğrudan sunucunun dosya sisteminde depolar ve bunları statik URL'ler kullanarak alır.”

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>

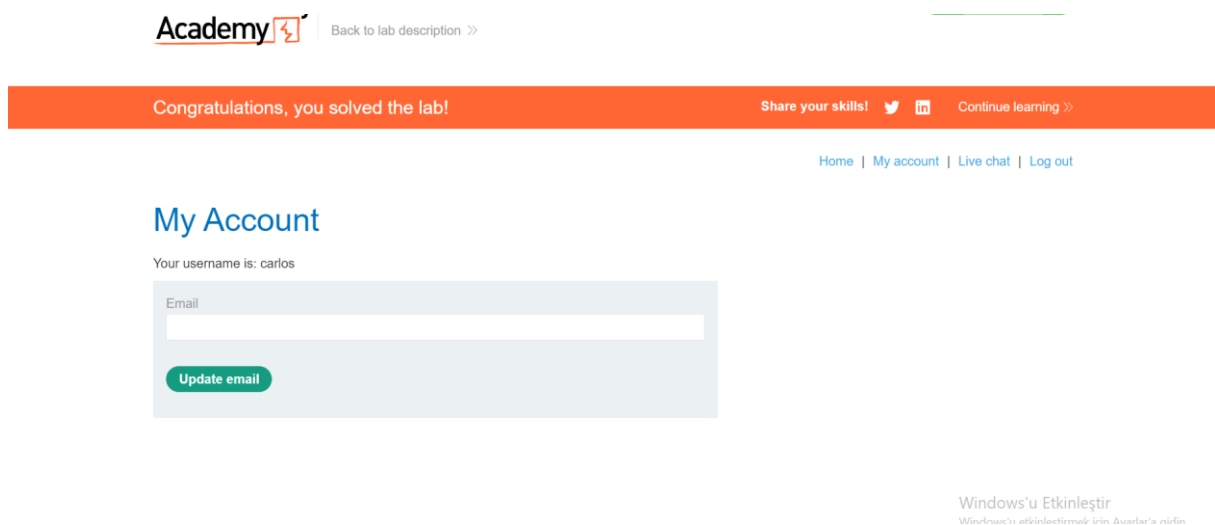
bu indirme linki sayesinde 1.txt dosyasına ulaştım.



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 three menu items: '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!
```

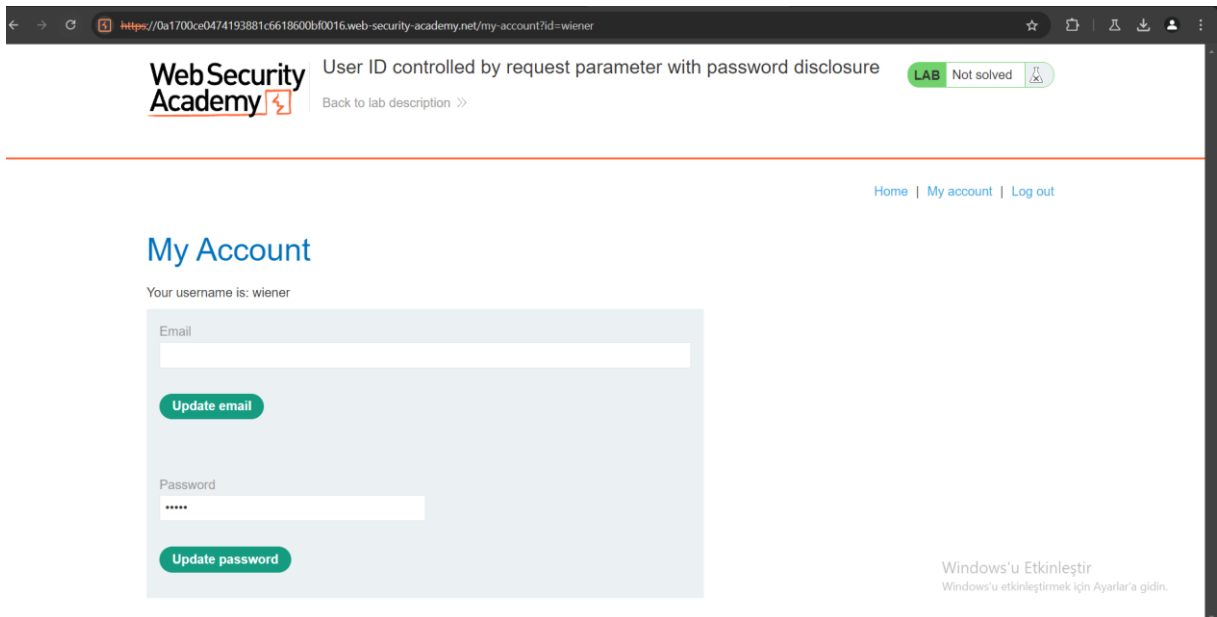
Txt dosyasından edindiğimiz şifre sayesinde Carlos un hesabına girdik.



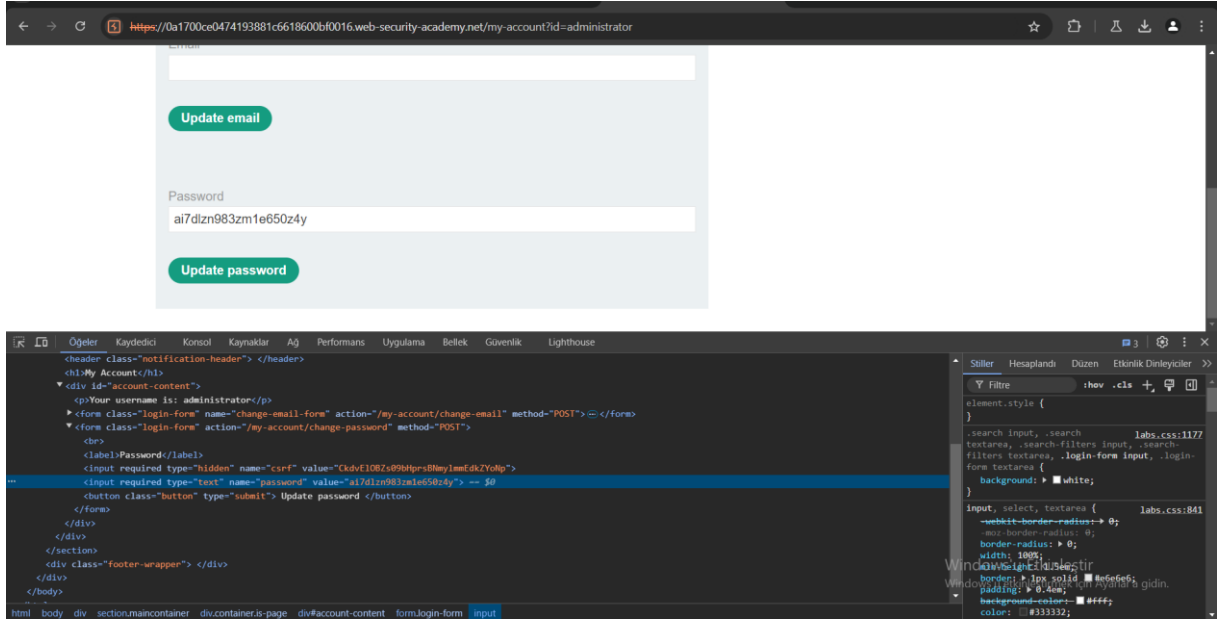
2) Lab: User ID controlled by request parameter with password disclosure

<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.

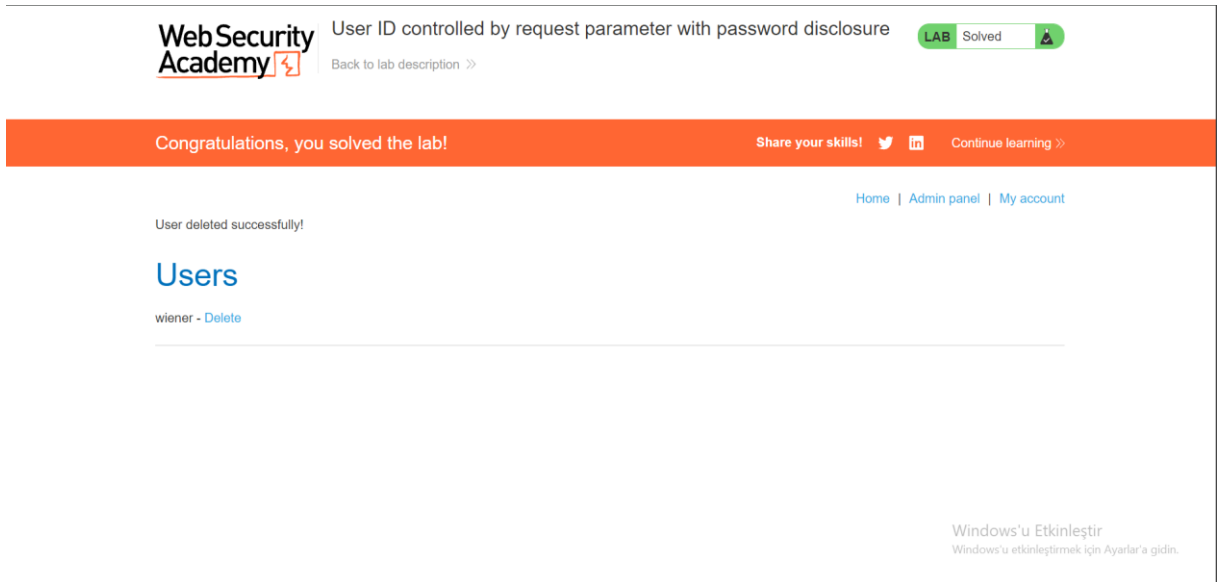


Wiener değiştirip admin ,administrator gibi kullanıcı adlarına sahip yetkilili bir kullanıcı olup olmadığını varsa geçiş yapıp yapamayacağımı denedim.



Administrator kullanıcıasına direkt geçiş yaptı şifre yerinde bir şifre olduğunu gördüm type ı password yerine text olarak değışince şifre gözükte.

Admin olarak giriş yaparak Carlos kullanıcıasını 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 Request tab is active, displaying a POST request to /login. The request body is a JSON object with fields: username, password, and api_key. The api_key value is M8duC6P6BcqW9ZwMiUJzYgddssSUj7At. The Inspector panel on the right shows the request headers, including Content-Type: application/json, 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, and 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. The status bar at the bottom indicates 0 highlights and 246.1MB memory usage.

Carlos olarak deęiřtirmem bir řeyi deęiřtirmedi.

```
Request
Pretty Raw Hex
1 GET /my-account?id=carlos HTTP/2
2 Host: 0a1e004503820e4880e867a500040034.web-security-academy.net
3 Cookie: session=1jvK4gzWvExtH8CqJekjeAIsj3CAYZJC
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium",v="127", "Not)A;Brand",v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: tr-TR
9 Upgrade-Insecure-Requests: 1
10 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
11 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
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://0a1e004503820e4880e867a500040034.web-security-academy.net/login
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19
20

Response
Pretty Raw Hex Render
50 </p>
51 <a href="/my-account?id=wiener">
52 My account
53 </a>
54 <p>
55 </p>
56 </p>
57 <a href="/logout">
58 Log out
59 </a>
60 <p>
61 </p>
62 </section>
63 </header>
64 <header class="notification-header">
65 </header>
66 <h1>
67 My Account
68 </h1>
69 <div id="account-content">
70 <p>
71 Your username is: carlos
72 </p>
73 <div>
74 Your API Key is: cHlnD8rvpB6jA8hBCEsc3MHaljoIuiU2
75 </div>
76 <br>
77 <form class="login-form" name="change-email-form" action="
78 /my-account/change-email" method="POST">
79 <label>
80 Email
81 </label>
82 <input required type="email" name="email" value="">
83 <input required type="hidden" name="csrf" value="
84 b8GTxJFgSbuBx1IEFwSkhyjS0dC4kMdt">
85 <button class="button" type="submit">
```

Bende repetir a tarak birde orda denedim ve Carlos un apı key ine ulaşmış oldum.

Web Security Academy

User ID controlled by request parameter with data leakage in redirect

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

Home | My account | Log out

My Account

Your username is: wiener

Your API Key is: M8duC6P6BcqW9ZwMIUJzYgddssSUj7At

Email

Update email

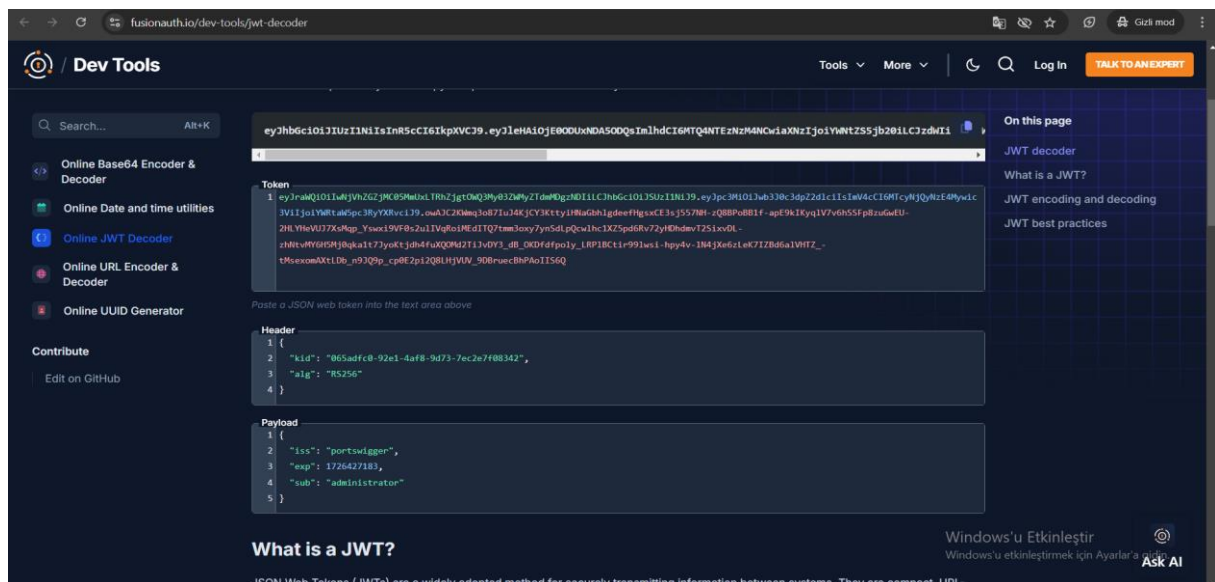
Ve cevap kısmına yapıştırdığımda lab çözülmüş oldu.

JWT (JSON Web Token)

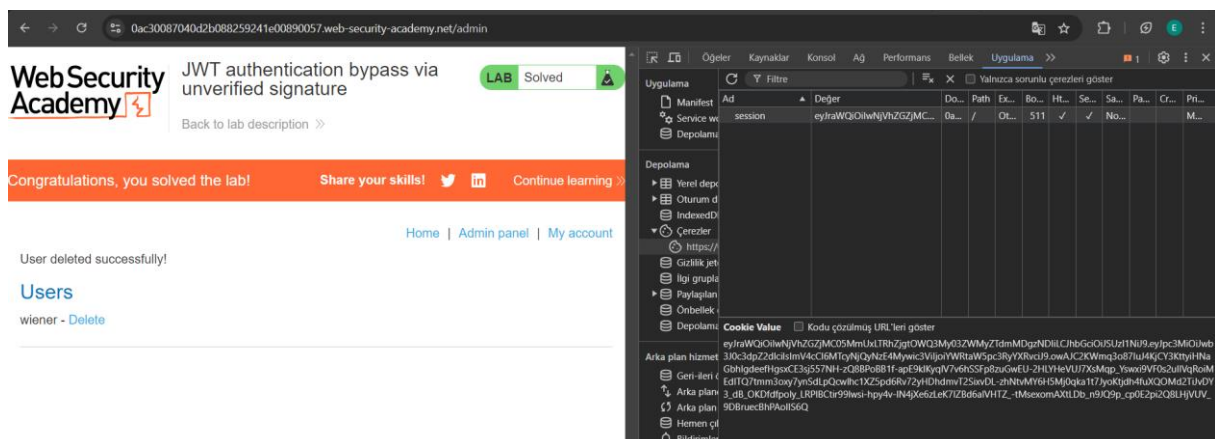
1) JWT authentication bypass via unverified signature

<https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-unverified-signature>

Labda bizden /admin e ulaşmamızı ardında Carlos kullanıcısını silmemizi istiyor.
wiener:peter olarak giriş yaptıktan sonra jwt toke ımı aldım ve düzenledim.



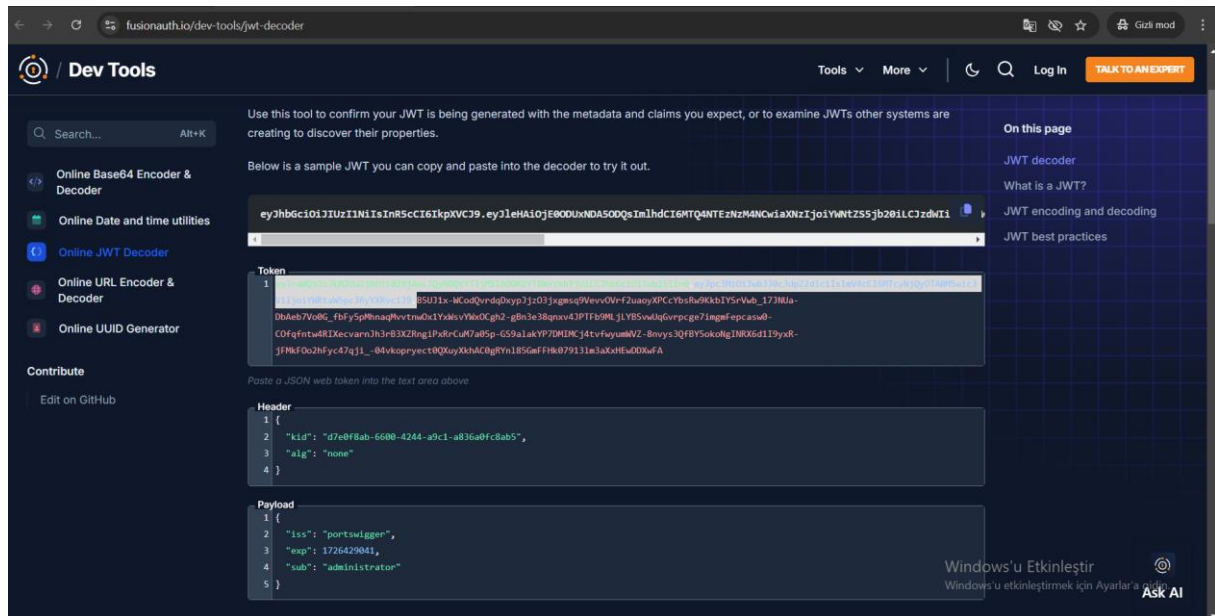
Yeni tokenımızı girdikten sonra kullanıcımızın administrator olarak değiştiğini gördüm ve Carlos kullancısını sildikten sonra lab çözülmüş oldu.



2) Lab: JWT authentication bypass via flawed signature verification

<https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-flawed-signature-verification>

Aynı şekilde labda verilen wiener:peter bilgileri ile giriş yaptıktan sonra elde ettiğim jwt token i düzenlemeye çalıştım ancak olmadı. Ardından Burp Suite ile araya girip farklı bir şey olup olmadığını kontrol ettim ancak yine elle tutulur bir şey bulamadım. Labda ki bilgileri tekrar okurken “Sunucu imzasız JWT'leri kabul edecek şekilde güvenli olmayan bir şekilde yapılandırılmıştır. “ bu kısım dikkatimi çekti ve internetten araştırdım. İmza algoritmasını “none” olarak değiştirdikten sonra sadece header ve payload kısmını session olarak kullanmam gerektiğini öğrendim.



Http isteğimi aşağıdaki gibi düzenledikten sonra admin olarak giriş yapabildim.

